

vSphere-Sicherheit

Update 2

Geändert am 27. April 2022

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

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

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

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

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

Copyright © 2009-2022 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Info zu vSphere Security 13

Aktualisierte Informationen 15

1 Sicherheit in der vSphere-Umgebung 17

Absichern des ESXi-Hypervisors 17

Sichern von vCenter Server-Systemen und zugehörigen Diensten 19

Sichern von virtuellen Maschinen 21

Schützen der virtuellen Netzwerkebene 22

Kennwörter in Ihrer vSphere-Umgebung 23

Best Practices und Ressourcen für die Sicherheit 25

2 vSphere-Authentifizierung mit vCenter Single Sign On 27

Grundlegendes zu vCenter Single Sign On 28

So schützt vCenter Single Sign On Ihre Umgebung 28

Komponenten für vCenter Single Sign On 31

Auswirkungen von vCenter Single Sign On auf Installationen 32

Auswirkungen von vCenter Single Sign On auf Upgrades 32

Verwenden von vCenter Single Sign On mit vSphere 35

Gruppen in der Domäne „vsphere.local“ 38

Kennwortanforderungen und Sperrverhalten für vCenter Server 39

Konfigurieren der vCenter Single Sign On-Identitätsquellen 40

Identitätsquellen für vCenter Server mit vCenter Single Sign On 41

Festlegen der Standarddomäne für vCenter Single Sign On 43

Hinzufügen einer vCenter Single Sign On-Identitätsquelle 44

Einstellungen der Active Directory-Identitätsquelle 46

Einstellungen der Active Directory-Identitätsquelle für LDAP-Server und OpenLDAP-Server 47

Bearbeiten einer vCenter Single Sign On-Identitätsquelle 48

Entfernen einer vCenter Single Sign On-Identitätsquelle 49

Verwenden von vCenter Single Sign On mit Windows-Sitzungsauthentifizierung 50

Zwei-Faktor-Authentifizierung vCenter Server 50

Konfigurieren der Smartcard-Authentifizierung für vCenter Single Sign-On 52

Konfigurieren der Smartcard-Authentifizierung über die Befehlszeile 53

Verwenden der Platform Services Controller-Webschnittstelle zum Verwalten der Smartcard-Authentifizierung 56

Festlegen von Widerrufsrichtlinien für die Smartcard-Authentifizierung 60

Einrichten der RSA SecurID-Authentifizierung 62

Verwalten des Anmelde-Banners	65
Verwenden von vCenter Single Sign On als Identitätsanbieter für andere Identitätsanbieter	65
Hinzufügen eines SAML-Dienstanbieters	66
Security Token Service STS	67
Generieren eines neuen STS-Signaturzertifikats auf der Appliance	68
Generieren eines neuen STS-Signaturzertifikats in einer Windows-Installation von vCenter	70
Aktualisieren des Zertifikats für den Security Token Service	71
Ermitteln des Ablaufdatums eines LDAPS-SSL-Zertifikats	73
Verwalten der vCenter Single Sign On-Richtlinien	73
Bearbeiten der vCenter Single Sign On-Kennwortrichtlinie	73
Bearbeiten der vCenter Single Sign On-Sperrrichtlinie	75
Bearbeiten der vCenter Single Sign On-Token-Richtlinie	75
Verwalten von vCenter Single Sign On-Benutzern und -Gruppen	77
Hinzufügen von vCenter Single Sign On-Benutzern	78
Aktivieren und Deaktivieren von vCenter Single Sign On-Benutzern	79
Löschen eines vCenter Single Sign On-Benutzers	80
Bearbeiten eines vCenter Single Sign On-Benutzers	80
Hinzufügen einer vCenter Single Sign On-Gruppe	81
Hinzufügen von Mitgliedern zu einer vCenter Single Sign On-Gruppe	81
Entfernen von Mitgliedern aus einer vCenter Single Sign On-Gruppe	82
Löschen von vCenter Single Sign On-Lösungsbenutzern	83
Ändern des vCenter Single Sign On-Kennworts	83
Best Practices für die Sicherheit von vCenter Single Sign On	84
Fehlerbehebung für vCenter Single Sign On	85
Ermitteln der Ursache eines Lookup Service-Fehlers	85
Anmelden unter Verwendung der Active Directory-Domänenauthentifizierung nicht möglich	87
vCenter Server-Anmeldung schlägt aufgrund des gesperrten Benutzerkontos fehl	88
Replizierung des VMware-Verzeichnisdiensts kann lange dauern	89

3 vSphere-Sicherheitszertifikate 91

Zertifikatsanforderungen für unterschiedliche Lösungspfade	92
Zertifikatsverwaltung – Übersicht	98
Übersicht Zertifikatsersetzung	100
Verwendung von Zertifikaten in vSphere 6.0	103
VMCA- und VMware-Kernidentitätsdienste	105
VMware Endpoint Certificate Store – Übersicht	106
Verwalten von Zertifikatswiderrufungen	108
Zertifikatsersetzung bei großen Bereitstellungen	108
Verwalten von Zertifikaten mit der Platform Services Controller-Webschnittstelle	111

Durchsuchen der Zertifikatspeicher über die Platform Services Controller-Webschnittstelle	112
Ersetzen von Zertifikaten durch neue VMCA-signierte Zertifikate über die Platform Services Controller-Webschnittstelle	113
Festlegen von VMCA über die Platform Services Controller-Webschnittstelle als Zwischenzertifizierungsstelle	114
Einrichten Ihres Systems für die Verwendung benutzerdefinierter Zertifikate des Platform Services Controller	117
Generieren von Zertifikatssignieranforderungen mit vSphere Certificate Manager (benutzerdefinierte Zertifikate)	117
Hinzufügen eines vertrauenswürdigen Rootzertifikats zum Zertifikatspeicher	118
Hinzufügen benutzerdefinierter Zertifikate aus dem Platform Services Controller	119
Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager	120
Rückgängigmachen des zuletzt ausgeführten Vorgangs durch die erneute Veröffentlichung alter Zertifikate	122
Alle Zertifikate zurücksetzen	122
Neugenerieren eines neuen VMCA-Rootzertifikats und Ersetzen aller Zertifikate	123
Festlegen von VMCA als Zwischenzertifizierungsstelle (Certificate Manager)	124
Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats (Zwischenzertifizierungsstelle)	124
Ersetzen des VMCA-Rootzertifikats durch benutzerdefiniertes Signierungszertifikat und Ersetzen aller Zertifikate	126
Ersetzen des Maschinen-SSL-Zertifikats durch ein VMCA-Zertifikat (Zwischenzertifizierungsstelle)	128
Ersetzen der Lösungsbenutzerzertifikate durch VMCA-Zertifikate (Zwischenzertifizierungsstelle)	129
Ersetzen aller Zertifikate durch benutzerdefinierte Zertifikate (Certificate Manager)	129
Generieren von Zertifikatssignieranforderungen mit vSphere Certificate Manager (benutzerdefinierte Zertifikate)	130
Ersetzen des Maschinen-SSL-Zertifikats durch ein benutzerdefiniertes Zertifikat	131
Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate	133
Manuelle Zertifikatsersetzung	134
Grundlegende Informationen zum Starten und Stoppen von Diensten	134
Ersetzen vorhandener VMCA-signierter Zertifikate durch neue VMCA-signierte Zertifikate	135
Generieren eines neuen VMCA-signierten Stammzertifikats	136
Ersetzen der Maschinen-SSL-Zertifikate durch VMCA-signierte Zertifikate	138
Ersetzen der Lösungsbenutzerzertifikate durch neue VMCA-signierte Stammzertifikate	142
Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus	148
Verwenden von VMCA als Zwischenzertifizierungsstelle	149
Ersetzen des Rootzertifikats (Zwischenzertifizierungsstelle)	150
Ersetzen der Maschinen-SSL-Zertifikate (Zwischenzertifizierungsstelle)	153
Ersetzen der Lösungsbenutzerzertifikate (Zwischenzertifizierungsstelle)	156
Ersetzen des VMware-Verzeichnisdienstzertifikats	162

Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus	163
Verwenden von Drittanbieterzertifikaten mit vSphere	164
Anfordern von Zertifikaten und Importieren eines benutzerdefinierten Rootzertifikats	165
Ersetzen der Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate	167
Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate	170
Ersetzen des VMware-Verzeichnisdienstzertifikats	171
Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus	173
Verwalten von Zertifikaten und Diensten mit CLI-Befehlen	174
Erforderliche Rechte für Zertifikatsverwaltungsvorgänge	175
Ändern der certool-Konfiguration	176
Befehlsreferenz für die certool-Initialisierung	177
Befehlsreferenz für die certool-Verwaltung	180
Befehlsreferenz für vecs-cli	183
Befehlsreferenz für dir-cli	187
Anzeigen von vCenter-Zertifikaten mit dem vSphere Web Client	193
Festlegen des Schwellenwerts für Warnungen zum Ablauf von vCenter-Zertifikaten	194

4 vSphere-Berechtigungen und Benutzerverwaltungsaufgaben 195

Grundlegende Informationen zur Autorisierung in vSphere	196
Grundlegendes zum vCenter Server-Berechtigungsmodell	197
Hierarchische Vererbung von Berechtigungen	199
Einstellungen für Mehrfachberechtigungen	201
Beispiel 1: Vererbung von mehreren Berechtigungen	202
Beispiel 2: Untergeordnete Berechtigungen, die übergeordnete Berechtigungen außer Kraft setzen	203
Beispiel 3: Überschreiben der Gruppenrolle durch die Benutzerrolle	203
Verwalten von Berechtigungen für vCenter-Komponenten	204
Hinzufügen einer Berechtigung zu einem Bestandslistenobjekt	205
Ändern von Berechtigungen	206
Entfernen von Berechtigungen	207
Ändern der Einstellungen für die Berechtigungsvalidierung	207
Globale Berechtigungen	208
Hinzufügen einer globalen Berechtigung	209
Berechtigungen für Tag-Objekte	210
Verwenden von Rollen zum Zuweisen von Rechten	211
vCenter Server-Systemrollen	213
Erstellen einer benutzerdefinierten Rolle	214
Klonen einer Rolle	214
Bearbeiten einer Rolle	215
Best Practices für Rollen und Berechtigungen	215

Erforderliche Berechtigungen für allgemeine Aufgaben 216

5 Sichern der ESXi-Hosts 220

Verwenden von Skripts zum Verwalten von Hostkonfigurationseinstellungen 221

Konfigurieren von ESXi-Hosts mit Hostprofilen 222

Allgemeine ESXi-Sicherheitsempfehlungen 223

Kennwörter und Kontosperrung für ESXi 225

ESXi-Netzwerksicherheitsempfehlungen 227

Deaktivieren des Browsers für verwaltete Objekte (MOB) 227

Deaktivieren autorisierter Schlüssel (SSH) 228

Zertifikatsverwaltung für ESXi-Hosts 228

Host-Upgrades und Zertifikate 231

Standardeinstellungen für ESXi-Zertifikate 232

Anzeigen von Informationen zum Ablauf von Zertifikaten für mehrere ESXi-Hosts 234

Anzeigen der Zertifikatsdetails für einen einzelnen ESXi-Host 234

Verlängern oder Aktualisieren von ESXi-Zertifikaten 235

Ändern der Standardeinstellungen für Zertifikate 236

Grundlegende Informationen zu Zertifikatmoduswechseln 236

Ändern des Zertifikatmodus 239

Ersetzen von ESXi SSL-Zertifikaten und -Schlüsseln 240

Voraussetzungen für ESXi-Zertifikatssignieranforderungen 241

Ersetzen des Standardzertifikats und -schlüssels über die ESXi Shell 241

Ersetzen eines Standardzertifikats und -schlüssels mit dem vifs-Befehl 242

Ersetzen eines Standardzertifikats mit HTTPS PUT 243

Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS (Benutzerdefinierte Zertifikate) 244

Verwenden benutzerdefinierter Zertifikate mit Auto Deploy 244

Wiederherstellen des ESXi-Zertifikats und der Schlüsseldateien 246

Anpassen von Hosts mit dem Sicherheitsprofil 247

ESXi-Firewall-Konfiguration 247

Verwalten von ESXi-Firewalleinstellungen 248

Hinzufügen von zulässigen IP-Adressen für einen ESXi-Host 249

Ein- und ausgehende Firewall-Ports für ESXi-Hosts 250

NFS-Client-Firewallverhalten 253

ESXi ESXCLI-Firewall-Befehle 254

Anpassen von ESXi-Diensten über das Sicherheitsprofil 255

Aktivieren oder Deaktivieren eines Diensts im Sicherheitsprofil 257

Sperrmodus 258

Verhalten im Sperrmodus 260

Aktivieren des Sperrmodus über vSphere Web Client 261

Deaktivieren des Sperrmodus mit dem vSphere Web Client 262

Aktivieren oder Deaktivieren des normalen Sperrmodus über die Benutzerschnittstelle der direkten Konsole	263
Angaben von Konten mit Zugriffsrechten im Sperrmodus	264
Überprüfen der Akzeptanzebenen von Hosts und VIBs	265
Zuweisen der Berechtigungen für ESXi	267
Rechte für Root-Benutzer	268
vpxuser-Rechte	269
DCUI-Benutzerrechte	269
Verwenden von Active Directory zum Verwalten von ESXi-Benutzern	270
Installieren oder Durchführen eines Upgrades von vSphere Authentication Proxy	270
Konfigurieren eines Hosts für die Verwendung von Active Directory	272
Hinzufügen eines Hosts zu einer Verzeichnisdienst-Domäne	273
Anzeigen der Verzeichnisdiensteinstellungen	274
Verwenden des vSphere Authentication Proxy	274
Installieren oder Durchführen eines Upgrades von vSphere Authentication Proxy	274
Konfigurieren eines Hosts zum Verwenden des vSphere Authentication Proxy für die Authentifizierung	276
Einrichten von vSphere Authentication Proxy	277
Exportieren des vSphere Authentication Proxy-Zertifikats	278
Importieren eines Proxy-Serverzertifikats in ESXi	278
Verwenden des vSphere Authentication Proxy zum Hinzufügen eines Hosts zu einer Domäne	279
Ersetzen des Authentifizierungs-Proxy-Zertifikats für den ESXi-Host	280
Empfohlene Vorgehensweisen für die Sicherheit von ESXi	280
PCI- und PCIe-Geräte sowie ESXi	281
Konfigurieren der Smartcard-Authentifizierung für ESXi	282
Smartcard-Authentifizierung aktivieren	283
Smartcard-Authentifizierung deaktivieren	284
Authentifizieren von Anmeldedaten im Falle von Konnektivitätsproblemen	284
Verwenden der Smartcard-Authentifizierung im Sperrmodus	284
ESXi-SSH-Schlüssel	285
SSH-Sicherheit	285
Hochladen eines SSH-Schlüssels mithilfe eines vifs-Befehls	286
Hochladen eines SSH-Schlüssels anhand von HTTPS PUT	286
Verwenden der ESXi Shell	287
Verwenden des vSphere Web Client zum Aktivieren des Zugriffs auf die ESXi Shell	288
Erstellen einer Zeitüberschreitung für die ESXi Shell-Verfügbarkeit im vSphere Web Client	289
Erstellen einer Zeitüberschreitung für ESXi Shell-Sitzungen im Leerlauf im vSphere Web Client	290
Verwenden der Benutzerschnittstelle der direkten Konsole (DCUI) für den Zugriff auf die ESXi Shell	290
Erstellen einer Zeitüberschreitung für die ESXi Shell-Verfügbarkeit in der Benutzerschnittstelle der direkten Konsole	291

Erstellen einer Zeitüberschreitung für die ESXi Shell-Sitzungen im Leerlauf	292
Anmelden bei der ESXi Shell zur Fehlerbehebung	292
Ändern von ESXi-Web-Proxy-Einstellungen	293
vSphere Auto Deploy-Sicherheitsüberlegungen	294
Verwalten der ESXi-Protokolldateien	294
Konfiguration von Syslog auf ESXi-Hosts	295
Speicherorte der ESXi-Protokolldateien	296
Sichern des Fault Tolerance-Protokollierungsdatenverkehrs	297
6 Sichern von vCenter Server-Systemen	298
Empfohlene Vorgehensweisen für die vCenter Server-Sicherheit	298
Best Practices für die vCenter Server-Zugriffssteuerung	298
Festlegen der vCenter Server-Kennwortrichtlinie	301
Schützen des vCenter Server Windows-Hosts	301
Entfernen abgelaufener oder widerrufen Zertifikate und Protokolle fehlgeschlagener Installationen	301
Begrenzen der vCenter Server-Netzwerkonnktivität	302
Einschränken der Verwendung von Linux-Clients	302
Untersuchen der installierten Plug-Ins	303
Empfohlene Vorgehensweisen für die Sicherheit von vCenter Server Appliance	304
Überprüfen der Fingerabdrücke bei Legacy-ESXi-Hosts	304
Überprüfen der Aktivierung der SSL-Zertifikatsvalidierung über eine Netzwerkdatei-Kopie	305
vCenter Server TCP- und UDP-Ports	306
Steuern des Zugriffs auf das CIM-basierte Hardwareüberwachungs-Tool	307
7 Sichern von virtuellen Maschinen	309
Beschränken informativer Meldungen von virtuellen Maschinen auf VMX-Dateien	309
Verhindern des Verkleinerns von virtuellen Festplatten	310
Virtuelle Maschine – Empfohlene Vorgehensweisen für die Sicherheit	311
Allgemeiner Schutz für virtuelle Maschinen	312
Verwendung von Vorlagen zum Bereitstellen von virtuellen Maschinen	313
Beschränken der Verwendung der VM-Konsole auf ein Minimum	313
Verhindern, dass virtuelle Maschinen Ressourcen in Besitz nehmen	314
Deaktivieren unnötiger Funktionen innerhalb von virtuellen Maschinen	314
Entfernen ungenutzter Hardwaregeräte	315
Deaktivieren nicht verwendeter Anzeigefunktionen	316
Deaktivieren nicht freigelegter Funktionen	316
Deaktivieren von HGFS-Dateiübertragungen	317
Deaktivieren von Kopier- und Einfügevorgängen zwischen Gastbetriebssystem und Remotekonsole	318
Begrenzen der Offenlegung vertraulicher Daten, die in die Zwischenablage kopiert wurden	319

- Beschränken der Ausführung von Befehlen durch Benutzer innerhalb einer virtuellen Maschine 319
- Verhindern, dass ein Benutzer oder Prozess auf einer virtuellen Maschine die Verbindung zu Geräten trennt 320
- Ändern des variablen Speicherlimits des Gastbetriebssystems 321
- Verhindern, dass Gastbetriebssystemprozesse Konfigurationsnachrichten an den Host senden 321
- Vermeiden der Verwendung von unabhängigen, nicht-dauerhaften Festplatten 322

8 Sichern der vSphere-Netzwerke 323

- Einführung in die Netzwerksicherheit in vSphere 323
- Absichern des Netzwerks mit Firewalls 325
 - Firewalls in Konfigurationen mit vCenter Server 326
 - Herstellen einer Verbindung mit einem vCenter Server über eine Firewall 327
 - Firewalls für Konfigurationen ohne vCenter Server 327
 - Verbinden von ESXi-Hosts über Firewalls 328
 - Herstellen einer Verbindung mit der VM-Konsole über eine Firewall 328
- Sichern des physischen Switches 329
- Sichern von Standard-Switch-Ports mit Sicherheitsrichtlinien 330
- Sichern von vSphere Standard-Switches 330
 - MAC-Adressänderungen 331
 - Gefälschte Übertragungen 332
 - Betrieb im Promiscuous-Modus 332
- Sichern von vSphere Distributed Switches und verteilten Portgruppen 333
- Absichern virtueller Maschinen durch VLANs 334
 - Sicherheitsempfehlungen für VLANs 335
 - Sichern von VLANs 336
- Erstellen einer Netzwerk-DMZ auf einem einzelnen ESXi-Host 336
- Erstellen mehrerer Netzwerke auf einem einzelnen ESXi-Host 338
- Internet Protocol Security (IPsec) 340
 - Auflisten der verfügbaren Sicherheitsverbindungen 341
 - Hinzufügen einer IPsec-Sicherheitsverbindung 341
 - Entfernen einer IPsec-Sicherheitsverbindung 342
 - Auflisten der verfügbaren IPsec-Sicherheitsrichtlinien 343
 - Erstellen einer IPsec-Sicherheitsrichtlinie 343
 - Entfernen einer IPsec-Sicherheitsrichtlinie 344
- Sicherstellen einer korrekten SNMP-Konfiguration 345
- Bedarfsgerechtes Verwenden von virtuellen Switches mit der vSphere Network Appliance-API 345
- vSphere Networking, empfohlene Vorgehensweisen für die Sicherheit 346
 - Allgemeine Netzwerksicherheitsempfehlungen 346
 - Bezeichnungen von Netzwerkkomponenten 348
 - Dokumentieren und Überprüfen der vSphere-VLAN-Umgebung 348

Einführen angemessener Netzwerkisolierungspraktiken 349

9 Empfohlene Vorgehensweisen für mehrere vSphere-Komponenten 351

Synchronisieren der Systemuhren im vSphere-Netzwerk 351

Synchronisieren der ESXi-Systemuhren mit einem NTP-Server 352

Konfigurieren der Uhrzeitsynchronisierungseinstellungen in vCenter Server Appliance 352

Verwenden der Uhrzeitsynchronisierung von VMware Tools 353

Hinzufügen oder Ersetzen von NTP-Servern in der vCenter Server Appliance-Konfiguration 353

Synchronisieren der Uhrzeit in vCenter Server Appliance mit einem NTP-Server 354

Speichersicherheit, empfohlene Vorgehensweisen 355

Absichern von iSCSI-Speicher 355

Schützen von iSCSI-Geräten 356

Schützen eines iSCSI-SAN 356

Maskieren von SAN-Ressourcen und Einteilen derselben in Zonen 357

Verwenden von Kerberos-Anmeldedaten für NFS 4.1 357

Überprüfen, ob das Senden von Host-Leistungsdaten an Gastbetriebssysteme deaktiviert ist 358

Einstellen von Zeitüberschreitungen für ESXi Shell und vSphere Web Client 359

10 Verwalten der Konfiguration des TLS-Protokolls mit dem TLS-Neukonfigurationsprogramm 360

Ports, die die Deaktivierung von TLS-Versionen unterstützen 360

Deaktivieren von TLS-Versionen in vSphere 362

Installieren des TLS-Konfigurationsprogramms 363

Durchführen einer optionalen manuellen Sicherung 364

Deaktivieren von TLS-Versionen auf vCenter Server-Systemen 366

Deaktivieren von TLS-Versionen auf ESXi-Hosts 367

Deaktivieren von TLS-Versionen auf Platform Services Controller-Systemen 369

Zurücksetzen von TLS-Konfigurationsänderungen 370

Deaktivieren von TLS-Versionen in vSphere Update Manager 372

Deaktivieren früherer TLS-Versionen für Update Manager-Port 9087 372

Deaktivieren früherer TLS-Versionen für Update Manager-Port 8084 373

Erneutes Aktivieren deaktivierter TLS-Versionen für Update Manager-Port 9087 374

Erneutes Aktivieren deaktivierter TLS-Versionen für Update Manager-Port 8084 375

11 Definierte Rechte 376

Alarmrechte 378

Rechte für Auto Deploy und Image-Profile 378

Zertifikatsrechte 380

Rechte für Inhaltsbibliotheken 380

Rechte für Datencenter 383

Berechtigungen für Datenspeicher 383

Rechte für Datenspeichercluster	384
Rechte für Distributed Switches	385
ESX Agent Manager-Rechte	386
Rechte für Erweiterungen	386
Rechte für Ordner	387
Globale Rechte	387
Host-CIM-Rechte	389
Rechte für die Hostkonfiguration	389
Hostbestandsliste	390
Rechte für lokale Hostoperationen	391
vSphere Replication-Rechte von Hosts	392
Hostprofil-Berechtigungen	392
Rechte für Inventory Service-Anbieter	393
Rechte für die Inventory Service-Kennzeichnung	393
Netzwerkberechtigungen	394
Leistungsrechte	395
Rechte für Berechtigungen	395
Profilgesteuerte Speicherrechte	396
Rechte für Ressourcen	396
Rechte für geplante Aufgaben	397
Sitzungsrechte	398
Speicheransichtsberechtigungen	398
Rechte für Aufgaben	399
Transfer Service-Rechte	399
VRM-Richtlinienberechtigungen	400
Berechtigungen für das Konfigurieren virtueller Maschinen	400
Rechte für Vorgänge als Gast auf virtuellen Maschinen	402
Rechte für die Interaktion virtueller Maschinen	403
Rechte für die Bestandsliste der virtuellen Maschine	416
Rechte für das Bereitstellen virtueller Maschinen	417
Rechte für die Dienstkonfiguration der virtuellen Maschine	419
Rechte für die Snapshot-Verwaltung von virtuellen Maschinen	420
vSphere Replication-Rechte der VM	420
dvPort-Gruppenrechte	421
vApp-Rechte	422
vServices-Rechte	423

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.

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
Authentifizierung mit vCenter Single Sign-On	<ul style="list-style-type: none">■ vCenter Single Sign-On-Funktionen und -Dienste.■ Hinzufügen und Verwalten von Identitätsquellen.■ vCenter Single Sign-On-Richtlinien.■ Benutzer und Gruppen.
Berechtigungen und Benutzerverwaltung	<ul style="list-style-type: none">■ Berechtigungsmodell (Rollen, Gruppen, Objekte).■ Erstellen von benutzerdefinierten Rollen.■ Festlegen von Berechtigungen.■ Verwalten globaler Berechtigungen.
Zertifikatsverwaltung	<ul style="list-style-type: none">■ ESXi-Zertifikatsverwaltung■ Zertifikatsverwaltung für vCenter Server und zugehörige Dienste.<ul style="list-style-type: none">■ Zertifikatsverwaltung über die Benutzeroberfläche.■ Zertifikatsverwaltung mit dem Dienstprogramm Certificate Manager.■ Verwenden der CLI für die manuelle Zertifikatsverwaltung (enthält Beispiele).
Funktionen für die Sicherheit von Hosts	<ul style="list-style-type: none">■ Sperrmodus und sonstige Sicherheitsprofilfunktionen.■ Smartcard-Authentifizierung für Host.■ vSphere Authentication Proxy.

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

Themen	Inhaltliche Schwerpunkte
Best Practices und Hardening für die Sicherheit	Best Practices und Rat von VMware-Sicherheitsexperten. <ul style="list-style-type: none"> ■ vCenter Server-Sicherheit. ■ Sicherheit von Hosts. ■ Sicherheit von virtuellen Maschinen. ■ Netzwerksicherheit.
vSphere-Rechte	Vollständige Auflistung aller in dieser Version unterstützten vSphere-Rechte.

Verwandte Dokumentation

Neben diesem Dokument veröffentlicht VMware für jede Version von vSphere ein *Hardening-Handbuch*, das unter <http://www.vmware.com/security/hardening-guides.html> verfügbar ist. Das *Hardening-Handbuch* ist ein Arbeitsblatt mit Einträgen für verschiedene potenzielle Sicherheitsprobleme. Es enthält Elemente für drei verschiedene Risikoprofile. Dieses *vSphere-Sicherheit*-Dokument enthält keine Informationen für Risikoprofil 1 (Umgebung mit der höchsten Sicherheit, zum Beispiel bei der höchsten Geheimhaltungsstufe in staatlichen Institutionen).

Zielgruppe

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

Aktualisierte Informationen

Die Dokumentation *vSphere-Sicherheit* wird in jeder Version des Produkts oder bei Bedarf aktualisiert.

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

Revision	Beschreibung
27. APR. 2022	<ul style="list-style-type: none">■ Geringfügiges Update für Speicheransichtsberechtigungen.
05. NOV. 2021	<ul style="list-style-type: none">■ Geringfügiges Update für Empfohlene Vorgehensweisen für die Sicherheit von ESXi.■ Deaktivieren von TLS-Versionen auf ESXi-Hosts wurde korrigiert, um anzugeben, dass Sie sich bei vCenter Server anmelden.
14. August 2020	<p>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.</p> <ul style="list-style-type: none">■ Geringfügiges Update für Sichern von virtuellen Maschinen.
4. Oktober 2017	<ul style="list-style-type: none">■ Geben Sie in Grundlegende Informationen zu Zertifikatmoduswechseln an, dass das Versetzen von Hosts in den Wartungsmodus und das Trennen der Verbindung akzeptabel sind, um den Moduswechsel durchzuführen. Das Entfernen der Hosts ist nicht erforderlich.
DE-001949-07	<ul style="list-style-type: none">■ Das neue Thema Zertifikatsanforderungen für unterschiedliche Lösungspfade, in dem Zertifikatsanforderungen beschrieben werden, wurde hinzugefügt. Das weniger ausführliche alte Thema wurde entfernt.■ Das neue Kapitel Kapitel 10 Verwalten der Konfiguration des TLS-Protokolls mit dem TLS-Neukonfigurationsprogramm wurde hinzugefügt.
DE-001949-06	<ul style="list-style-type: none">■ Unter Konfigurieren der Smartcard-Authentifizierung über die Befehlszeile wird jetzt deutlich darauf hingewiesen, dass Leerzeichen in durch Kommas getrennten Listen von Zertifikaten nicht zulässig sind.■ Der Skriptspeicherort wurde unter Konfigurieren der Smartcard-Authentifizierung über die Befehlszeile hinzugefügt.■ Unter Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate wurde klargestellt, dass die vollständige Zertifikatskette benötigt wird.■ In der Einführung zu Einstellungen für Mehrfachberechtigungen wurde ein Fehler korrigiert.
DE-001949-05	<ul style="list-style-type: none">■ Informationen zur Validierung und zum Validierungszeitraum wurden unter Ändern der Einstellungen für die Berechtigungsvalidierung hinzugefügt.
DE-001949-04	<ul style="list-style-type: none">■ Unter Überprüfen der Aktivierung der SSL-Zertifikatsvalidierung über eine Netzwerkdatei-Kopie wurde ein Fehler in einem Parameternamen korrigiert.■ Informationen zum Speicherort des Befehls <code>service-control</code> unter Windows wurden unter Verwalten von Zertifikaten und Diensten mit CLI-Befehlen hinzugefügt.

Revision	Beschreibung
DE-001949-03	<ul style="list-style-type: none"> ■ Informationen zu Tag-Berechtigungen wurden unter Berechtigungen für Tag-Objekte hinzugefügt. ■ Die Reihenfolge der Zertifikate wird in Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats (Zwischenzertifizierungsstelle) definiert.
DE-001949-02	<ul style="list-style-type: none"> ■ Ein Hinweis zur Anmeldung mit dem vSphere Client wurde in Kapitel 2 vSphere-Authentifizierung mit vCenter Single Sign On hinzugefügt. ■ Klarstellung unter Einstellungen der Active Directory-Identitätsquelle. Das System muss mit einem Active Directory-Namen verknüpft werden, und der Domänenname muss über DNS aufgelöst werden können.
DE-001949-01	<ul style="list-style-type: none"> ■ Die Reihenfolge der Zertifikate wurde unter Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats (Zwischenzertifizierungsstelle) korrigiert. ■ Der Abschnitt Kennwörter und Kontosperrung für ESXi wurde aktualisiert. Kennwortsätze sind standardmäßig nicht aktiviert. ■ Die Schritte für den Zugriff auf die Appliance-Shell wurden unter Konfigurieren der Smartcard-Authentifizierung über die Befehlszeile korrigiert. ■ Richtigstellung unter Ändern des vCenter Single Sign On-Kennworts. Wenn Ihr Kennwort abläuft, müssen Sie sich an den Administrator wenden. ■ Das PowerCLI-Skript unter Verwenden von Skripten zum Verwalten von Hostkonfigurationseinstellungen wurde aktualisiert. ■ Die Informationen zur Anzahl der vCenter Server-Instanzen in Auswirkungen von vCenter Single Sign On auf Installationen wurden aktualisiert. ■ Mehrere Änderungen an Konfigurieren der Smartcard-Authentifizierung über die Befehlszeile, Verwenden der Platform Services Controller-Webschnittstelle zum Verwalten der Smartcard-Authentifizierung und Einrichten der RSA SecurID-Authentifizierung. ■ Korrekturen unter vCenter Server TCP- und UDP-Ports. Beispielsweise werden Port 903 und Port 5900-5964 auf dem Host und nicht auf dem vCenter Server-System verwendet, und einige andere Ports, wie z. B. 9090, werden nur intern verwendet. ■ Informationen über DSA-Schlüssel wurden unter Hochladen eines SSH-Schlüssels mithilfe eines vifs-Befehls gelöscht. ■ Security Token Service STS wurde aktualisiert und enthält jetzt die Vorgehensweise zum Generieren eines neuen STS-Signaturzertifikats.
DE-001949-00	Erstversion.

Sicherheit in der vSphere-Umgebung

1

Die Komponenten einer vSphere-Umgebung sind ab Werk durch eine Vielzahl von Merkmalen wie Zertifikaten, Autorisierung, Firewalls auf jedem ESXi, beschränkten Zugriff 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. Damit genießen Sie höchste Flexibilität beim Sichern von vCenter Server-Systemen, ESXi-Hosts und virtuellen Maschinen.

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
- Sichern von vCenter Server-Systemen und zugehörigen Diensten
- Sichern von virtuellen Maschinen
- Schützen der virtuellen Netzwerkebene
- Kennwörter in Ihrer vSphere-Umgebung
- Best Practices und Ressourcen für die Sicherheit

Absichern des ESXi-Hypervisors

Der ESXi-Hypervisor ist standardmäßig gesichert. Sie können ESXi-Hosts mithilfe des Sperrmodus und anderer integrierter Funktionen noch besser schützen. Wenn Sie einen Referenzhost einrichten und anhand der Hostprofile dieses Hosts an allen Hosts Änderungen vornehmen oder wenn Sie Verwaltung mit Skripten durchführen, verbessern Sie den Schutz Ihrer Umgebung, indem Sie sicherstellen, dass Änderungen für alle Hosts gelten.

Verwenden Sie die folgenden, in diesem Handbuch ausführlich erläuterten Funktionen zum Erhöhen der Sicherheit von ESXi-Hosts, die von vCenter Server verwaltet werden. Weitere Informationen finden Sie im Whitepaper *Security of the VMware vSphere Hypervisor*.

Beschränkung 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 zum Hostobjekt über den vCenter Server, der den Host verwaltet, fest.

Verwenden von benannten Benutzern und der geringsten Berechtigung

Viele Aufgaben können vom Root-Benutzer standardmäßig durchgeführt werden. Anstatt Administratoren die Anmeldung beim ESXi-Host mit dem Root-Benutzerkonto zu erlauben, können Sie über die Schnittstelle von vCenter Server zum Verwalten von Berechtigungen verschiedene Rechte für die Hostkonfiguration für unterschiedliche benannte Benutzer anwenden. Sie können benutzerdefinierte Rollen erstellen, der Rolle Berechtigungen zuweisen und die Rolle mit einem benannten Benutzer und einem ESXi-Hostobjekt über den vSphere Web Client verknüpfen.

In einem Einzelhostszenario verwalten Sie Benutzer direkt. Informationen finden Sie in der Dokumentation *vSphere-Verwaltung mit dem vSphere 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.

Siehe [ESXi-Firewall-Konfiguration](#).

Automatisieren der ESXi-Hostverwaltung

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

Unter [Verwenden von Skripten zum Verwalten von Hostkonfigurationseinstellungen](#) und *Installations- und Einrichtungshandbuch für 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 und Ausnahmen für Benutzer definieren, um Direktzugriff auf Dienstkonten, wie beispielsweise Sicherheits-Agenten, zu ermöglichen.

Siehe [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 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.

Siehe [Überprüfen der Akzeptanzebenen von Hosts und VIBs](#).

Verwalten von ESXi-Zertifikaten

Ab vSphere 6.0 stellt die VMware-Zertifizierungsstelle (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 signiert wurden.

Siehe [Zertifikatsverwaltung für ESXi-Hosts](#).

Smartcard-Authentifizierung

Ab vSphere 6.0 unterstützt ESXi Chipkarten-Authentifizierung als Option anstelle der Authentifizierung mit dem Benutzernamen und dem Kennwort.

Siehe [Konfigurieren der Smartcard-Authentifizierung für ESXi](#).

ESXi-Kontosperrung

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 zehn fehlgeschlagenen Anmeldeversuchen gesperrt. Das Konto wird standardmäßig nach zwei Minuten entsperrt.

Siehe [Kennwörter und Kontosperrung für ESXi](#).

Die Sicherheitsüberlegungen für eigenständige Hosts sind ähnlich, obwohl die Verwaltungsaufgaben sich möglicherweise unterscheiden. Informationen finden Sie in der Dokumentation *vSphere-Verwaltung mit dem vSphere 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 einen 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. Siehe [Kapitel 3 vSphere-Sicherheitszertifikate](#).

Um zusätzlichen Schutz zu gewährleisten, entfernen Sie abgelaufene oder widerrufen 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 legen Sie ein Kennwort für den Benutzer „administrator@vsphere.local“ fest. Nur diese Domäne ist als Identitätsquelle verfügbar. Sie können weitere Identitätsquellen (entweder Active Directory oder LDAP) hinzufügen und eine Standardidentitätsquelle bestimmen. Ab diesem Zeitpunkt können die von einer Identitätsquelle authentifizierbaren Benutzer auch Objekte anzeigen und Aufgaben ausführen, sofern Sie die entsprechende Berechtigung besitzen. Siehe [Kapitel 2 vSphere-Authentifizierung mit vCenter Single Sign On](#).

Zuweisen von Rollen zu Benutzern und 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](#).

Achten Sie auf die zweckgemäße Verwendung der Administratorrechte und 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.

Siehe [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 Skripten 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 *vSphere-Administratorhandbuch für virtuelle 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.

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, virtuelle Netzwerkadapter usw. Beachten Sie auch folgende Richtlinien, über die Sie ausführlicher unter [Kapitel 8 Sichern der vSphere-Netzwerke](#) nachlesen können.

Isolieren des Netzwerkdatenverkehrs

Die Isolierung des Netzwerkdatenverkehrs ist für eine sichere ESXi-Umgebung maßgeblich. 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. Auf dieses Netzwerk dürfen nur System-, Netzwerk- und Sicherheitsadministratoren Zugriff haben.

Siehe [ESXi-Netzwerksicherheitsempfehlungen](#).

Schützen virtueller Netzwerkelemente durch Firewalls

Sie können Firewall-Ports öffnen und schließen und alle Elemente im virtuellen Netzwerk eigens schützen. Firewallregeln verknüpfen Dienste mit den entsprechenden Firewalls und die ESXi-Firewall je nach Dienststatus öffnen oder schließen.

Siehe [ESXi-Firewall-Konfiguration](#).

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*.

Schützen von VM-Netzwerken

Die Methoden, die Sie zur Absicherung eines Netzwerks von virtuellen Maschinen verwenden, hängen unter anderem davon ab, welches Gastbetriebssystem installiert wurde und ob die virtuellen Maschinen in einer sicheren 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.

Siehe [Kapitel 8 Sichern der vSphere-Netzwerke](#).

Schützen Ihrer Umgebung durch VLANs

ESXi unterstützt VLANs nach IEEE 802.1q, die zum weiteren Schutz des VM-Netzwerks oder der Speicherconfiguration verwendet werden können. Mit VLANs können Sie ein physisches Netzwerk in Segmente aufteilen, sodass zwei Computer im gleichen physischen Netzwerk nur dann Pakete untereinander versenden können, wenn sie sich im gleichen VLAN befinden.

Siehe [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 und – falls von Ihren Unternehmensrichtlinien so vorgeschrieben – beiderseitigem CHAP konfigurieren. Dies erfolgt über den vSphere Web Client oder über CLIs.

Siehe [Speichersicherheit, empfohlene Vorgehensweisen](#).

Verwendung von IPSec

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

Siehe [Internet Protocol Security \(IPsec\)](#).

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

Kennwörter in Ihrer vSphere-Umgebung

Kennwortbeschränkungen, Kennwortsperrn und der Kennwortablauf 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. Siehe [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, die Kennwortsperren und der Kennwortablauf sind abhängig von der Domäne des Benutzers sowie vom Benutzer.

administrator@vsphere.local

Das Kennwort für den Benutzer „administrator@vsphere.local“ bzw. für den Benutzer „administrator@*meineDomäne*“, falls Sie bei der Installation eine andere Domäne ausgewählt haben, läuft nicht ab und unterliegt nicht der Sperrrichtlinie. Ansonsten muss das Kennwort die in der vCenter Single Sign On-Kennwortrichtlinie festgelegten Beschränkungen einhalten. Siehe [Bearbeiten der vCenter Single Sign On-Kennwortrichtlinie](#).

Sollten Sie das Kennwort für diesen Benutzer vergessen, suchen Sie im VMware-Knowledgebase-System nach Informationen zum Zurücksetzen des Kennworts.

Andere vsphere.local-Benutzer

Die Kennwörter für andere vsphere.local-Benutzer bzw. für Benutzer der von Ihnen bei der Installation angegebenen lokalen Domäne müssen die von der vCenter Single Sign On-Kennwortrichtlinie und -Sperrrichtlinie festgelegten Beschränkungen einhalten. Siehe [Bearbeiten der vCenter Single Sign On-Kennwortrichtlinie](#) und [Bearbeiten der vCenter Single Sign On-Sperrrichtlinie](#). Diese Kennwörter laufen standardmäßig nach 90 Tage ab. Die Administratoren können jedoch den Kennwortablauf im Rahmen der Kennwortrichtlinie ändern.

Wenn ein Benutzer das Kennwort für vsphere.local vergisst, kann ein Administratorbenutzer das Kennwort mit dem Befehl `dir-cli` zurücksetzen.

Andere Benutzer

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

vCenter Single Sign On unterstützt eine Standardidentitätsquelle, und die Benutzer können sich beim vSphere Client mit ihren Benutzernamen anmelden. Die Domäne bestimmt die Kennwortparameter. Wenn sich Benutzer in einer Nicht-Standarddomäne als Benutzer anmelden möchten, können sie den Domänennamen angeben, also *Benutzer@Domäne* oder *Domäne\Benutzer*. Die Domänenkennwortparameter gelten auch in diesem Fall.

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 ein Kennwort für den Root-Benutzer der Appliance unter dem Linux-Betriebssystem und ein Kennwort für den Benutzer „administrator@vsphere.local“ an. Über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) 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	Empfohlene Vorgehensweisen für die Sicherheit von ESXi
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 benötigen.

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

Tabelle 1-2. Sicherheitsressourcen von VMware im Internet

Thema	Ressource
Sicherheitsrichtlinien von VMware, aktuelle Sicherheitswarnungen, Sicherheitsdownloads und themenspezifische Abhandlungen zu Sicherheitslücken.	http://www.vmware.com/go/security
Richtlinie zur Sicherheitsantwort	http://www.vmware.com/support/policies/security_response.html VMware hat es sich zur Aufgabe gemacht, Sie bei der Absicherung Ihrer virtuellen Umgebung zu unterstützen. Sicherheitslücken werden so schnell wie möglich beseitigt. Die VMware-Richtlinie zur Sicherheitsantwort dokumentiert unseren Einsatz für die Behebung möglicher Schwachstellen in unseren Produkten.
Richtlinie zur Unterstützung von Drittanbieter-Software	http://www.vmware.com/support/policies/vmtn/resources/ 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, wird der technische Support versuchen, 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
Hardening-Richtlinien für verschiedene Versionen von vSphere und anderen VMware-Produkten.	https://www.vmware.com/support/support-resources/hardening-guides.html
<i>Security of the VMware vSphere Hypervisor</i> (Whitepaper)	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

vSphere-Authentifizierung mit vCenter Single Sign On

2

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

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

Ab vSphere 6.0 ist vCenter Single Sign On Teil des Platform Services Controller. Der Platform Services Controller enthält die gemeinsam genutzten Dienste, die vCenter Server und vCenter Server-Komponenten unterstützen. Zu diesen Diensten gehören vCenter Single Sign On, VMware-Zertifizierungsstelle, Lizenzdienst und Lookup Service. Weitere Informationen zum Platform Services Controller finden Sie unter *Installations- und Einrichtungshandbuch für vSphere*.

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

Nachdem sich ein Benutzer bei vCenter Single Sign On authentifiziert hat, können Sie ihm erlauben, bestimmte Aufgaben durchzuführen. In den meisten Fällen weisen Sie vCenter Server-Berechtigungen zu, aber vSphere enthält andere Berechtigungsmodelle. Weitere Informationen hierzu finden Sie unter [Grundlegende Informationen zur Autorisierung in vSphere](#).

Hinweis Wenn Sie einem Active Directory-Benutzer die Anmeldung bei einer vCenter Server-Instanz unter Verwendung des vSphere Client mit SSPI ermöglichen möchten, müssen Sie die vCenter Server-Instanz zur Active Directory-Domäne hinzufügen. Informationen zum Hinzufügen einer vCenter Server Appliance mit einem externen Platform Services Controller zu einer Active Directory-Domäne finden Sie in dem VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/2118543>.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zu vCenter Single Sign On](#)
- [Konfigurieren der vCenter Single Sign On-Identitätsquellen](#)
- [Zwei-Faktor-Authentifizierung vCenter Server](#)

- Verwenden von vCenter Single Sign On als Identitätsanbieter für andere Identitätsanbieter
- Security Token Service STS
- Verwalten der vCenter Single Sign On-Richtlinien
- Verwalten von vCenter Single Sign On-Benutzern und -Gruppen
- Best Practices für die Sicherheit von vCenter Single Sign On
- Fehlerbehebung für vCenter Single Sign On

Grundlegendes zu vCenter Single Sign On

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



Domänen und Sites von vCenter Single Sign-On 6.0

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_y9pxac75/uiConfId/49694343/)

So schützt vCenter Single Sign On Ihre Umgebung

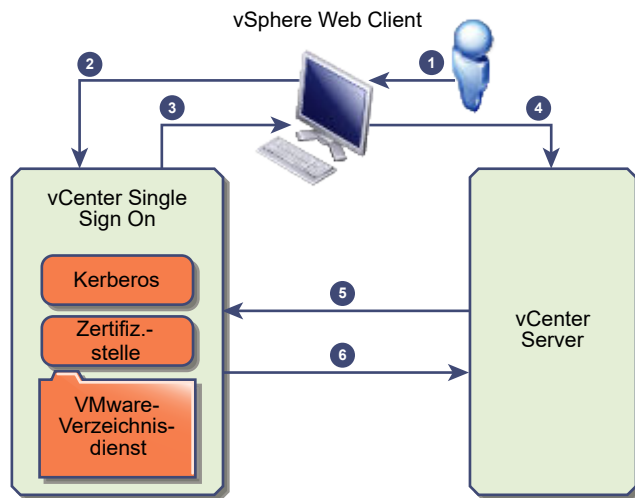
vCenter Single Sign On ermöglicht vSphere-Komponenten, über einen sicheren Token-Mechanismus miteinander zu kommunizieren, ohne dass die Benutzer sich bei jeder Komponente einzeln authentifizieren müssen.

vCenter Single Sign On verwendet eine Kombination aus STS (Security Token Service), SSL für sicheren Datenverkehr und Authentifizierung von Lösungsbenutzern durch Zertifikate und von anderen Benutzern (Personen) durch Active Directory oder OpenLDAP.

vCenter Single Sign On-Handshake für Personen als Benutzer

Die folgende Abbildung zeigt den Handshake für Personen als Benutzer.

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



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

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

- 2 Der vSphere Web Client leitet die Anmeldeinformationen an den vCenter Single Sign On-Dienst weiter, der das SAML-Token des vSphere Web Client überprüft. Wenn der vSphere Web Client über ein gültiges Token verfügt, überprüft vCenter Single Sign On weiterhin, ob sich der Benutzer in der konfigurierten Identitätsquelle (z. B. Active Directory) befindet.
 - Wenn nur der Benutzername verwendet wird, überprüft vCenter Single Sign On die Standarddomäne.
 - Ist ein Domänenname im Benutzernamen enthalten (*DOMÄNE\Benutzer1* oder *Benutzer1@DOMÄNE*), überprüft vCenter Single Sign On diese Domäne.
- 3 Wenn sich der Benutzer bei der Identitätsquelle authentifizieren kann, gibt vCenter Single Sign On ein Token zurück, das für den vSphere Web Client den Benutzer darstellt.
- 4 Der vSphere Web Client leitet das Token an das vCenter Server-System weiter.
- 5 vCenter Server überprüft gemeinsam mit dem vCenter Single Sign On-Server, ob das Token gültig und noch nicht abgelaufen ist.
- 6 Der vCenter Single Sign On-Server gibt das Token an das vCenter Server-System zurück und nutzt das Autorisierungs-Framework von vCenter Server, um den Benutzerzugriff zu ermöglichen.

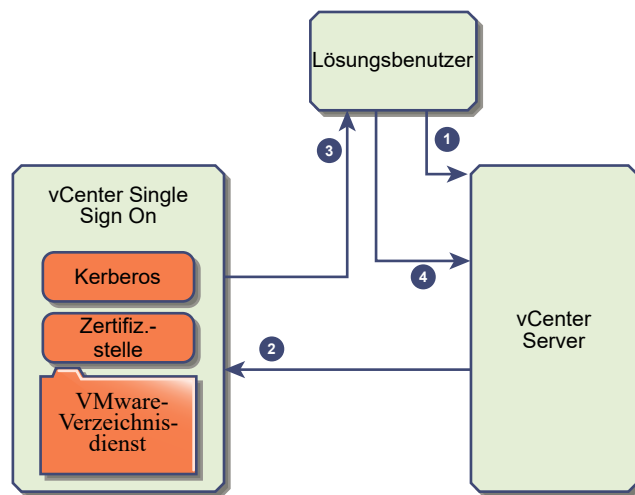
Der Benutzer kann sich nun authentifizieren und alle Objekte anzeigen und ändern, für die die Benutzerrolle über die entsprechenden Berechtigungen verfügt.

Hinweis Zu Beginn wird jedem Benutzer die Rolle „Kein Zugriff“ zugewiesen. Ein vCenter Server-Administrator muss dem jeweiligen Benutzer mindestens die Rolle für den Zugriff „Nur Lesen“ zuweisen, bevor sich der Benutzer anmelden kann. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer Berechtigung zu einem Bestandslistenobjekt](#).

vCenter Single Sign On-Handshake für Lösungsbenutzer

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

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



Für Lösungsbenutzer verläuft die Interaktion folgendermaßen:

- 1 Der Lösungsbenutzer versucht, eine Verbindung mit einem vCenter-Dienst herzustellen,
- 2 Der Lösungsbenutzer wird zu vCenter Single Sign On weitergeleitet. Wenn der Lösungsbenutzer für vCenter Single Sign On neu ist, muss er ein gültiges Zertifikat vorweisen.
- 3 Wenn das Zertifikat gültig ist, weist vCenter Single Sign On dem Lösungsbenutzer ein SAML-Token (Bearer-Token) zu. Das Token wird durch vCenter Single Sign On signiert.
- 4 Der Lösungsbenutzer wird dann zu vCenter Single Sign On weitergeleitet und kann Aufgaben entsprechend seinen Berechtigungen ausführen.
- 5 Wenn sich der Lösungsbenutzer beim nächsten Mal authentifizieren muss, kann er das SAML-Token zum Anmelden bei vCenter Server verwenden.

Dieser Handshake erfolgt standardmäßig automatisch, weil VMCA beim Starten Zertifikate für Lösungsbenutzer bereitstellt. Wenn gemäß der Unternehmensrichtlinie Drittanbieterzertifikate einer Zertifizierungsstelle benötigt werden, können Sie die Lösungsbenutzerzertifikate durch Drittanbieterzertifikate einer Zertifizierungsstelle ersetzen. Wenn diese Zertifikate gültig sind, weist vCenter Single Sign On dem Lösungsbenutzer ein SAML-Token zu. Siehe [Verwenden von Drittanbieterzertifikaten mit vSphere](#).

Komponenten für vCenter Single Sign On

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

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

STS (Security Token Service)

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

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

Verwaltungsserver

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

VMware Directory Service (vmdir)

Der VMware Directory Service (vmdir) ist der Domäne zugeordnet, die Sie während der Installation angeben, und wird in jede eingebettete Bereitstellung sowie auf jedem Platform Services Controller eingeschlossen. Bei diesem Dienst handelt es sich um einen mehrmandantenfähigen Verzeichnisdienst mit Peer-Replikation, der ein LDAP-Verzeichnis auf Port 389 zur Verfügung stellt. Der Dienst verwendet weiterhin Port 11711, um die Abwärtskompatibilität mit vSphere 5.5 und früheren Systemen zu gewährleisten.

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

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

Identitäts-Verwaltungsdienst

Bearbeitete Identitätsquellen und STS-Authentifizierungsanforderungen.

Auswirkungen von vCenter Single Sign On auf Installationen

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

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

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

Die Installationsreihenfolge ist wichtig.

Erste Installation

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

Nachfolgende Installationen

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

Auswirkungen von vCenter Single Sign On auf Upgrades

Wenn Sie ein Upgrade einer einfachen Installationsumgebung (Simple Install) auf eine eingebettete Bereitstellung von vCenter Server 6 durchführen, erfolgt das Upgrade nahtlos.

Beim Upgrade einer benutzerdefinierten Installation ist der vCenter Single Sign On-Dienst nach dem Upgrade Bestandteil des Platform Services Controller. Welche Benutzer sich nach der Durchführung eines Upgrades bei vCenter Server anmelden können, hängt von der Version, von der aus Sie das Upgrade durchführen, und von der Bereitstellungsconfiguration ab.

Im Rahmen des Upgrades können Sie festlegen, dass anstelle von „vsphere.local“ ein anderer vCenter Single Sign On-Domänenname verwendet wird.

Upgrade-Pfade

Das Ergebnis des Upgrades ist abhängig von den ausgewählten Installationsoptionen und vom Bereitstellungsmodell, auf das Sie upgraden.

Tabelle 2-1. Upgrade-Pfade

Quelle	Ergebnis
vSphere 5.5 und früher – einfache Installation	vCenter Server mit eingebettetem Platform Services Controller.
vSphere 5.5 und früher – benutzerdefinierte Installation	<p>Wenn sich vCenter Single Sign On auf einem anderen Knoten als vCenter Server befand, erhalten Sie eine Umgebung mit einem externen Platform Services Controller.</p> <p>Wenn sich vCenter Single Sign On auf demselben Knoten wie vCenter Server befand, andere Dienste jedoch auf anderen Knoten, erhalten Sie eine Umgebung mit einem eingebetteten Platform Services Controller.</p> <p>Wenn in der benutzerdefinierten Installation mehrere replizierte vCenter Single Sign On-Server vorhanden waren, erhalten Sie eine Umgebung mit mehreren replizierten Platform Services Controller-Instanzen.</p>

Benutzer, die sich nach dem Upgrade einer einfachen Installation anmelden können

Wenn Sie ein Upgrade einer Umgebung durchführen, die Sie mit der einfachen Installationsoption bereitgestellt haben, erhalten Sie stets eine Installation mit einem eingebetteten Platform Services Controller. Welche Benutzer sich anmelden dürfen, hängt davon ab, ob in der Quellumgebung vCenter Single Sign On vorhanden ist.

Tabelle 2-2. Anmelderechte nach dem Upgrade der einfachen Installationsumgebung

Quellversion	Anmeldezugriff für	Anmerkungen
vSphere 5.0	Benutzer des lokalen Betriebssystems administrator@vsphere.local	Möglicherweise werden Sie bei der Installation aufgefordert, die Administratoranmeldedaten des Root-Ordners in der vSphere-Bestandslistenhierarchie anzugeben. Wenn Ihre vorherige Installation Active Directory-Benutzer unterstützt hat, können Sie die Active Directory-Domäne als Identitätsquelle hinzufügen.
vSphere 5.1	Benutzer des lokalen Betriebssystems administrator@vsphere.local Admin@SystemDomain	Ab vSphere 5.5 unterstützt vCenter Single Sign On nur eine einzige standardmäßige Identitätsquelle. Die standardmäßige Identitätsquelle können Sie festlegen. Benutzer in einer Nicht-Standarddomäne können bei der Anmeldung die Domäne angeben (<i>DOMÄNE\Benutzer</i> oder <i>Benutzer@DOMÄNE</i>).
vSphere 5.5	„administrator@vsphere.local“ oder der Administrator der Domäne, die Sie während des Upgrades angegeben haben. Alle Benutzer aus allen Identitätsquellen können sich wie bisher anmelden.	

Bei einem Upgrade von vSphere 5.0, das vCenter Single Sign On nicht beinhaltet, auf eine Version, die vCenter Single Sign On beinhaltet, spielen die Benutzer in einem Verzeichnisdienst wie etwa Active Directory eine wesentlich wichtigere Rolle als Benutzer des lokalen Betriebssystems. Somit ist es nicht immer möglich oder sogar unerwünscht, lokale Betriebssystembenutzer als authentifizierte Nutzer beizubehalten.

Benutzer, die sich nach dem Upgrade einer benutzerdefinierten Installation anmelden können

Wenn Sie ein Upgrade einer Umgebung durchführen, die Sie mit der benutzerdefinierten Installationsoption bereitgestellt haben, hängt das Ergebnis von den ausgewählten Optionen ab:

- Wenn sich vCenter Single Sign On auf demselben Knoten wie das vCenter Server-System befand, erhalten Sie eine Installation mit einem eingebetteten Platform Services Controller.
- Wenn sich vCenter Single Sign On auf einem anderen Knoten als das vCenter Server-System befand, erhalten Sie eine Installation mit einem externen Platform Services Controller.

- Bei einem Upgrade von vSphere 5.0 können Sie im Rahmen des Upgrade-Vorgangs einen externen oder eingebetteten Platform Services Controller auswählen.

Die Anmelderechte nach dem Upgrade hängen von mehreren Faktoren ab.

Tabelle 2-3. Anmelderechte nach dem Upgrade der benutzerdefinierten Installationsumgebung

Quellversion	Anmeldezugriff für	Anmerkungen
vSphere 5.0	<p>vCenter Single Sign On erkennt Benutzer des lokalen Betriebssystems für die Maschine, auf der der Platform Services Controller installiert ist, jedoch nicht für die Maschine, auf der vCenter Server installiert ist.</p> <hr/> <p>Hinweis Die Verwendung von Benutzern des lokalen Betriebssystems für die Administration wird nicht empfohlen, insbesondere für Verbundumgebungen.</p> <hr/> <p>„administrator@vsphere.local“ kann sich bei vCenter Single Sign On und jeder vCenter Server-Instanz als Administratorbenutzer anmelden.</p>	<p>Wenn Ihre Installation der Version 5.0 zuvor Active Directory-Benutzer unterstützt hat, haben diese Benutzer nach dem Upgrade keinen Zugriff mehr. Die Active Directory-Domäne können Sie als Identitätsquelle hinzufügen.</p>
vSphere 5.1 oder vSphere 5.5	<p>vCenter Single Sign On erkennt Benutzer des lokalen Betriebssystems für die Maschine, auf der der Platform Services Controller installiert ist, jedoch nicht für die Maschine, auf der vCenter Server installiert ist.</p> <hr/> <p>Hinweis Die Verwendung von Benutzern des lokalen Betriebssystems für die Administration wird nicht empfohlen, insbesondere für Verbundumgebungen.</p> <hr/> <p>„administrator@vsphere.local“ kann sich bei vCenter Single Sign On und jeder vCenter Server-Instanz als Administratorbenutzer anmelden.</p> <p>Für Upgrades von vSphere 5.1 verfügt „Admin@SystemDomain“ über dieselben Rechte wie „administrator@vsphere.local“.</p>	<p>Ab vSphere 5.5 unterstützt vCenter Single Sign On nur eine einzige standardmäßige Identitätsquelle.</p> <p>Die standardmäßige Identitätsquelle können Sie festlegen.</p> <p>Benutzer in einer Nicht-Standarddomäne können bei der Anmeldung die Domäne angeben (<i>DOMÄNE\Benutzer</i> oder <i>Benutzer@DOMÄNE</i>).</p>

Verwenden von vCenter Single Sign On mit vSphere

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

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

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

vCenter Server-Berechtigungseinstellungen bestimmen in der Regel, welche Objekte der Benutzer anzeigen und welche Aufgaben er ausführen kann. vCenter Server-Administratoren weisen diese Berechtigungen über die Schnittstelle **Berechtigungen > verwalten** im vSphere Web Client zu, und nicht über vCenter Single Sign On. Weitere Informationen hierzu finden Sie unter [Kapitel 4 vSphere-Berechtigungen und Benutzerverwaltungsaufgaben](#).

vCenter Single Sign On- und vCenter Server-Benutzer

Mithilfe des vSphere Web Client authentifizieren sich Benutzer bei vCenter Single Sign On, indem sie ihre Anmeldedaten auf der Anmeldeseite des vSphere Web Client eingeben. Nach dem Herstellen der Verbindung mit vCenter Server können authentifizierte Benutzer alle vCenter Server-Instanzen oder andere vSphere-Objekte anzeigen, für die sie über die entsprechenden Rechte verfügen. Es ist keine weitere Authentifizierung erforderlich. Weitere Informationen hierzu finden Sie unter [Kapitel 4 vSphere-Berechtigungen und Benutzerverwaltungsaufgaben](#).

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

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

vCenter Single Sign On-Administratorbenutzer

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

Um vCenter Single Sign On zu konfigurieren und vCenter Single Sign On-Benutzer und -Gruppen zu verwalten, muss sich der Benutzer „administrator@vsphere.local“ oder ein Benutzer in der vCenter Single Sign On-Administratorengruppe beim vSphere Web Client anmelden. Bei der Authentifizierung kann der Benutzer über den vCenter Single Sign On auf die vSphere Web Client-Verwaltungsschnittstelle zugreifen und Identitätsquellen und Standarddomänen verwalten, Kennwortrichtlinien angeben und andere Verwaltungsaufgaben durchführen. Weitere Informationen hierzu finden Sie unter [Konfigurieren der vCenter Single Sign On-Identitätsquellen](#).

Hinweis Sie können den Benutzer administrator@vsphere.local nicht umbenennen.

Um die Sicherheit zu verbessern, können Sie zusätzliche benannte Benutzer in der Domäne „vsphere.local“ erstellen und ihnen Administratorrechte zuweisen. Verwenden Sie administrator@vsphere.local dann nicht mehr.

Authentifizierung in verschiedenen Versionen von vSphere

Wenn ein Benutzer eine Verbindung zu einem vCenter Server-System mit Version 5.0.x oder früher herstellt, authentifiziert vCenter Server den Benutzer, indem dieser anhand einer Active Directory-Domäne bzw. der Liste der lokalen Benutzer des Betriebssystems validiert wird. In vCenter Server 5.1 und höher authentifizieren sich Benutzer über vCenter Single Sign-On.

Hinweis Sie können vSphere Web Client nicht verwenden, um vCenter Server der Version 5.0 oder früher zu verwalten. Aktualisieren Sie vCenter Server auf Version 5.1 oder höher.

ESXi-Benutzer

ESXi ist nicht in vCenter Single Sign On integriert. Sie fügen den ESXi-Host explizit zu einer Active Directory-Domäne hinzu. Weitere Informationen hierzu finden Sie unter [Konfigurieren eines Hosts für die Verwendung von Active Directory](#).

Sie können weiterhin lokale ESXi-Benutzer mit vSphere Client, vCLI oder PowerCLI erstellen. vCenter Server kennt keine lokalen Benutzer von ESXi und ESXi kennt keine vCenter Server-Benutzer.

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

Vorgehensweise zum Anmelden bei vCenter Server-Komponenten

Wenn sich ein Benutzer vom vSphere Web Client aus bei einem vCenter Server-System anmeldet, hängt das Anmeldeverhalten davon ab, ob der Benutzer sich in der Standarddomäne befindet, d. h., in der als Standard-Identitätsquelle festgelegten Domäne.

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

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

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

Gruppen in der Domäne „vsphere.local“

Die Gruppe „vsphere.local domain“ enthält mehrere vordefinierte Gruppen. Weisen Sie einer dieser Gruppen Benutzer zu, damit sie die entsprechenden Aktionen ausführen können.

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

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

Folgende Gruppen sind in vsphere.local vordefiniert.

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

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

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

Recht	Beschreibung
Benutzer	Benutzer in der Domäne vsphere.local
SolutionUsers	Gruppe der Lösungsbenutzer in vCenter-Diensten. Jeder Lösungsbenutzer authentifiziert sich mit einem Zertifikat einzeln bei vCenter Single Sign On. Standardmäßig liefert VMCA die Zertifikate für Lösungsbenutzer. Fügen Sie dieser Gruppe Mitglieder nicht explizit zu.
CAAdmins	Mitglieder der Gruppe CAAAdmins besitzen Administratorrechte für VMCA. Das Hinzufügen von Mitgliedern zu dieser Gruppe wird generell nicht empfohlen.

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

Recht	Beschreibung
DCAdmins	<p>Mitglieder der Gruppe DCAdmins dürfen Domänencontroller-Administratoraktionen im VMware-Verzeichnisdienst ausführen.</p> <p>Hinweis Verwalten Sie den Domänencontroller nicht direkt. Verwenden Sie für die entsprechenden Aufgaben stattdessen die <code>vmdir</code>-CLI oder den vSphere Web Client.</p>
SystemConfiguration.BashShellAdministrators	Diese Gruppe ist auf Bereitstellungen der vCenter Server Appliance beschränkt. Ein Benutzer in dieser Gruppe kann den Zugriff auf die BASH-Shell aktivieren und deaktivieren. Standardmäßig können Benutzer, die sich über SSH mit der vCenter Server Appliance verbinden, nur Befehle in der eingeschränkten Shell verwenden. Benutzer in dieser Gruppe haben hingegen Zugriff auf die BASH-Shell.
ActAsUsers	Mitglieder der Gruppe ActAsUsers dürfen ActAs-Token aus vCenter Single Sign On abrufen.
ExternalIPDUsers	Diese Gruppe wird in vSphere nicht verwendet. Sie wird nur in Verbindung mit VMware vCloud Air benötigt.
SystemConfiguration.Administrators	Mitglieder der Gruppe SystemConfiguration.Administrators können die Systemkonfiguration im vSphere Web Client anzeigen und verwalten. Diese Benutzer dürfen Dienste anzeigen, starten und neu starten, Fehlerbehebung in den Diensten ausführen und die verfügbaren Knoten anzeigen und verwalten.
DCClients	<p>Diese Gruppe wird intern verwendet, um dem Verwaltungsknoten den Datenzugriff im VMware-Verzeichnisdienst zu ermöglichen.</p> <p>Hinweis Nehmen Sie an dieser Gruppe keine Änderungen vor. Jede Änderung kann Ihre Zertifikatinfrastruktur beeinträchtigen.</p>
ComponentManager.Administrators	Mitglieder der Gruppe ComponentManager.Administrators dürfen Component Manager-APIs abrufen, mit denen ein Dienst registriert oder dessen Registrierung aufgehoben werden kann. Das bedeutet, dass sie Dienste ändern können. Für einen reinen Lesezugriff auf die Dienste ist die Mitgliedschaft in dieser Gruppe nicht notwendig.
LicenseService.Administrators	Mitglieder der Gruppe LicenseService.Administrators haben vollständigen Schreibzugriff auf alle lizenzierungsbezogenen Daten und dürfen Seriennummernschlüssel für alle im Lizenzierungsdienst registrierten Produktassets hinzufügen, entfernen, zuweisen und widerrufen.
Administratoren	Administratoren des VMware-Verzeichnisdiensts (<code>vmdir</code>). Mitglieder dieser Gruppe können Verwaltungsaufgaben in vCenter Single Sign On ausführen. Das Hinzufügen von Mitgliedern zu dieser Gruppe wird generell nicht empfohlen.

Kennwortanforderungen und Sperrverhalten für vCenter Server

Beim Verwalten der Umgebung müssen Sie die vCenter Single Sign On-Kennwortrichtlinie, die vCenter Server-Kennwörter und das Sperrverhalten berücksichtigen.

vCenter Single Sign On-Administratorkennwort

Das Kennwort für administrator@vsphere.local muss die folgenden Anforderungen erfüllen:

- Mindestens 8 Zeichen
- Mindestens einen Kleinbuchstaben
- Mindestens ein numerisches Zeichen
- Mindestens ein Sonderzeichen

Das Kennwort für administrator@vsphere.local darf maximal 20 Zeichen lang sein. Nur sichtbare ASCII-Zeichen sind zulässig. Das bedeutet beispielsweise, dass kein Leerzeichen verwendet werden darf.

vCenter Server-Kennwörter

In vCenter Server werden die Kennwortanforderungen von vCenter Single Sign On oder von der konfigurierten Identitätsquelle bestimmt, die Active Directory, OpenLDAP oder das lokale Betriebssystem für den vCenter Single Sign On-Server (nicht empfohlen) sein können.

Sperrverhalten

Benutzer werden nach einer vorher festgelegten Anzahl von aufeinanderfolgenden Fehlversuchen gesperrt. Standardmäßig werden Benutzer innerhalb von drei Minuten nach fünf aufeinanderfolgenden Fehlerversuchen gesperrt. Ein gesperrtes Konto wird automatisch nach fünf Minuten wieder entsperrt. Sie können diese Standardeinstellungen anhand der Sperrrichtlinie ändern. Weitere Informationen hierzu finden Sie unter [Bearbeiten der vCenter Single Sign On-Sperrrichtlinie](#).

Ab vSphere 6.0 ist der Systemdomänenadministrator, also standardmäßig administrator@vsphere.local, von der Sperrrichtlinie nicht betroffen.

Jeder Benutzer kann sein Kennwort mit dem Befehl `dir-cli password change` ändern. Wenn ein Benutzer das Kennwort vergisst, kann der Administrator das Kennwort mit dem Befehl `dir-cli password reset` zurücksetzen.

Unter [Kennwörter und Kontosperrung für ESXi](#) werden Kennwörter von lokalen ESXi-Benutzern besprochen.

Konfigurieren der vCenter Single Sign On-Identitätsquellen

Wenn sich ein Benutzer anmeldet, überprüft vCenter Single Sign On für die Standardidentitätsquelle, ob sich dieser Benutzer authentifizieren kann. Sie können Identitätsquellen hinzufügen und entfernen sowie den Standardwert ändern.

Sie konfigurieren vCenter Single Sign On über den vSphere Web Client. Um vCenter Single Sign On zu konfigurieren, müssen Sie über vCenter Single Sign On-Administratorrechte verfügen. vCenter Single Sign On-Administratorrechte unterscheiden sich von der Administratorrolle in vCenter Server oder ESXi. Standardmäßig verfügt in einer neuen Installation nur der Benutzer `administrator@vsphere.local` über Administratorrechte für den vCenter Single Sign On-Server.

- **Identitätsquellen für vCenter Server mit vCenter Single Sign On**

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

- **Festlegen der Standarddomäne für vCenter Single Sign On**

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

- **Hinzufügen einer vCenter Single Sign On-Identitätsquelle**

Benutzer können sich nur bei vCenter Server anmelden, wenn sie sich in einer Domäne befinden, die als eine vCenter Single Sign On-Identitätsquelle hinzugefügt wurde. vCenter Single Sign On-Administratorbenutzer können Identitätsquellen aus dem vSphere Web Client hinzufügen.

- **Bearbeiten einer vCenter Single Sign On-Identitätsquelle**

vSphere-Benutzer werden in einer Identitätsquelle definiert. Sie können die Details einer Identitätsquelle bearbeiten, die vCenter Single Sign On zugewiesen ist.

- **Entfernen einer vCenter Single Sign On-Identitätsquelle**

vSphere-Benutzer werden in einer Identitätsquelle definiert. Sie können eine Identitätsquelle aus der Liste der registrierten Identitätsquellen entfernen.

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

Sie können vCenter Single Sign On mit der Windows-Sitzungsauthentifizierung (SSPI) verwenden. Um das Kontrollkästchen auf der Anmeldeseite verfügbar zu machen, muss das Client-Integrations-Plug-In installiert werden.

Identitätsquellen für vCenter Server mit vCenter Single Sign On

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

Eine Identitätsquelle ist eine Sammlung von Benutzer- und Gruppendaten. Die Benutzer- und Gruppendaten werden in Active Directory, OpenLDAP oder lokal im Betriebssystem der Maschine, auf der vCenter Single Sign On installiert ist, gespeichert.

Nach der Installation hat jede Instanz von vCenter Single Sign On die Identitätsquelle *Ihr_Domänenname*, z. B. „vsphere.local“. Diese Identitätsquelle ist für vCenter Single Sign On intern. Ein vCenter Single Sign On-Administrator kann Identitätsquellen hinzufügen, die Standardidentitätsquelle festlegen und Benutzer und Gruppen in der Identitätsquelle „vsphere.local“ erstellen.

Typen von Identitätsquellen

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

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

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

- vCenter Single Sign On-Systembenutzer. Genau eine Systemidentitätsquelle, nämlich „vsphere.local“, wird bei der Installation von vCenter Single Sign On erstellt. Wird als **vsphere.local** auf dem vSphere Web Client angezeigt.

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

Die vCenter Single Sign On-Identitätsquellen werden von vCenter Single Sign On-Administratorbenutzern verwaltet.

Sie können einer vCenter Single Sign On-Serverinstanz Identitätsquellen hinzufügen. Remoteidentitätsquellen sind auf Active Directory- und OpenLDAP-Server-Implementierungen beschränkt.

Festlegen der Standarddomäne für vCenter Single Sign On

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

Wenn sich ein Benutzer vom vSphere Web Client aus bei einem vCenter Server-System anmeldet, hängt das Anmeldeverhalten davon ab, ob der Benutzer sich in der Standarddomäne befindet, d. h., in der als Standard-Identitätsquelle festgelegten Domäne.

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

Verfahren

- 1 Melden Sie sich beim vSphere Web Client als „administrator@vsphere.local“ oder als anderer Benutzer mit vCenter Single Sign On-Administratorrechten an.
Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Navigieren Sie zu **Verwaltung > Single Sign On > Konfiguration**.

- 3 Wählen Sie auf der Registerkarte **Identitätsquellen** eine Identitätsquelle aus, und klicken Sie auf das Symbol **Als Standarddomäne festlegen**.

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

Hinzufügen einer vCenter Single Sign On-Identitätsquelle

Benutzer können sich nur bei vCenter Server anmelden, wenn sie sich in einer Domäne befinden, die als eine vCenter Single Sign On-Identitätsquelle hinzugefügt wurde. vCenter Single Sign On-Administratorbenutzer können Identitätsquellen aus dem vSphere Web Client hinzufügen.

Eine Identitätsquelle kann eine native Active Directory-Domäne (Integrierte Windows-Authentifizierung) oder ein OpenLDAP-Verzeichnisdienst sein. Active Directory ist als ein LDAP-Server verfügbar, um die Abwärtskompatibilität zu gewährleisten. Siehe [Identitätsquellen für vCenter Server mit vCenter Single Sign On](#).

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

localos

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

vsphere.local

Enthält die internen Benutzer von vCenter Single Sign On.

Voraussetzungen

Die Domäne, die Sie als Identitätsquelle hinzufügen möchten, muss für die Maschine verfügbar sein, auf der vCenter Single Sign On ausgeführt wird. Wenn Sie eine vCenter Server Appliance verwenden, finden Sie dazu weitere Informationen in der Dokumentation zu *vCenter Server Appliance-Konfiguration*.

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Navigieren Sie zu **Verwaltung > Single Sign-On > Konfiguration**.
- 3 Klicken Sie auf der Registerkarte **Identitätsquelle** auf das Symbol **Identitätsquelle hinzufügen**.

- 4 Wählen Sie die Art der Identitätsquelle aus und geben Sie die Einstellungen für die Identitätsquelle ein.

Option	Beschreibung
Active Directory (Integrierte Windows-Authentifizierung)	Verwenden Sie diese Option für native Active Directory-Implementierungen. Die Maschine, auf der der vCenter Single Sign On-Dienst ausgeführt wird, muss sich in einer Active Directory-Domäne befinden, wenn Sie diese Option verwenden möchten. Weitere Informationen hierzu finden Sie unter Einstellungen der Active Directory-Identitätsquelle .
Active Directory als ein LDAP-Server	Diese Option ist verfügbar, um die Abwärtskompatibilität zu gewährleisten. Sie setzt voraus, dass Sie den Domänencontroller und andere Informationen angeben. Weitere Informationen hierzu finden Sie unter Einstellungen der Active Directory-Identitätsquelle für LDAP-Server und OpenLDAP-Server .
OpenLDAP	Verwenden Sie diese Option für eine OpenLDAP-Identitätsquelle. Weitere Informationen hierzu finden Sie unter Einstellungen der Active Directory-Identitätsquelle für LDAP-Server und OpenLDAP-Server .
LocalOS	Verwenden Sie diese Option, um das lokale Betriebssystem als Identitätsquelle hinzuzufügen. Sie müssen nur den Namen des lokalen Betriebssystems angeben. Bei Auswahl dieser Option werden alle Benutzer der angegebenen Maschine von vCenter Single Sign On erkannt, auch wenn diese Benutzer nicht zu einer anderen Domäne gehören.

Hinweis Wenn das Benutzerkonto gesperrt oder deaktiviert ist, schlagen die Authentifizierungen sowie Gruppen- und Benutzersuchvorgänge in der Active Directory-Domäne fehl. Das Benutzerkonto muss über Nur-Lesen-Zugriff auf die Organisationseinheit (OU) „Benutzer und Gruppe“ verfügen und in der Lage sein, Benutzer- und Gruppenattribute zu lesen. Dies ist die Standardkonfiguration der Active Directory-Domäne für Authentifizierungsberechtigungen. VMware empfiehlt die Verwendung eines speziellen Dienstbenutzers.

- 5 Wenn Sie Active Directory als einen LDAP-Server oder als eine OpenLDAP-Identitätsquelle konfigurieren, klicken Sie auf **Testverbindung**, um sicherzustellen, dass Sie eine Verbindung mit der Identitätsquelle herstellen können.
- 6 Klicken Sie auf **OK**.

Nächste Schritte

Wenn eine Identitätsquelle hinzugefügt wird, können alle Benutzer authentifiziert werden, verfügen aber über die Rolle **Kein Zugriff**. Ein Benutzer mit dem vCenter Server-Recht **Berechtigung ändern** kann Benutzern oder Benutzergruppen Rechte zuweisen, damit sie sich bei vCenter Server anmelden und Objekte anzeigen und verwalten können. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

Einstellungen der Active Directory-Identitätsquelle

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

Voraussetzungen für die Verwendung einer Active Directory-Identitätsquelle

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

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

Hinweis Active Directory (integrierte Windows-Authentifizierung) verwendet immer der Stamm der Active Directory-Domänengestamtstruktur. Informationen zur Konfiguration Ihrer Identitätsquelle für die integrierte Windows-Authentifizierung mit einer untergeordneten Domäne in Ihrer Active Directory-Gesamtstruktur finden Sie im VMware-Knowledgebase-Artikel [2070433](#).

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

Hinweis In vSphere 5.5 verwendet vCenter Single Sign On das Maschinenkonto, selbst wenn Sie den SPN angeben. Weitere Informationen hierzu finden Sie im VMware-Knowledgebase-Artikel [2087978](#).

Tabelle 2-5. Hinzufügen von Einstellungen der Identitätsquelle

Textfeld	Beschreibung
Domänenname	FQDN des Domänennamens, zum Beispiel „mydomain.com“. Geben Sie keine IP-Adresse an. Dieser Domänenname muss durch das vCenter Server-System per DNS auflösbar sein. Wenn Sie eine vCenter Server Appliance nutzen, verwenden Sie die Informationen zum Konfigurieren der Netzwerkeinstellungen, um die DNS-Servereinstellungen zu aktualisieren.
Maschinenkonto verwenden	Wählen Sie diese Option aus, um das Konto der lokalen Maschine als SPN zu verwenden. Mit dieser Option geben Sie nur den Domänennamen an. Verwenden Sie diese Option nicht, wenn Sie diese Maschine voraussichtlich umbenennen werden.

Tabelle 2-5. Hinzufügen von Einstellungen der Identitätsquelle (Fortsetzung)

Textfeld	Beschreibung
SPN (Dienstprinzipalname) verwenden	Wählen Sie diese Option aus, wenn Sie die lokale Maschine voraussichtlich umbenennen werden. Sie müssen einen SPN, einen Benutzer, der sich mit der Identitätsquelle authentifizieren kann, und ein Kennwort für den Benutzer angeben.
SPN (Dienstprinzipalname)	Der SPN, mit dem Kerberos den Active Directory-Dienst identifiziert. Schließen Sie die Domäne in den Namen ein. Beispiel: „STS/example.com“. Der SPN muss innerhalb der Domäne eindeutig sein. Durch Ausführen von <code>setspn -S</code> wird sichergestellt, dass keine Duplikate erstellt werden. Weitere Informationen zu <code>setspn</code> finden Sie in der Microsoft-Dokumentation.
UPN (Benutzerprinzipalname) Kennwort	Der Name und das Kennwort eines Benutzers, der sich mit dieser Identitätsquelle authentifizieren kann. Verwenden Sie beispielsweise folgendes E-Mail-Adressformat: „ jchin@mydomain.com“. Den Benutzerprinzipalnamen können Sie mit dem Active Directory-Dienstschnittstellen-Editor (ADSI Edit) überprüfen.

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

Das Active Directory als Identitätsquelle für LDAP-Server ist zur Abwärtskompatibilität verfügbar. Verwenden Sie die Active Directory-Option (Integrierte Windows-Authentifizierung) für ein Setup, für das weniger Eingaben erforderlich sind. Die Identitätsquelle für den OpenLDAP-Server ist für Umgebungen verfügbar, die OpenLDAP verwenden.

Wenn Sie eine OpenLDAP-Identitätsquelle konfigurieren, finden Sie weitere Anforderungen im VMware-Knowledgebase-Artikel [2064977](#).

Tabelle 2-6. Active Directory als LDAP-Server und OpenLDAP-Einstellungen

Feld	Beschreibung
Name	Name der Identitätsquelle
Basis-DN für Benutzer	Basis-DN (Distinguished Name) für Benutzer.
Domänenname	FQDN der Domäne, zum Beispiel example.com. Geben Sie in diesem Feld keine IP-Adresse an.
Domänen-Alias	Für Active Directory-Identitätsquellen, der NetBIOS-Name der Domäne. Fügen Sie den NetBIOS-Namen der Active Directory-Domäne wie Alias der Identitätsquelle hinzu, wenn Sie SSPI-Authentifizierungen verwenden. Für OpenLDAP-Identitätsquellen wird der Domänenname in Großbuchstaben hinzugefügt, wenn Sie keinen Alias angeben.
Basis-DN für Gruppen	Der Basis-DN (Distinguished Name) für Gruppen.

Tabelle 2-6. Active Directory als LDAP-Server und OpenLDAP-Einstellungen (Fortsetzung)

Feld	Beschreibung
URL des primären Servers	LDAP-Server des primären Domänencontrollers für die Domäne. Verwenden Sie das Format ldap://hostname: port oder ldaps://hostname:port. Der Port ist in der Regel 389 für ldap: Verbindungen und 636 für ldaps: Verbindungen. Für Active Directory-Bereitstellungen über mehrere Domänencontroller ist der Port in der Regel 3268 für ldap: Verbindungen und 3269 für ldaps: Verbindungen. Ein Zertifikat, das das Vertrauen für den LDAPS-Endpunkt des Active Directory-Servers festlegt, ist erforderlich, wenn Sie ldaps:// in der primären oder sekundären LDAP-URL verwenden.
URL des sekundären Servers	Adresse eines LDAP-Servers des sekundären Domänencontrollers, der für das Failover verwendet wird.
Auswählen eines Zertifikats	Um LDAPS mit Ihrem Active Directory-LDAP-Server oder -OpenLDAP-Server verwenden zu können, wird eine Auswahl Schaltfläche angezeigt, nachdem Sie ldaps:// in das URL-Feld eingegeben haben. Eine sekundäre URL ist nicht erforderlich.
Benutzername	ID eines Benutzers in der Domäne, der über einen minimalen Base-DN-Zugriff (nur Lesen) für Benutzer und Gruppen verfügt
Kennwort	Kennwort des Benutzers, der vom Benutzernamen angegeben wird

Bearbeiten einer vCenter Single Sign On-Identitätsquelle

vSphere-Benutzer werden in einer Identitätsquelle definiert. Sie können die Details einer Identitätsquelle bearbeiten, die vCenter Single Sign On zugewiesen ist.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client als „administrator@vsphere.local“ oder als anderer Benutzer mit vCenter Single Sign On-Administratorrechten an.
Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Navigieren Sie zu **Verwaltung > Single Sign On > Konfiguration**.
- 3 Klicken Sie auf die Registerkarte **Identitätsquellen**.
- 4 Klicken Sie mit der rechten Maustaste auf die Identitätsquelle in der Tabelle und wählen Sie **Identitätsquelle bearbeiten**.

- 5 Bearbeiten Sie die Einstellungen für die Identitätsquelle. Die verfügbaren Optionen hängen vom Typ der ausgewählten Identitätsquelle ab.

Option	Beschreibung
Active Directory (Integrierte Windows-Authentifizierung)	Verwenden Sie diese Option für native Active Directory-Implementierungen. Die Maschine, auf der der vCenter Single Sign On-Dienst ausgeführt wird, muss sich in einer Active Directory-Domäne befinden, wenn Sie diese Option verwenden möchten. Weitere Informationen hierzu finden Sie unter Einstellungen der Active Directory-Identitätsquelle .
Active Directory als ein LDAP-Server	Diese Option ist verfügbar, um die Abwärtskompatibilität zu gewährleisten. Sie setzt voraus, dass Sie den Domänencontroller und andere Informationen angeben. Weitere Informationen hierzu finden Sie unter Einstellungen der Active Directory-Identitätsquelle für LDAP-Server und OpenLDAP-Server .
OpenLDAP	Verwenden Sie diese Option für eine OpenLDAP-Identitätsquelle. Weitere Informationen hierzu finden Sie unter Einstellungen der Active Directory-Identitätsquelle für LDAP-Server und OpenLDAP-Server .
LocalOS	Verwenden Sie diese Option, um das lokale Betriebssystem als Identitätsquelle hinzuzufügen. Sie müssen nur den Namen des lokalen Betriebssystems angeben. Bei Auswahl dieser Option werden alle Benutzer der angegebenen Maschine von vCenter Single Sign On erkannt, auch wenn diese Benutzer nicht zu einer anderen Domäne gehören.

- 6 Klicken Sie auf **Testverbindung**, um sicherzustellen, dass Sie eine Verbindung zur Identitätsquelle herstellen können.
- 7 Klicken Sie auf **OK**.

Entfernen einer vCenter Single Sign On-Identitätsquelle

vSphere-Benutzer werden in einer Identitätsquelle definiert. Sie können eine Identitätsquelle aus der Liste der registrierten Identitätsquellen entfernen.

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Navigieren Sie zu **Verwaltung > Single Sign On > Konfiguration**.
- 3 Wählen Sie auf der Registerkarte **Identitätsquellen** eine Identitätsquelle aus und klicken Sie auf das Symbol **Identitätsquelle löschen**.
- 4 Klicken Sie auf **Ja**, wenn Sie zur Bestätigung aufgefordert werden.

Verwenden von vCenter Single Sign On mit Windows-Sitzungsauthentifizierung

Sie können vCenter Single Sign On mit der Windows-Sitzungsauthentifizierung (SSPI) verwenden. Um das Kontrollkästchen auf der Anmeldeseite verfügbar zu machen, muss das Client-Integrations-Plug-In installiert werden.

Die Verwendung von SSPI beschleunigt die Anmeldung des Benutzers, der aktuell bei der Maschine angemeldet ist.

Voraussetzungen

Ihre Windows-Domäne muss ordnungsgemäß eingerichtet sein. Weitere Informationen hierzu finden Sie im VMware-Knowledgebase-Artikel [2064250](#).

Verfahren

- 1 Navigieren Sie zur vSphere Web Client-Anmeldeseite.
- 2 Wenn das Kontrollkästchen **Windows-Sitzungsauthentifizierung verwenden** nicht verfügbar ist, klicken Sie im unteren Bereich der Anmeldeseite auf **Client-Integrations-Plug-In herunterladen**.

- 3 Falls der Browser die Installation durch Zertifikatfehler oder durch Ausführen eines Popup-Blockers blockiert, finden Sie in der Hilfe des Browsers Anweisungen zum Beheben des Problems.

- 4 Schließen Sie andere Browser, wenn Sie dazu aufgefordert werden.

Nach der Installation ist das Plug-In für alle Browser verfügbar. Wenn das Plug-In vom Browser benötigt wird, müssen Sie es möglicherweise für einzelne Sitzungen oder für alle Sitzungen zulassen.

- 5 Beenden Sie Ihren Browser und starten Sie ihn neu.

Nach dem Neustart können Sie das Kontrollkästchen **Windows-Sitzungsauthentifizierung verwenden** auswählen.

Zwei-Faktor-Authentifizierung vCenter Server

Mit vCenter Single Sign-On können Sie sich mit dem Namen und Kennwort eines Benutzers bei einer Identitätsquelle authentifizieren, die vCenter Single Sign-On bekannt ist, oder mit der Windows-Sitzungsauthentifizierung bei Active Directory-Identitätsquellen. Ab vSphere 6.0 Update 2 können Sie sich zudem mithilfe einer Smartcard (UPN-basierte allgemeine Zugriffskarte oder CAC) oder mithilfe eines RSA SecurID-Tokens authentifizieren.

Zwei-Faktor-Authentifizierungsmethoden

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

Authentifizierung mit einer allgemeinen Zugriffskarte (CAC-Authentifizierung)

Mit der CAC-Authentifizierung erhalten nur die Benutzer Zugriff, die eine physische Karte an das USB-Laufwerk des Computers anschließen, bei dem sie sich anmelden. Wenn die PKI so bereitgestellt wurde, dass die Smartcard-Zertifikate die einzigen durch die Zertifizierungsstelle ausgegebenen Client-Zertifikate sind, werden dem Benutzer nur Smartcard-Zertifikate angezeigt. Der Benutzer wählt ein Zertifikat aus und wird anschließend zur Eingabe der PIN aufgefordert. Es können sich nur diejenigen Benutzer anmelden, die sowohl über eine physische Karte als auch über die mit dem Zertifikat übereinstimmende PIN verfügen.

RSA SecurID-Authentifizierung

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

Hinweis vCenter Single Sign-On unterstützt nur die native SecurID-Authentifizierung, jedoch nicht die RADIUS-Authentifizierung.

Angeben einer nicht standardmäßigen Authentifizierungsmethode

Administratoren können die Einrichtung über die Platform Services Controller-Webschnittstelle durchführen oder aber mithilfe des Skripts `sso-config` (`sso-config.bat` auf Windows und `sso-config.sh` auf der Appliance).

- Bei der Authentifizierung mit einer allgemeinen Zugriffskarte richten Sie Ihren Webbrowser mithilfe des Skripts `sso-config` ein, und Sie können vCenter Single Sign-On über die Platform Services Controller-Webschnittstelle oder mithilfe von `sso-config` einrichten. Das Setup umfasst das Aktivieren der CAC-Authentifizierung, das Konfigurieren der Zertifikatswiderrufsrichtlinie und das Einrichten eines Anmelde-Banners.
- Bei RSA SecureID verwenden Sie das Skript `sso-config`, um RSA Authentication Manager für die Domäne zu konfigurieren und die RSA-Tokenauthentifizierung zu aktivieren. Die Authentifizierungsmethode wird in der Platform Services Controller-Webschnittstelle angezeigt (sofern aktiviert), aber die RSA SecureID-Authentifizierung kann nicht über die Webschnittstelle konfiguriert werden.

Kombinieren unterschiedlicher Authentifizierungsmethoden

Mithilfe von `sso-config` können Sie jede Authentifizierungsmethode separat aktivieren bzw. deaktivieren. Es kann beispielsweise sinnvoll sein, die Benutzernamen- und Kennwort-Authentifizierung aktiviert zu lassen, wenn Sie eine der Zwei-Faktor-Authentifizierungsmethoden testen, und dabei nur eine Authentifizierungsmethode als aktiviert festzulegen.

Konfigurieren der Smartcard-Authentifizierung für vCenter Single Sign-On

Sie können Ihre Umgebung so einstellen, dass die Smartcard-Authentifizierung erforderlich ist, wenn ein Benutzer eine Verbindung zu einem vCenter Server oder verknüpften Platform Services Controller des vSphere Web Client herstellt.

Anmeldung mit der Smartcard-Authentifizierung

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

Wenn Sie die Smartcard-Authentifizierung für vCenter Single Sign-On konfigurieren, werden Benutzer, die sich bei einem vCenter Server- oder Platform Services Controller-System anmelden, dazu aufgefordert, sich mithilfe einer Smartcard und einer PIN-Kombination wie folgt zu authentifizieren:

- 1 Wenn der Benutzer die Smartcard in ein Smartcard-Lesegerät einschiebt, liest vCenter Single Sign-On die Zertifikate auf der Karte.
- 2 vCenter Single Sign-On fordert den Benutzer zur Auswahl eines Zertifikats und anschließend zur Eingabe der PIN für dieses Zertifikat auf.
- 3 vCenter Single Sign-On überprüft, ob das Zertifikat auf der Smartcard bekannt und die PIN korrekt ist. Wenn die Überprüfung des Widerrufs eingeschaltet ist, überprüft vCenter Single Sign-On auch, ob das Zertifikat widerrufen wurde.
- 4 Wenn das Zertifikat bekannt ist und es sich nicht um ein widerrufenes Zertifikat handelt, wird der Benutzer authentifiziert und kann anschließend Aufgaben ausführen, über deren Berechtigungen er verfügt.

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

Konfigurieren der Smartcard-Authentifizierung über die Befehlszeile

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

Wenn Sie die Smartcard-Authentifizierung über die Befehlszeile konfigurieren, richten Sie immer zuerst den Platform Services Controller mit dem Befehl `sso-config` ein. Sie können dann andere Aufgaben über die Platform Services Controller-Webschnittstelle durchführen.

- 1 Konfigurieren Sie den Platform Services Controller so, dass der Webbrowser die Übermittlung des Smartcard-Zertifikats anfordert, wenn der Benutzer sich anmeldet.
- 2 Konfigurieren Sie die Authentifizierungsrichtlinie. Sie können die Richtlinie mit dem Skript `sso-config` oder über die Platform Services Controller-Webschnittstelle konfigurieren. Die Konfiguration von unterstützten Authentifizierungstypen und Widerrufseinstellungen wird in VMware Directory Service gespeichert und über alle Platform Services Controller-Instanzen einer vCenter Single Sign-On-Domäne hinweg repliziert.

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

Wenn das Anmelden über den vSphere Web Client nicht funktioniert und die Benutzernamen- und Kennwort-Authentifizierung deaktiviert ist, kann ein Root- oder Administratorbenutzer die Benutzernamen- und Kennwort-Authentifizierung über die Platform Services Controller-Befehlszeile wieder aktivieren, indem er den folgenden Befehl ausführt: Das Beispiel ist für Windows. Verwenden Sie für Linux `sso-config.sh`.

```
sso-config.bat -set_authn_policy -pwdAuthn true
```

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

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

Voraussetzungen

- Stellen Sie sicher, dass Ihre Umgebung Platform Services Controller Version 6.0 Update 2 oder höher verwendet und Sie vCenter Server Version 6.0 oder höher verwenden. Führen Sie bei Knoten der Version 5.5 ein Upgrade auf Version 6.0 durch.
- Stellen Sie sicher, dass in Ihrer Umgebung ein Unternehmens-PKI-Schlüssel (Public Key Infrastructure) eingerichtet ist und die Zertifikate die folgenden Anforderungen erfüllen:
 - Ein Benutzerprinzipalname (User Principal Name, UPN), der einem Active Directory-Konto in der Erweiterung „Alternativname für Betreff“ (SAN) entspricht.
 - Die Client-Authentifizierung muss im Feld „Anwendungsrichtlinie“ oder „Erweiterte Schlüsselnutzung“ eines Zertifikats angegeben werden, da dieses Zertifikat andernfalls im Browser nicht angezeigt wird.

- Stellen Sie sicher, dass das Zertifikat der Platform Services Controller-Webschnittstelle für die Workstation des Endbenutzers vertrauenswürdig ist, da der Browser andernfalls keinen Versuch zur Authentifizierung unternimmt.
- Konfigurieren Sie eine Active Directory-Identitätsquelle und fügen Sie diese zu vCenter Single Sign-On als Identitätsquelle hinzu.
- Weisen Sie die vCenter Server-Administratorrolle einem oder mehreren Benutzern in der Active Directory-Identitätsquelle zu. Diese Benutzer können sich dann authentifizieren, da sie sich in der Active Directory-Gruppe befinden, und sie verfügen über vCenter Server-Administratorrechte. Der Benutzer „administrator@vsphere.local“ kann keine Smartcard-Authentifizierung ausführen.
- Wenn Ihre Umgebung über die Platform Services Controller-HA-Lösung verfügen soll, schließen Sie die gesamte HA-Konfiguration ab, bevor Sie die Smartcard-Authentifizierung einrichten. Weitere Informationen finden Sie im VMware Knowledge Base Artikel [2112085](#) (Windows) oder [2113315](#) (vCenter Server Appliance).

Verfahren

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

Option	Beschreibung
Windows	Melden Sie sich bei der Platform Services Controller-Windows-Installation an und verwenden Sie WinSCP oder ein ähnliches Dienstprogramm, um die Dateien zu kopieren.
Appliance	<ol style="list-style-type: none"> a Melden Sie sich bei der Appliance-Konsole entweder direkt oder mithilfe von SSH an. b Aktivieren Sie die Appliance-Shell wie folgt: <pre> shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root </pre> c Kopieren Sie die Zertifikate mithilfe von WinSCP oder einem ähnlichen Dienstprogramm in das Verzeichnis <code>/usr/lib/vmware-sso/vmware-sts/conf</code> auf dem Platform Services Controller. d Optional können Sie die Appliance-Shell wie folgt deaktivieren: <pre> chsh -s "bin/appliancesh" root </pre>

- 2 Konfigurieren Sie auf jedem Platform Services Controller-Knoten die Einstellungen der Smartcard-Authentifizierung unter Verwendung der `sso-config-CLI`.
 - a Navigieren Sie zu dem Verzeichnis, in dem sich das `sso-config`-Skript befindet.

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

- b Führen Sie den folgenden Befehl aus:

```
sso-config.[bat|sh] -set_tc_cert_authn -switch true -cacerts
[FirstTrustedCA.cer,SecondTrustedCA.cer,...] -t tenant
```

Beispiel:

```
sso-config.bat -set_tc_cert_authn -switch true -cacerts MySmartCA1.cer -t vsphere.local
```

- c Starten Sie die virtuelle bzw. physische Maschine neu.

```
service-control --stop vmware-std
service-control --start vmware-std
```

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

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

Beispiel:

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

Wenn Sie mehrere Zertifikate angeben, sind keine Leerzeichen zwischen Zertifikaten zulässig.

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

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

Sie können diese Befehle verwenden, um unterschiedliche Authentifizierungsmethoden je nach Bedarf zu aktivieren und zu deaktivieren.

- 5 (Optional) Führen Sie zum Einrichten einer Positivliste mit Zertifikatsrichtlinien den folgenden Befehl aus:

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

Wenn Sie mehrere Richtlinien angeben möchten, trennen Sie diese durch einen Befehl, z. B.:

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

In der Positivliste sind Objekt-IDs von Richtlinien angegeben, die in der Zertifikatsrichtlinienerweiterung des Zertifikats zulässig sind. Ein X509-Zertifikat kann eine Zertifikatsrichtlinienerweiterung aufweisen.

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

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

Verwenden der Platform Services Controller-Webschnittstelle zum Verwalten der Smartcard-Authentifizierung

Sie können über die Platform Services Controller-Webschnittstelle die Smartcard-Authentifizierung aktivieren und deaktivieren, das Anmelde-Banner anpassen und die Widerrufsrichtlinie einrichten.

Wenn Sie die Smartcard-Authentifizierung über die Befehlszeile konfigurieren, richten Sie immer zuerst den Platform Services Controller mit dem Befehl `sso-config` ein. Sie können dann andere Aufgaben über die Platform Services Controller-Webschnittstelle durchführen.

- 1 Konfigurieren Sie den Platform Services Controller so, dass der Webbrowser die Übermittlung des Smartcard-Zertifikats anfordert, wenn der Benutzer sich anmeldet.
- 2 Konfigurieren Sie die Authentifizierungsrichtlinie. Sie können die Richtlinie mit dem Skript `sso-config` oder über die Platform Services Controller-Webschnittstelle konfigurieren. Die Konfiguration von unterstützten Authentifizierungstypen und Widerrufseinstellungen wird in VMware Directory Service gespeichert und über alle Platform Services Controller-Instanzen einer vCenter Single Sign-On-Domäne hinweg repliziert.

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

Wenn das Anmelden über den vSphere Web Client nicht funktioniert und die Benutzernamen- und Kennwort-Authentifizierung deaktiviert ist, kann ein Root- oder Administratorbenutzer die Benutzernamen- und Kennwort-Authentifizierung über die Platform Services Controller-Befehlszeile wieder aktivieren, indem er den folgenden Befehl ausführt: Das Beispiel ist für Windows. Verwenden Sie für Linux `sso-config.sh`.

```
sso-config.bat -set_authn_policy -pwdAuthn true
```


Voraussetzungen

- Stellen Sie sicher, dass Ihre Umgebung Platform Services Controller Version 6.0 Update 2 oder höher verwendet und Sie vCenter Server Version 6.0 oder höher verwenden. Führen Sie bei Knoten der Version 5.5 ein Upgrade auf Version 6.0 durch.
- Stellen Sie sicher, dass in Ihrer Umgebung ein Unternehmens-PKI-Schlüssel (Public Key Infrastructure) eingerichtet ist und die Zertifikate die folgenden Anforderungen erfüllen:
 - Ein Benutzerprinzipalname (User Principal Name, UPN), der einem Active Directory-Konto in der Erweiterung „Alternativname für Betreff“ (SAN) entspricht.
 - Die Client-Authentifizierung muss im Feld „Anwendungsrichtlinie“ oder „Erweiterte Schlüsselnutzung“ eines Zertifikats angegeben werden, da dieses Zertifikat andernfalls im Browser nicht angezeigt wird.
- Stellen Sie sicher, dass das Zertifikat der Platform Services Controller-Webschnittstelle für die Workstation des Endbenutzers vertrauenswürdig ist, da der Browser andernfalls keinen Versuch zur Authentifizierung unternimmt.
- Konfigurieren Sie eine Active Directory-Identitätsquelle und fügen Sie diese zu vCenter Single Sign-On als Identitätsquelle hinzu.
- Weisen Sie die vCenter Server-Administratorrolle einem oder mehreren Benutzern in der Active Directory-Identitätsquelle zu. Diese Benutzer können sich dann authentifizieren, da sie sich in der Active Directory-Gruppe befinden, und sie verfügen über vCenter Server-Administratorrechte. Der Benutzer „administrator@vsphere.local“ kann keine Smartcard-Authentifizierung ausführen.
- Wenn Ihre Umgebung über die Platform Services Controller-HA-Lösung verfügen soll, schließen Sie die gesamte HA-Konfiguration ab, bevor Sie die Smartcard-Authentifizierung einrichten. Weitere Informationen finden Sie im VMware Knowledge Base Artikel [2112085](#) (Windows) oder [2113315](#) (vCenter Server Appliance).

Verfahren

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

Option	Beschreibung
Windows	Melden Sie sich bei der Platform Services Controller-Windows-Installation an und verwenden Sie WinSCP oder ein ähnliches Dienstprogramm, um die Dateien zu kopieren.
Appliance	<ol style="list-style-type: none"> a Melden Sie sich bei der Appliance-Konsole entweder direkt oder mithilfe von SSH an. b Aktivieren Sie die Appliance-Shell wie folgt: <pre>shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root</pre> c Kopieren Sie die Zertifikate mithilfe von WinSCP oder einem ähnlichen Dienstprogramm in das Verzeichnis <code>/usr/lib/vmware-sso/vmware-sts/conf</code> auf dem Platform Services Controller. d Optional können Sie die Appliance-Shell wie folgt deaktivieren: <pre>chsh -s "bin/appliancesh" root</pre>

- 2 Konfigurieren Sie auf jedem Platform Services Controller-Knoten die Einstellungen der Smartcard-Authentifizierung unter Verwendung der `sso-config-CLI`.

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

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

- b Führen Sie den folgenden Befehl aus:

```
sso-config.[bat|sh] -set_tc_cert_authn -switch true -cacerts
[FirstTrustedCA.cer,SecondTrustedCA.cer,...] -t tenant
```

Beispiel:

```
sso-config.bat -set_tc_cert_authn -switch true -cacerts MySmartCA1.cer,MySmartCA2.cer
-t vsphere.local
```

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

- c Starten Sie die virtuelle bzw. physische Maschine neu.

```
service-control --stop vmware-std
service-control --start vmware-std
```

- 3 Stellen Sie über einen Browser eine Verbindung zum Platform Services Controller her, indem Sie folgende URL eingeben:

`https://psc_hostname_or_IP/psc`

In einer eingebetteten Bereitstellung ist der Hostname oder die IP-Adresse von Platform Services Controller identisch mit dem Hostnamen oder der IP-Adresse von vCenter Server.

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

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

- 5 Navigieren Sie zu **Single Sign-On > Konfiguration**.

- 6 Klicken Sie auf **Smartcard-Konfiguration** und wählen Sie die Registerkarte **Vertrauenswürdige CA-Zertifikate** aus.

- 7 Um ein oder mehrere vertrauenswürdige Zertifikate hinzuzufügen, klicken Sie auf **Zertifikat hinzufügen** und anschließend auf **Durchsuchen**. Wählen Sie dann alle Zertifikate von vertrauenswürdigen Zertifizierungsstellen aus und klicken Sie auf **OK**.

- 8 Klicken Sie zum Festlegen der Authentifizierungskonfiguration neben **Authentifizierungskonfiguration** auf **Bearbeiten** und aktivieren bzw. deaktivieren Sie Authentifizierungsmethoden.

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

Festlegen von Widerrufsrichtlinien für die Smartcard-Authentifizierung

Sie können die Überprüfung des Zertifikatswiderrufs anpassen und angeben, wo vCenter Single Sign-On nach Informationen zu widerrufenen Zertifikaten suchen soll.

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

- Wenn die Überprüfung des Widerrufs deaktiviert ist, ignoriert vCenter Single Sign-On alle Einstellungen für die Zertifikatswiderrufsliste (Certificate Revocation List, CRL) oder das Onlinestatusprotokoll des Zertifikats (Online Certificate Status Protocol, OCSP).
- Wenn die Überprüfung des Widerrufs aktiviert ist, hängt das empfohlene Setup vom PKI-Setup ab.

Nur OCSP

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

Nur CRL

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

OCSP und CRL

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

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

OCSP-URL

vCenter Single Sign-On überprüft standardmäßig den Speicherort des OCSP-Responders, der im validierten Zertifikat definiert ist. Sie können ausdrücklich einen Speicherort angeben, wenn im Zertifikat die Erweiterung „Zugriff auf Stelleninformationen“ nicht vorhanden ist oder Sie diese überschreiben möchten, da sie z. B. in Ihrer Umgebung nicht verfügbar ist.

CRL aus Zertifikat verwenden

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

CRL-Speicherort

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

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

Voraussetzungen

- Stellen Sie sicher, dass Ihre Umgebung Platform Services Controller Version 6.0 Update 2 oder höher verwendet und Sie vCenter Server Version 6.0 oder höher verwenden. Führen Sie bei Knoten der Version 5.5 ein Upgrade auf Version 6.0 durch.
- Stellen Sie sicher, dass in Ihrer Umgebung ein Unternehmens-PKI-Schlüssel (Public Key Infrastructure) eingerichtet ist und die Zertifikate die folgenden Anforderungen erfüllen:
 - Ein Benutzerprinzipalname (User Principal Name, UPN), der einem Active Directory-Konto in der Erweiterung „Alternativname für Betreff“ (SAN) entspricht.
 - Die Client-Authentifizierung muss im Feld „Anwendungsrichtlinie“ oder „Erweiterte Schlüsselnutzung“ eines Zertifikats angegeben werden, da dieses Zertifikat andernfalls im Browser nicht angezeigt wird.
- Stellen Sie sicher, dass das Zertifikat der Platform Services Controller-Webschnittstelle für die Workstation des Endbenutzers vertrauenswürdig ist, da der Browser andernfalls keinen Versuch zur Authentifizierung unternimmt.
- Konfigurieren Sie eine Active Directory-Identitätsquelle und fügen Sie diese zu vCenter Single Sign-On als Identitätsquelle hinzu.
- Weisen Sie die vCenter Server-Administratorrolle einem oder mehreren Benutzern in der Active Directory-Identitätsquelle zu. Diese Benutzer können sich dann authentifizieren, da sie sich in der Active Directory-Gruppe befinden, und sie verfügen über vCenter Server-Administratorrechte. Der Benutzer „administrator@vsphere.local“ kann keine Smartcard-Authentifizierung ausführen.

- Wenn Ihre Umgebung über die HA-Lösung des Platform Services Controller verfügen soll, schließen Sie die gesamte HA-Konfiguration ab, bevor Sie die Smartcard-Authentifizierung einrichten. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel [2113085](#) (Windows) oder [2113315](#) (vCenter Server Appliance).

Verfahren

- 1 Stellen Sie über einen Browser eine Verbindung zum Platform Services Controller her, indem Sie folgende URL eingeben:

`https://psc_hostname_or_IP/psc`

In einer eingebetteten Bereitstellung ist der Hostname oder die IP-Adresse von Platform Services Controller identisch mit dem Hostnamen oder der IP-Adresse von vCenter Server.

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

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

- 3 Navigieren Sie zu **Single Sign-On > Konfiguration**.
- 4 Klicken Sie auf **Einstellungen des Zertifikatswiderrufs** und aktivieren bzw. deaktivieren Sie die Überprüfung des Widerrufs.
- 5 Falls in Ihrer Umgebung Zertifikatsrichtlinien gelten, können Sie im Bereich **Von Zertifikatsrichtlinien akzeptiert** eine Richtlinie hinzufügen.

Einrichten der RSA SecurID-Authentifizierung

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

Informationen finden Sie in den zwei vSphere Blog-Beiträgen über die [RSA SecurID-Einrichtung](#).

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

Voraussetzungen

- Stellen Sie sicher, dass Ihre Umgebung Platform Services Controller Version 6.0 Update 2 oder höher verwendet und Sie vCenter Server Version 6.0 oder höher verwenden. Führen Sie bei Knoten der Version 5.5 ein Upgrade auf Version 6.0 durch.
- Stellen Sie sicher, dass RSA Authentication Manager in Ihrer Umgebung ordnungsgemäß konfiguriert wurde und dass Benutzer über RSA-Token verfügen. RSA Authentication Manager Version 8.0 oder höher ist erforderlich.

- Stellen Sie sicher, dass die von RSA Manager verwendete Identitätsquelle zu vCenter Single Sign-On hinzugefügt wurde. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer vCenter Single Sign On-Identitätsquelle](#).
- Stellen Sie sicher, dass das RSA Authentication Manager-System den Platform Services Controller-Hostnamen auflösen kann und dass das Platform Services Controller-System den RSA Authentication Manager-Hostnamen auflösen kann.
- Exportieren Sie die Datei `sdconf.rec` aus dem RSA Manager, indem Sie **Zugriff > Authentifizierungsagenten > Konfigurationsdatei generieren** auswählen. Dekomprimieren Sie die resultierende Datei `AM_Config.zip` und suchen Sie nach der Datei `sdconf.rec`.
- Kopieren Sie die Datei `sdconf.rec` in den Platform Services Controller-Knoten.

Verfahren

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

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

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

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

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

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

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

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

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

Beispiel:

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

Sie können die folgenden Optionen angeben.

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

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

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

Die Standardwerte sind normalerweise angemessen, z.B.:

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

- 6 (Optional) Wenn Ihre Identitätsquelle nicht den Benutzerprinzipalname als Benutzer-ID verwendet, konfigurieren Sie die Identitätsquelle als userID-Attribut.

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

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

Beispiel:

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

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

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

Ergebnisse

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

Verwalten des Anmelde-Banners

Ab vSphere 6.0 Update 2 können Sie ein Anmelde-Banner in Ihre Umgebung einfügen. Sie können einen Text anzeigen oder fordern, dass Benutzer auf ein Kontrollkästchen klicken müssen, um beispielsweise anzugeben, dass sie die Nutzungsbedingungen akzeptieren. Sie können das Anmelde-Banner aktivieren und deaktivieren sowie fordern, dass Benutzer für die ausdrückliche Zustimmung auf ein Kontrollkästchen klicken müssen.

Verfahren

- 1 Stellen Sie über einen Browser eine Verbindung zum Platform Services Controller her, indem Sie folgende URL eingeben:

`https://psc_hostname_or_IP/psc`

In einer eingebetteten Bereitstellung ist der Hostname oder die IP-Adresse von Platform Services Controller identisch mit dem Hostnamen oder der IP-Adresse von vCenter Server.

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

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

- 3 Wählen Sie unter „Single Sign-On“ die Option **Konfiguration** aus und klicken Sie auf die Registerkarte **Anmelde-Banner**.
- 4 Klicken Sie auf **Bearbeiten** und konfigurieren Sie das Anmelde-Banner.

Option	Beschreibung
Status	Klicken Sie auf das Kontrollkästchen Aktiviert , um das Anmelde-Banner zu aktivieren. Sie können die anderen Felder nur dann ändern, wenn Sie auf dieses Kontrollkästchen klicken.
Ausdrückliche Zustimmung	Klicken Sie auf das Kontrollkästchen Ausdrückliche Zustimmung , damit Benutzer auf ein Kontrollkästchen klicken müssen, bevor sie sich anmelden können. Sie können auch eine Meldung ohne Kontrollkästchen anzeigen.
Titel	Titel des Banners. Standardmäßig lautet der Text des Anmelde-Banners I agree to the. Sie können dazu z. B. Terms and Conditions hinzufügen.
Meldung	Meldung, die Benutzern beim Klicken auf das Banner angezeigt wird. Beispiel: Der Text der Nutzungsbedingungen. Diese Meldung ist erforderlich, wenn Sie die ausdrückliche Zustimmung verwenden.

Verwenden von vCenter Single Sign On als Identitätsanbieter für andere Identitätsanbieter

Der vSphere Web Client wird bei vCenter Single Sign-On automatisch als vertrauenswürdiger SAML 2.0-Dienstanbieter (SP) registriert. Sie können der Identity Federation weitere vertrauenswürdige Dienstanbieter hinzufügen, wobei vCenter Single Sign-On als SAML-Identitätsprovider (IDP) fungiert. Die Dienstanbieter müssen dem SAML 2.0-Protokoll

entsprechen. Nachdem die Federation eingerichtet wurde, gewährt der Dienstanbieter einem Benutzer Zugriff, wenn dieser sich bei vCenter Single Sign On identifizieren kann.

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

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

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

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

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

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

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

Hinzufügen eines SAML-Dienstanbieters

Sie fügen einen SAML-Dienstanbieter zu vCenter Single Sign On hinzu und fügen vCenter Single Sign On als Identitätsanbieter zu diesem Dienst hinzu. Anschließend authentifiziert der Dienstanbieter Benutzer mit vCenter Single Sign On, wenn diese sich beim Dienstanbieter anmelden.

Verwenden Sie diesen Vorgang, wenn Sie die Single Sign-On-Lösung integrieren möchten, die in VMware vRealize Automation 7.0 und höher sowie später im vCenter Single Sign On-Identitätsanbieter enthalten ist, oder wenn Sie mit einem anderen externen SAML-Dienstanbieter arbeiten.

Der Vorgang umfasst den Import der Metadaten aus Ihrem SAML-Dienstanbieter in vCenter Single Sign On und umgekehrt den Import der Metadaten von vCenter Single Sign On in Ihren SAML-Dienstanbieter, damit die beiden Anbieter gemeinsam über alle Daten verfügen.

Voraussetzungen

Der Zieldienst muss den Standard von SAML 2.0 vollständig unterstützen.

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

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

Sie können derzeit keine Metadaten von SAML-Identitätsanbietern aus dem vSphere Web Client importieren.

Verfahren

- 1 Exportieren Sie die Metadaten aus Ihrem Dienstanbieter in eine Datei.
- 2 Importieren Sie die Metadaten des Dienstanbieters in vCenter Single Sign On.
 - a Melden Sie sich beim vSphere Web Client als „administrator@vsphere.local“ oder als anderer Benutzer mit vCenter Single Sign On-Administratorrechten an.

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
 - b Navigieren Sie zu **Single Sign-On > Konfiguration**.
 - c Gehen Sie zur Registerkarte **SAML-Dienstanbieter**.
 - d Klicken Sie im Feld **Metadaten Ihres SAML-Dienstanbieters** auf **Importieren** und fügen Sie die XML-Zeichenfolgen in das Dialogfeld ein, oder klicken Sie zum Importieren einer Datei auf **Aus Datei importieren** und anschließend auf **Importieren**.
- 3 Exportieren Sie die Metadaten von vCenter Single Sign On.
 - a Klicken Sie im Feld **Metadaten Ihres SAML-Dienstanbieters** auf **Herunterladen**.
 - b Geben Sie einen Speicherort an.
- 4 Wechseln Sie zum SAML-Dienstanbieter, z. B. VMware vRealize Automation 7.0 oder später, und befolgen Sie die Anweisungen für Ihren SAML-Dienstanbieter, um die vCenter Single Sign On-Metadaten zu diesem Dienstanbieter hinzuzufügen.

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

Security Token Service STS

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

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

Benutzer

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

Anwendungsb Benutzer

Gültiges Zertifikat.

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

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

Generieren eines neuen STS-Signaturzertifikats auf der Appliance

Wenn Sie das Standard-Security Token Service (STS)-Serverzertifikat von vCenter Single Sign-On ersetzen möchten, müssen Sie ein neues Zertifikat generieren und dem Java Keystore hinzufügen. In diesem Thema werden die Schritte auf einer eingebetteten Bereitstellungs-Appliance oder einer externen Platform Services Controller-Appliance erläutert.

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

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

Verfahren

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

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

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

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

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

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

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

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

- Generieren Sie den Schlüssel.

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

- Generieren Sie das Zertifikat.

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

- Konvertieren Sie das Zertifikat in das PK12-Format.

```
openssl pkcs12 -export -in /root/newsts/newsts.cer -inkey /root/newsts/sts.key -certfile /etc/vmware-ss0/keys/ssoserverRoot.crt -name "newstssigning" -passout pass:changeme -out newsts.p12
```

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

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

/usr/java/jre-vmware/bin/keytool -v -importcert -keystore root-trust.jks -deststoretype JKS -storepass testpassword -keypass testpassword -file /etc/vmware-ss0/keys/ssoserverRoot.crt -alias root-ca
```

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

Nächste Schritte

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

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

Wenn Sie das standardmäßige STS-Signaturzertifikat ersetzen möchten, müssen Sie zuerst ein neues Zertifikat generieren und zum Java Keystore hinzufügen. In diesem Verfahren werden die Schritte in einer Windows-Installation beschrieben.

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

Wenn Sie eine virtuelle Appliance verwenden, ziehen Sie [Generieren eines neuen STS-Signaturzertifikats auf der Appliance](#) zurate.

Verfahren

- 1 Erstellen Sie ein neues Verzeichnis zum Speichern des neuen Zertifikats.

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

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

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

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

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

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

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

- 4 Generieren Sie den Schlüssel.

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

5 Generieren Sie das Zertifikat.

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

6 Konvertieren Sie das Zertifikat in das PK12-Format.

```
"C:\Program Files\VMware\VCenter Server\openssl\openssl.exe" pkcs12 -export -in newsts.cer -inkey sts.key -certfile ..\ssoserverRoot.crt -name "newstssigning" -passout pass:changeme -out newsts.p12
```

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

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

Nächste Schritte

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

Aktualisieren des Zertifikats für den Security Token Service

Der vCenter Single Sign On-Server enthält einen Security Token Service (STS). Der Security Token Service ist ein Webservice, der Sicherheitstoken ausstellt, validiert und erneuert. Sie können das vorhandene Zertifikat für den Security Token Service manuell im vSphere Web Client aktualisieren, wenn es abläuft oder geändert wird.

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

Lösungsbenuutzer

Gültiges Zertifikat

Andere Benutzer

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

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

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

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

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

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

Voraussetzungen

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

Platform Services Controller-Appliance

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

Beispiel:

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

Windows-Installation

Zertifikatspeicherort\root-trust.jks

Beispiel:

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

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.

- 2 Wählen Sie die Registerkarte **Zertifikate** und die Unterregisterkarte **STS-Signierung** und klicken Sie auf das Symbol **STS-Signaturzertifikat hinzufügen**.

- 3 Fügen Sie das Zertifikat hinzu.

- a Klicken Sie auf **Durchsuchen**, um zur Keystore-Datei (JKS) zu navigieren, die das neue Zertifikat enthält, und klicken Sie auf **Öffnen**.
- b Geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.
- c Klicken Sie ganz oben in die STS-Alias-Kette und dann auf **OK**.
- d Geben Sie das Kennwort erneut ein, wenn Sie dazu aufgefordert werden.

- 4 Klicken Sie auf **OK**.
- 5 Starten Sie den Platform Services Controller-Knoten neu, damit der STS-Dienst und vSphere Web Client neu gestartet werden.

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

Ermitteln des Ablaufdatums eines LDAPS-SSL-Zertifikats

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

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

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Navigieren Sie zu **Verwaltung > Single Sign On > Konfiguration**.
- 3 Klicken Sie auf die Registerkarte **Zertifikate** und dann auf die Unterregisterkarte **Identitätsquellen-TrustStore**.
- 4 Suchen Sie nach dem Zertifikat und verifizieren Sie das Ablaufdatum im Textfeld **Gültig bis**.

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

Verwalten der vCenter Single Sign On-Richtlinien

vCenter Single Sign On-Richtlinien erzwingen die Sicherheitsregeln in Ihrer Umgebung. Die standardmäßigen Kennwörter, Sperrrichtlinien und Token-Richtlinien von vCenter Single Sign On können Sie anzeigen und bearbeiten.

Bearbeiten der vCenter Single Sign On-Kennwortrichtlinie

Die vCenter Single Sign On-Kennwortrichtlinie ist ein Satz von Regeln und Beschränkungen für das Format und den Ablauf von vCenter Single Sign On-Benutzerkennwörtern. Die Kennwortrichtlinie gilt nur für Benutzer in der vCenter Single Sign On-Domäne (vsphere.local).

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

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.

- 2 Navigieren Sie zu **Verwaltung > Single Sign-On > Konfiguration**.
- 3 Klicken Sie auf die Registerkarte **Richtlinien** und wählen Sie **Kennwortrichtlinien**.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Bearbeiten Sie Richtlinienparameter für das Kennwort.

Option	Beschreibung
Beschreibung	Beschreibung der Kennwortrichtlinie.
Maximale Lebensdauer	Maximale Gültigkeitsdauer in Tagen für ein Kennwort, bevor der Benutzer es ändern muss.
Wiederverwendung einschränken	Anzahl der vorhergehenden Kennwörter, die der Benutzer nicht auswählen kann. Beispiel: Falls ein Benutzer eines der letzten sechs Kennwörter nicht wiederverwenden darf, geben Sie „6“ ein.
Maximallänge	Maximal zulässige Zeichenanzahl für das Kennwort.
Mindestlänge	Mindestens erforderliche Zeichenanzahl für das Kennwort. Die Mindestlänge darf nicht unter der Summe der erforderlichen Mindestanzahl von alphabetischen und numerischen Zeichen sowie Sonderzeichen liegen.
Zeichenanforderungen	<p>Mindestens erforderliche Anzahl verschiedener Zeichenarten für das Kennwort. Die Anzahl der verschiedenen Zeichenarten können Sie wie folgt angeben:</p> <ul style="list-style-type: none"> ■ Sonderzeichen: & # % ■ Buchstaben: A b c D ■ Großbuchstaben: A B C ■ Kleinbuchstaben: a b c ■ Zahlen: 1 2 3 <p>Die Mindestanzahl alphabetischer Zeichen muss mindestens der Summe der Anforderungen für Groß- und Kleinbuchstaben entsprechen.</p> <p>In vSphere 6.0 und höher werden Nicht-ASCII-Zeichen in Kennwörtern unterstützt. In älteren Versionen von vCenter Single Sign On existieren Beschränkungen in Bezug auf unterstützte Zeichen.</p>
Identische benachbarte Zeichen	Maximal zulässige Anzahl identischer benachbarter Zeichen für das Kennwort. Die Zahl muss größer als 0 sein. Wenn Sie beispielsweise 1 eingeben, ist das folgende Kennwort nicht zulässig: p@\$\$.word.

- 6 Klicken Sie auf **OK**.

Bearbeiten der vCenter Single Sign On-Sperrrichtlinie

Eine vCenter Single Sign On-Sperrrichtlinie legt die Bedingungen fest, unter denen ein vCenter Single Sign On-Benutzerkonto gesperrt wird, wenn ein Benutzer versucht, sich mit falschen Anmeldedaten anzumelden. Sie können die Sperrrichtlinie bearbeiten.

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

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

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Navigieren Sie zu **Verwaltung > Single Sign On > Konfiguration**.
- 3 Klicken Sie auf die Registerkarte **Richtlinien** und wählen Sie **Sperrrichtlinie** aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Bearbeiten Sie die Parameter.

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

- 6 Klicken Sie auf **OK**.

Bearbeiten der vCenter Single Sign On-Token-Richtlinie

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

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie **Verwaltung > Single Sign On** und danach **Konfiguration**.
- 3 Klicken Sie auf die Registerkarte **Richtlinien** und wählen Sie **Token-Richtlinie**.

Der vSphere Web Client zeigt die aktuellen Konfigurationseinstellungen an. Wenn Sie die Standardeinstellungen nicht geändert haben, verwendet vCenter Single Sign On diese Einstellungen.

- 4 Bearbeiten Sie die Konfigurationsparameter der Token-Richtlinie.

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

- 5 Klicken Sie auf **OK**.

Verwalten von vCenter Single Sign On-Benutzern und -Gruppen

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

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

- **Hinzufügen von vCenter Single Sign On-Benutzern**

Benutzer, die im vSphere Web Client auf der Registerkarte **Benutzer** aufgeführt sind, sind aus der Perspektive von vCenter Single Sign On interne Benutzer und gehören zur Domäne „vsphere.local“.

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

Wenn ein vCenter Single Sign On-Benutzerkonto deaktiviert ist, kann sich der Benutzer beim vCenter Single Sign On-Server nur anmelden, wenn das Konto von einem Administrator aktiviert wird. Sie können Benutzer von der vSphere Web Client-Benutzeroberfläche aus deaktivieren und aktivieren.

- **Löschen eines vCenter Single Sign On-Benutzers**

Sie können Benutzer in der Domäne „vsphere.local“ über vCenter Single Sign On löschen. Lokale Betriebssystembenutzer oder Benutzer in einer anderen Domäne können auf dem vSphere Web Client nicht gelöscht werden.

- **Bearbeiten eines vCenter Single Sign On-Benutzers**

Sie können das Kennwort oder andere Details eines vCenter Single Sign On-Benutzers im vSphere Web Client ändern. In der vsphere.local-Domäne können Sie keine Benutzer umbenennen. Das bedeutet, dass Sie administrator@vsphere.local nicht umbenennen können.

- **Hinzufügen einer vCenter Single Sign On-Gruppe**

Im vCenter Single Sign On sind Gruppen, die auf der Registerkarte **Gruppen** aufgeführt werden, von vCenter Single Sign On als interne Gruppen eingestuft. Mit einer Gruppe können Sie einen Container für eine Sammlung von Gruppenmitgliedern (Prinzipale) erstellen.

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

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

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

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

■ Löschen von vCenter Single Sign On-Lösungsbenutzern

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

■ Ändern des vCenter Single Sign On-Kennworts

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

Hinzufügen von vCenter Single Sign On-Benutzern

Benutzer, die im vSphere Web Client auf der Registerkarte **Benutzer** aufgeführt sind, sind aus der Perspektive von vCenter Single Sign On interne Benutzer und gehören zur Domäne „vsphere.local“.

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

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Klicken Sie auf **Home** und navigieren Sie zu **Verwaltung > Single Sign On > Benutzer und Gruppen**.
- 3 Wenn es sich bei der derzeit ausgewählten Domäne nicht um „vsphere.local“ handelt, wählen Sie sie aus dem Dropdown-Menü aus.

Sie können keine Benutzer zu anderen Domänen hinzufügen.
- 4 Klicken Sie auf der Registerkarte **Benutzer** auf das Symbol **Neuer Benutzer**.
- 5 Geben Sie einen Benutzernamen und ein Kennwort für den neuen Benutzer ein.

Sie können den Benutzernamen nicht ändern, nachdem Sie einen Benutzer angelegt haben.
Das Kennwort muss die Anforderungen der Kennwortrichtlinie für das System erfüllen.
- 6 (Optional) Geben Sie den Vornamen und den Nachnamen des neuen Benutzers ein.
- 7 (Optional) Geben Sie eine E-Mail-Adresse und Beschreibung für den Benutzer ein.
- 8 Klicken Sie auf **OK**.

Ergebnisse

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

Nächste Schritte

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

Aktivieren und Deaktivieren von vCenter Single Sign On-Benutzern

Wenn ein vCenter Single Sign On-Benutzerkonto deaktiviert ist, kann sich der Benutzer beim vCenter Single Sign On-Server nur anmelden, wenn das Konto von einem Administrator aktiviert wird. Sie können Benutzer von der vSphere Web Client-Benutzeroberfläche aus deaktivieren und aktivieren.

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

Voraussetzungen

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

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Klicken Sie auf **Home** und navigieren Sie zu **Verwaltung > Single Sign On > Benutzer und Gruppen**.
- 3 Wählen Sie einen Benutzer aus, klicken Sie auf das Symbol **Deaktivieren** und klicken Sie auf **Ja**, wenn Sie dazu aufgefordert werden.
- 4 Um den Benutzer erneut zu aktivieren, klicken Sie mit der rechten Maustaste auf den Benutzer, wählen **Aktivieren** aus und klicken auf **Ja**, wenn Sie dazu aufgefordert werden.

Löschen eines vCenter Single Sign On-Benutzers

Sie können Benutzer in der Domäne „vsphere.local“ über vCenter Single Sign On löschen. Lokale Betriebssystembenutzer oder Benutzer in einer anderen Domäne können auf dem vSphere Web Client nicht gelöscht werden.

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

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.

- 2 Klicken Sie auf **Home** und navigieren Sie zu **Verwaltung > Single Sign On > Benutzer und Gruppen**.

- 3 Wählen Sie die Registerkarte **Benutzer** und dann die Domäne „vsphere.local“ aus.

- 4 Wählen Sie in der Liste mit den Benutzern den Benutzer aus, den Sie löschen möchten, und klicken Sie auf das Symbol **Löschen**.

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

Bearbeiten eines vCenter Single Sign On-Benutzers

Sie können das Kennwort oder andere Details eines vCenter Single Sign On-Benutzers im vSphere Web Client ändern. In der vsphere.local-Domäne können Sie keine Benutzer umbenennen. Das bedeutet, dass Sie administrator@vsphere.local nicht umbenennen können.

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

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

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

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.

- 2 Klicken Sie auf **Home** und navigieren Sie zu **Verwaltung > Single Sign On > Benutzer und Gruppen**.
- 3 Klicken Sie auf die Registerkarte **Benutzer**.
- 4 Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie **Benutzer bearbeiten**.
- 5 Nehmen Sie Änderungen am Benutzer vor.
 Sie können den Benutzernamen des Benutzers nicht ändern.
 Das Kennwort muss die Anforderungen der Kennwortrichtlinie für das System erfüllen.
- 6 Klicken Sie auf **OK**.

Hinzufügen einer vCenter Single Sign On-Gruppe

Im vCenter Single Sign On sind Gruppen, die auf der Registerkarte **Gruppen** aufgeführt werden, von vCenter Single Sign On als interne Gruppen eingestuft. Mit einer Gruppe können Sie einen Container für eine Sammlung von Gruppenmitgliedern (Prinzipale) erstellen.

Wenn Sie eine vCenter Single Sign On-Gruppe über die Verwaltungsschnittstelle des vSphere Web Client hinzufügen, wird diese Gruppe zur Domäne „vsphere.local“ hinzugefügt.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client als „administrator@vsphere.local“ oder als anderer Benutzer mit vCenter Single Sign On-Administratorrechten an.
 Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Klicken Sie auf **Home** und navigieren Sie zu **Verwaltung > Single Sign On > Benutzer und Gruppen**.
- 3 Wählen Sie die Registerkarte **Gruppen** aus und klicken Sie auf das Symbol **Neue Gruppe**.
- 4 Geben Sie einen Namen und eine Beschreibung für die Gruppe ein.
 Sie können den Gruppennamen nicht ändern, nachdem Sie die Gruppe angelegt haben.
- 5 Klicken Sie auf **OK**.

Nächste Schritte

- Fügen Sie dieser Gruppe Mitglieder hinzu.

Hinzufügen von Mitgliedern zu einer vCenter Single Sign On-Gruppe

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

Sie können einer vCenter Single Sign On-Gruppe Mitglieder von Microsoft Active Directory- oder OpenLDAP-Gruppen hinzufügen. Einer vCenter Single Sign On-Gruppe können Sie keine Gruppen aus externen Identitätsquellen hinzufügen.

Gruppen, die auf der Registerkarte **Gruppen** im vSphere Web Client aufgeführt werden, sind Teil der Domäne „vsphere.local“. Siehe [Gruppen in der Domäne „vsphere.local“](#).

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Klicken Sie auf **Home** und navigieren Sie zu **Verwaltung > Single Sign On > Benutzer und Gruppen**.
- 3 Klicken Sie auf die Registerkarte **Gruppen** und klicken Sie auf die Gruppe (z. B. Administratoren).
- 4 Klicken Sie im Gruppenmitgliederbereich auf das Symbol **Mitglieder hinzufügen**.
- 5 Wählen Sie die Identitätsquelle, die das Mitglied enthält, das zur Gruppe hinzugefügt werden soll.
- 6 (Optional) Geben Sie einen Suchbegriff ein und klicken Sie auf **Suchen**.
- 7 Wählen Sie das Mitglied aus und klicken Sie auf **Hinzufügen**.

Sie können gleichzeitig mehrere Mitglieder hinzufügen.
- 8 Klicken Sie auf **OK**.

Entfernen von Mitgliedern aus einer vCenter Single Sign On-Gruppe

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

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Klicken Sie auf **Home** und navigieren Sie zu **Verwaltung > Single Sign On > Benutzer und Gruppen**.
- 3 Wählen Sie die Registerkarte **Gruppen** aus und klicken Sie auf die Gruppe.
- 4 Wählen Sie in der Liste der Gruppenmitglieder den Benutzer oder die Gruppe aus, den oder die Sie entfernen möchten, und klicken Sie auf das Symbol **Mitglied entfernen**.

- 5 Klicken Sie auf **OK**.

Ergebnisse

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

Löschen von vCenter Single Sign On-Lösungsbenutzern

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

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

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

Verfahren

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

Benutzer mit vCenter Single Sign On-Administratorrechten befinden sich in der Administratorengruppe in der Domäne „vsphere.local“.
- 2 Klicken Sie auf **Home** und navigieren Sie zu **Verwaltung > Single Sign On > Benutzer und Gruppen**.
- 3 Klicken Sie auf die Registerkarte **Lösungsbenutzer** und anschließend auf den Lösungsbenutzernamen.
- 4 Klicken Sie auf das Symbol **Lösungsbenutzer löschen**.
- 5 Klicken Sie auf **Ja**.

Ergebnisse

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

Ändern des vCenter Single Sign On-Kennworts

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

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

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

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

Verfahren

- 1 Stellen Sie über einen Browser eine Verbindung zum Platform Services Controller her, indem Sie folgende URL eingeben:

`https://psc_hostname_or_IP/psc`

In einer eingebetteten Bereitstellung ist der Hostname oder die IP-Adresse von Platform Services Controller identisch mit dem Hostnamen oder der IP-Adresse von vCenter Server.

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

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

- 3 Klicken Sie im oberen Navigationsbereich links vom Hilfemenü auf Ihren Benutzernamen, um das Pulldown-Menü zu öffnen.

Alternativ können Sie auch **Single Sign-On > Benutzer und Gruppen** auswählen und dann im Kontextmenü die Option **Benutzer bearbeiten** auswählen.

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

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

Das Kennwort muss der Kennwortrichtlinie entsprechen.

- 6 Klicken Sie auf **OK**.

Best Practices für die Sicherheit von vCenter Single Sign On

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

Die Authentifizierungs- und Zertifikatinfrastruktur von vSphere 6.0 sorgt für hohe Sicherheit in Ihrer vSphere-Umgebung. Um sicherzugehen, dass keine Sicherheitsrisiken in der Infrastruktur entstehen, befolgen Sie die Best Practices für vCenter Single Sign On.

Prüfen des Kennwortablaufs

Die Standardkennwortrichtlinie für vCenter Single Sign On sieht vor, dass Kennwörter nach 90 Tagen ablaufen. Nach 90 Tagen kann ein Kennwort nicht mehr zur Anmeldung verwendet werden. Überprüfen Sie das Ablaufdatum und aktualisieren Sie die Kennwörter rechtzeitig.

Konfigurieren von NTP

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

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

Fehlerbehebung für vCenter Single Sign On

Das Konfigurieren von vCenter Single Sign On kann ein komplexer Vorgang sein.

Die folgenden Themen bieten einen guten Einstieg in die Fehlerbehebung für vCenter Single Sign On. Zusätzliche Pointer finden Sie in diesem Dokumentationscenter und im VMware-Knowledgebase-System.

Ermitteln der Ursache eines Lookup Service-Fehlers

Bei der Installation von vCenter Single Sign On wird ein Fehler angezeigt, der sich auf vCenter Server oder den vSphere Web Client bezieht.

Problem

Die Installationsprogramme von vCenter Server und Web Client zeigen folgenden Fehler an: Der Lookup Service konnte nicht kontaktiert werden. Einzelheiten hierzu finden Sie in der Datei 'VM_ssoreg.log' im temporären Systemordner.

Ursache

Dieses Problem kann mehrere Ursachen haben. Dazu zählen nicht synchronisierte Uhren auf den Hostmaschinen, Firewall-Blockierung und nicht gestartete Dienste.

Lösung

- 1 Vergewissern Sie sich, dass die Uhren auf den Hostmaschinen synchronisiert sind, auf denen vCenter Single Sign On, vCenter Server und Web Client ausgeführt werden.

2 Zeigen Sie die in der Fehlermeldung angegebene Protokolldatei an.

„Temporärer Systemordner“ in der Meldung bezieht sich auf %TEMP%.

3 Suchen Sie in der Protokolldatei nach den folgenden Meldungen.

Die Protokolldatei enthält die Ausgaben aller Installationsversuche. Suchen Sie die letzte Meldung mit folgendem Inhalt `Registrierungsprovider wird initialisiert...`

Meldung	Ursache und Lösung
java.net.ConnectException: Connection timed out: connect	Die IP-Adresse ist falsch, eine Firewall blockiert den Zugriff auf vCenter Single Sign On oder vCenter Single Sign On ist überlastet. Stellen Sie sicher, dass der vCenter Single Sign On-Port (standardmäßig 7444) nicht von einer Firewall blockiert wird und die Maschine, auf der vCenter Single Sign On installiert ist, über entsprechende freie CPU-, E/A- und RAM-Kapazitäten verfügt.
java.net.ConnectException: Connection refused: connect	Die IP-Adresse oder der FQDN ist falsch und der vCenter Single Sign On-Dienst wurde nicht oder innerhalb der letzten Minute gestartet. Vergewissern Sie sich, dass vCenter Single Sign On ausgeführt wird, indem Sie den Status des vCenter Single Sign On-Diensts (Windows) bzw. des vmware-ss0-Daemons (Linux) prüfen. Starten Sie den Dienst neu. Wenn das Problem dadurch nicht behoben wird, finden Sie weitere Informationen im Handbuch für vSphere-Fehlerbehebung im Abschnitt zur Wiederherstellung.
Unerwarteter Statuscode: 404. Fehler bei der Initialisierung des SSO-Servers	Starten Sie vCenter Single Sign On neu. Wenn das Problem dadurch nicht behoben wird, finden Sie weitere Informationen im <i>Handbuch für vSphere-Fehlerbehebung</i> im Abschnitt zur Wiederherstellung.
Die auf der Benutzeroberfläche angezeigte Fehlermeldung beginnt mit Es konnte keine Verbindung zu vCenter Single Sign On hergestellt werden.	Außerdem wird der Rückgabecode <code>SslHandshakeFailed</code> angezeigt. Es handelt sich hierbei um einen ungewöhnlichen Fehler. Er gibt an, dass die bereitgestellte IP-Adresse oder der bereitgestellte FQDN, die bzw. der in den vCenter Single Sign On-Host aufgelöst wird, nicht mit der Angabe bei der Installation von vCenter Single Sign On übereinstimmt. Suchen Sie in %TEMP%\VM_ssoreg.log die Zeile, die die folgende Meldung enthält. Hostname im Zertifikat stimmt nicht überein: <Bei der Installation konfigurierter FQDN bzw. konfigurierte IP-Adresse> != <A> oder oder <C>. Dabei ist A der während der Installation von vCenter Single Sign On eingegebene FQDN, und B und C sind systemgenerierte zulässige Alternativen. Korrigieren Sie die Konfiguration so, dass der auf der rechten Seite des Ungleichheitszeichens (!=) in der Protokolldatei angegebene FQDN verwendet wird. In den meisten Fällen können Sie den während der Installation von vCenter Single Sign On angegebenen FQDN verwenden. Wenn keine der Alternativen in Ihrer Netzwerkkonfiguration verwendet werden kann, stellen Sie Ihre SSL-Konfiguration von vCenter Single Sign On wieder her.

Anmelden unter Verwendung der Active Directory-Domänenauthentifizierung nicht möglich

Sie melden sich bei einer vCenter Server-Komponente über den vSphere Web Client an. Sie verwenden Ihren Benutzernamen und Ihr Kennwort von Active Directory. Authentifizierung schlägt fehl.

Problem

Sie fügen eine Active Directory-Identitätsquelle zu vCenter Single Sign On hinzu, aber die Benutzer können sich nicht bei vCenter Server anmelden.

Ursache

Benutzer verwenden ihren Benutzernamen und ihr Kennwort, um sich bei der Standarddomäne anzumelden. Für alle anderen Domänen müssen Benutzer den Domänennamen angeben (user@domain oder DOMÄNE\Benutzer).

Wenn Sie die vCenter Server Appliance verwenden, liegen möglicherweise andere Probleme vor.

Lösung

Sie können die standardmäßige Identitätsquelle für alle vCenter Single Sign On-Bereitstellungen ändern. Benutzer können sich nach dieser Änderung nur mit dem Benutzernamen und Kennwort bei der standardmäßigen Identitätsquelle anmelden.

Informationen zur Konfiguration Ihrer Identitätsquelle für die integrierte Windows-Authentifizierung mit einer untergeordneten Domäne in Ihrer Active Directory-Gesamtstruktur finden Sie im VMware-Knowledgebase-Artikel [2070433](#). Standardmäßig verwendet die integrierte Windows-Authentifizierung die Rootdomäne Ihrer Active Directory-Gesamtstruktur.

Wenn Sie die vCenter Server Appliance verwenden und eine Änderung der standardmäßigen Identitätsquelle das Problem nicht behebt, führen Sie die folgenden zusätzlichen Schritte zur Fehlerbehebung durch:

- 1 Synchronisieren Sie die Uhren zwischen der vCenter Server Appliance und den Active Directory-Domänencontrollern.
- 2 Stellen Sie sicher, dass jeder Domänencontroller über einen Pointer Record (PTR) im DNS-Dienst der Active Directory-Domäne verfügt und dass die PTR-Informationen mit dem DNS-Namen des Controllers übereinstimmen. Wenn Sie die vCenter Server Appliance verwenden, können Sie die folgenden Befehle ausführen, um die Aufgabe durchzuführen:
 - a Führen Sie den folgenden Befehl aus, um die Domänencontroller aufzulisten:

```
# dig SRV _ldap._tcp.my-ad.com
```

Die relevanten Adressen befinden sich, wie im folgenden Beispiel, im Antwort-Bereich:

```
;; ANSWER SECTION:
_ldap._tcp.my-ad.com. (...) my-controller.my-ad.com
...
```

- b Stellen Sie die Forward- und Reverse-Auflösung für jeden Domänencontroller fest, indem Sie den folgenden Befehl ausführen:

```
# dig my-controller.my-ad.com
```

Die relevanten Adressen befinden sich, wie im folgenden Beispiel, im Antwort-Bereich:

```
;; ANSWER SECTION:
my-controller.my-ad.com (...) IN A controller IP address
...
```

```
# dig -x <controller IP address>
```

Die relevanten Adressen befinden sich, wie im folgenden Beispiel, im Antwort-Bereich:

```
;; ANSWER SECTION:
IP-in-reverse.in-addr.arpa. (...) IN PTR my-controller.my-ad.com
...
```

- 3 Wenn das Problem dadurch nicht gelöst wird, entfernen Sie die vCenter Server Appliance aus der Active Directory-Domäne und treten anschließend der Domäne wieder bei. Informationen finden Sie in der Dokumentation *vCenter Server Appliance-Konfiguration*.
- 4 Schließen Sie alle mit der vCenter Server Appliance verbundenen Browsersitzungen und starten Sie alle Dienste neu.

```
/bin/service-control --restart --all
```

vCenter Server-Anmeldung schlägt aufgrund des gesperrten Benutzerkontos fehl

Wenn Sie sich von der vSphere Web Client-Anmeldeseite aus bei vCenter Server anmelden, zeigt eine Fehlermeldung an, dass das Benutzerkonto gesperrt ist.

Problem

Nach mehreren fehlgeschlagenen Versuchen können Sie sich mithilfe von vCenter Single Sign On nicht mehr beim vSphere Web Client anmelden. Sie erhalten die Meldung, dass Ihr Konto gesperrt ist.

Ursache

Sie haben die maximale Anzahl an fehlgeschlagenen Anmeldeversuchen überschritten.

Lösung

- ◆ Wenn Sie sich als Benutzer der Systemdomäne (vsphere.local) anmelden, bitten Sie Ihren vCenter Single Sign On-Administrator, Ihr Konto zu entsperren. Alternativ können Sie warten, bis Ihr Konto entsperrt wird, falls in den Kennwortrichtlinien eine Frist für den Ablauf der Sperre eingestellt ist. vCenter Single Sign On-Administratoren können mit Befehlen der Befehlszeilenschnittstelle Ihr Konto entsperren.
- ◆ Wenn Sie sich als Benutzer von Active Directory oder der LDAP-Domäne anmelden, bitten Sie Ihren Active Directory- bzw. LDAP-Administrator, Ihr Konto zu entsperren.

Replizierung des VMware-Verzeichnisdiensts kann lange dauern

Wenn in Ihrer Umgebung mehrere Platform Services Controller-Instanzen vorhanden sind und eine der Platform Services Controller-Instanzen nicht mehr verfügbar ist, kann Ihre Umgebung weiterhin verwendet werden. Sobald der Platform Services Controller wieder verfügbar ist, werden Benutzerdaten und sonstige Informationen in der Regel innerhalb von 60 Sekunden repliziert. Unter bestimmten Umständen kann die Replizierung jedoch lange dauern.

Problem

In bestimmten Situationen wird die Replizierung für die VMware-Verzeichnisdienst-Instanzen nicht sofort angezeigt. Beispielsweise, wenn in Ihrer Umgebung mehrere Platform Services Controller-Instanzen an unterschiedlichen Orten vorhanden sind und Sie umfangreiche Änderungen vornehmen, während ein Platform Services Controller nicht verfügbar ist. Beispielsweise wird ein neuer Benutzer, der zu einer verfügbaren Platform Services Controller-Instanz hinzugefügt wurde, erst nach Abschluss der Replizierung in der anderen Instanz angezeigt.

Ursache

Im regulären Betrieb werden Änderungen an einer Instanz des VMware-Verzeichnisdiensts (vmdir) in einer Platform Services Controller-Instanz (Knoten) für den direkten Replizierungspartner innerhalb von etwa 60 Sekunden angezeigt. In Abhängigkeit von der Replizierungstopologie müssen Änderungen an einem Knoten möglicherweise über Zwischenknoten weitergegeben werden, bevor sie für jede vmdir-Instanz in jedem Knoten angezeigt werden. Zu den replizierten Informationen zählen Benutzerinformationen, Zertifikatsinformationen, Lizenzinformationen für virtuelle Maschinen, die mit VMware VMotion erstellt, geklont oder migriert werden, usw.

Wenn die Replizierungsverbindung unterbrochen wird, beispielsweise aufgrund eines Netzausfalls oder weil ein Knoten nicht mehr verfügbar ist, werden Änderungen im Verbund nicht vereinheitlicht. Nach der Wiederherstellung des nicht verfügbaren Knotens versucht jeder Knoten, alle Änderungen zu übernehmen. Letztlich weisen alle vmdir-Instanzen einen einheitlichen Status auf. Es kann jedoch eine Weile dauern, um diesen Status zu erreichen, wenn viele Änderungen vorgenommen wurden, während ein Knoten nicht verfügbar war.

Lösung

Ihre Umgebung kann während der Replizierung wie gewohnt verwendet werden. Nehmen Sie nur dann eine Fehlerbehebung vor, wenn der Vorgang länger als eine Stunde dauert.

vSphere-Sicherheitszertifikate

3

vSphere-Komponenten verwenden SSL für die sichere Kommunikation miteinander und mit ESXi. Die SSL-Kommunikation sorgt für die Vertraulichkeit und Integrität der Daten. Die Daten sind geschützt und können nicht unbemerkt bei der Übertragung geändert werden.

Zertifikate werden auch von vCenter Server-Diensten wie dem vSphere Web Client für die anfängliche Authentifizierung bei vCenter Single Sign On verwendet. vCenter Single Sign On stellt für jede Komponente ein SAML-Token bereit, das die Komponente künftig für die Authentifizierung verwendet.

Ab vSphere 6.0 stellt die VMware Certificate Authority (VMCA) für jeden ESXi-Host und jeden vCenter Server-Dienst ein Zertifikat bereit, das standardmäßig von VMCA signiert ist.

Sie können die vorhandenen Zertifikate durch neue VMCA-signierte Zertifikate ersetzen, VMCA als untergeordnete Zertifizierungsstelle einrichten oder alle Zertifikate durch benutzerdefinierte Zertifikate ersetzen. Es sind mehrere Optionen verfügbar:

Tabelle 3-1. Unterschiedliche Methoden für die Zertifikatsersetzung

Option	Informationen hierzu finden Sie unter
Mithilfe der Webschnittstelle von Platform Services Controller (vSphere 6.0 Update 1 und höher)	Verwalten von Zertifikaten mit der Platform Services Controller-Webschnittstelle
Mithilfe des Dienstprogramms vSphere Certificate Manager über die Befehlszeile	Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager
Mithilfe von CLI-Befehlen für die manuelle Zertifikatsersetzung	Verwalten von Zertifikaten und Diensten mit CLI-Befehlen



vSphere-Zertifikatsverwaltung

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

Dieses Kapitel enthält die folgenden Themen:

- [Zertifikatsanforderungen für unterschiedliche Lösungspfade](#)
- [Zertifikatsverwaltung – Übersicht](#)
- [Verwalten von Zertifikaten mit der Platform Services Controller-Webschnittstelle](#)
- [Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager](#)

- [Manuelle Zertifikatsersetzung](#)
- [Verwalten von Zertifikaten und Diensten mit CLI-Befehlen](#)
- [Anzeigen von vCenter-Zertifikaten mit dem vSphere Web Client](#)
- [Festlegen des Schwellenwerts für Warnungen zum Ablauf von vCenter-Zertifikaten](#)

Zertifikatsanforderungen für unterschiedliche Lösungspfade

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

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

Anforderungen für alle importierten Zertifikate

- Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
- PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Schlüssel, die Sie zu VECS hinzufügen, werden in PKCS8 konvertiert.
- x509 Version 3
- „SubjectAltName“ muss DNS-Name= *Maschinen-FQDN* enthalten
- CRT-Format
- Enthält die folgenden Schlüsselerwendungen: digitale Signatur, Unleugbarkeit, Schlüsselverschlüsselung.
- Client- und Serverauthentifizierung sind für „Erweiterte Schlüsselerwendung“ nicht zulässig.

Die folgenden Zertifikate werden von VMCA nicht unterstützt.

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

Einhaltung von RFC 2253 bei Zertifikaten

Das Zertifikat muss RFC 2253 einhalten.

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

String	Attributtyp X.500
CN	commonName
N	localityName

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

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

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

Anforderungen für die Verwendung von VMCA als Zwischenzertifizierungsstelle

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

Zertifikatstyp	Zertifikatsanforderungen
Rootzertifikat	<ul style="list-style-type: none"> ■ Sie können vSphere Certificate Manager zum Generieren der CSR verwenden. Siehe Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats (Zwischenzertifizierungsstelle). ■ Wenn Sie die CSR manuell erstellen möchten, muss das Zertifikat, das Sie zum Signieren senden, die folgenden Anforderungen erfüllen. <ul style="list-style-type: none"> ■ Schlüsselgröße: mindestens 2.048 Bit ■ PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert. ■ x509 Version 3 ■ Wenn Sie benutzerdefinierte Zertifikate verwenden, muss die Zertifizierungsstellenerweiterung für Stammzertifikate auf „true“ festgelegt werden, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein. ■ CRL-Signatur muss aktiviert sein. ■ „Erweiterte Schlüsselverwendung“ darf keine Clientauthentifizierung oder Serverauthentifizierung enthalten. ■ Keine explizite Beschränkung der Zertifikatskettenlänge. VMCA verwendet den OpenSSL-Standardwert von 10 Zertifikaten. ■ Zertifikate mit Platzhalterzeichen oder mehr als einem DNS-Namen werden nicht unterstützt. ■ Untergeordnete Zertifizierungsstellen von VMCA können nicht erstellt werden. <p>Im VMware Knowledge Base-Artikel 2112009, „Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0“, finden Sie ein Beispiel für die Verwendung der Microsoft-Zertifizierungsstelle.</p>
Maschinen-SSL-Zertifikat	<p>Sie können die CSR mithilfe des vSphere Certificate Manager oder manuell erstellen.</p> <p>Wenn Sie die CSR manuell erstellen, muss sie die weiter oben unter <i>Anforderungen für alle importierten Zertifikate</i> aufgeführten Anforderungen erfüllen. Darüber hinaus müssen Sie den FQDN für den Host angeben.</p>
Lösungsbenutzerzertifikat	<p>Sie können die CSR mithilfe des vSphere Certificate Manager oder manuell erstellen.</p> <p>Hinweis Sie müssen für jeden Lösungsbenutzer einen eindeutigen Wert für den Namen verwenden. Wenn Sie das Zertifikat manuell generieren, wird es in Abhängigkeit vom verwendeten Tool möglicherweise unter Betreff als CN angezeigt.</p>

Zertifikatstyp	Zertifikatsanforderungen
	Wenn Sie vSphere Certificate Manager verwenden, werden Sie für jeden Lösungsbenutzer zur Eingabe von Zertifikatsinformationen aufgefordert. vSphere Certificate Manager speichert die Informationen in der Datei <code>certtool.cfg</code> . Weitere Informationen hierzu finden Sie unter <i>Von Certificate Manager angeforderte Informationen</i> .

Anforderungen für benutzerdefinierte Zertifikate

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

Zertifikatstyp	Zertifikatsanforderungen
Maschinen-SSL-Zertifikat	<p>Für das Maschinen-SSL-Zertifikat auf jedem Knoten ist ein separates Zertifikat von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle erforderlich.</p> <ul style="list-style-type: none"> ■ Sie können die CSRs mit vSphere Certificate Manager generieren oder aber manuell erstellen. CSRs müssen die weiter oben unter <i>Anforderungen für alle importierten Zertifikate</i> aufgeführten Anforderungen erfüllen. ■ Wenn Sie vSphere Certificate Manager verwenden, werden Sie für jeden Lösungsbenutzer zur Eingabe von Zertifikatsinformationen aufgefordert. vSphere Certificate Manager speichert die Informationen in der Datei <code>certtool.cfg</code>. Weitere Informationen hierzu finden Sie unter <i>Von Certificate Manager angeforderte Informationen</i>. ■ Für die meisten Felder können Sie den Standardwert übernehmen oder aber standortspezifische Werte eingeben. Der FQDN der Maschine ist erforderlich.
Lösungsbenutzerzertifikat	<p>Für jeden Lösungsbenutzer auf jedem Knoten ist ein separates Zertifikat von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle erforderlich.</p> <ul style="list-style-type: none"> ■ Sie können die CSRs mit vSphere Certificate Manager generieren oder aber selbst erstellen. CSRs müssen die weiter oben unter <i>Anforderungen für alle importierten Zertifikate</i> aufgeführten Anforderungen erfüllen. ■ Wenn Sie vSphere Certificate Manager verwenden, werden Sie für jeden Lösungsbenutzer zur Eingabe von Zertifikatsinformationen aufgefordert. vSphere Certificate Manager speichert die Informationen in der Datei <code>certtool.cfg</code>. Weitere Informationen hierzu finden Sie unter <i>Von Certificate Manager angeforderte Informationen</i>. <p>Hinweis Sie müssen für jeden Lösungsbenutzer einen eindeutigen Wert für den Namen verwenden. Wenn Sie das Zertifikat manuell generieren, wird es in Abhängigkeit vom verwendeten Tool möglicherweise unter Betreff als CN angezeigt.</p> <p>Wenn Sie später Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate ersetzen, geben Sie die vollständige Signaturzertifikatkette der Drittanbieterzertifizierungsstelle an.</p>

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

Zertifikatsverwaltung – Übersicht

Die Auswirkungen der neuen Zertifikatinfrastruktur sind abhängig von den Anforderungen in Ihrer Umgebung, ob Sie eine Neuinstallation oder ein Upgrade durchführen und ob Sie ESXi oder vCenter Server verwenden.

Administratoren, die VMware-Zertifikate nicht ersetzen

Wenn Sie ein Administrator sind, der aktuell VMware-Zertifikate nicht ersetzt, kann VMCA die komplette Zertifikatsverwaltung für Sie übernehmen. VMCA stellt vCenter Server-Komponenten und ESXi-Hosts Zertifikate bereit, die VMCA als Stammzertifizierungsstelle verwenden. Wenn Sie ein Upgrade auf vSphere 6 von einer früheren Version von vSphere durchführen, werden alle selbstsignierten Zertifikate durch Zertifikate ersetzt, die durch VMCA signiert wurden.

Administratoren, die VMware-Zertifikate durch benutzerdefinierte Zertifikate ersetzen

Für eine Neuinstallation haben Administratoren diese Optionen, wenn die Unternehmensrichtlinien von einer Drittanbieter- oder Unternehmenszertifizierungsstelle signierte Zertifikate oder benutzerdefinierte Zertifikatinformationen verlangen.

- Ersetzen Sie das VMCA-Stammzertifikat durch ein von einer Zertifizierungsstelle signiertes Zertifikat. In diesem Szenario handelt es sich beim VMCA-Zertifikat um ein Zwischenzertifikat dieser Drittanbieter-Zertifizierungsstelle. VMCA stellt vCenter Server-Komponenten und ESXi-Hosts Zertifikate bereit, die die vollständige Zertifikatskette beinhalten.
- Wenn die Unternehmensrichtlinien keine Zwischenzertifikate in der Zertifikatskette zulassen, müssen Sie Zertifikate explizit ersetzen. Sie können das Dienstprogramm vSphere Certificate Manager verwenden oder Zertifikate mithilfe der Zertifikatsverwaltungs-CLIs manuell ersetzen.

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

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

Nach dem Upgrade von vCenter Server können Administratoren den Zertifikatsmodus „Benutzerdefiniert“ festlegen (siehe [Ändern des Zertifikatsmodus](#)). Wenn der Zertifikatsmodus „VMCA“ lautet (Standardwert) und der Benutzer über den vSphere Web Client ein Zertifikat aktualisiert, werden die benutzerdefinierten Zertifikate durch VMCA-signierte Zertifikate ersetzt.

- Die vorhandene Umgebung bestimmt, was bei vCenter Server-Komponenten passiert.
 - Wenn Sie ein Upgrade einer einfachen Installation auf eine eingebettete Bereitstellung durchführen, werden benutzerdefinierte Zertifikate von vCenter Server beibehalten. Die Funktionsweise der Umgebung ist nach dem Upgrade unverändert.

- Bei einem Upgrade einer Bereitstellung mit mehreren Sites, in der sich vCenter Single Sign On auf einer anderen Maschine als andere vCenter Server-Komponenten befindet, wird eine Bereitstellung mit mehreren Knoten erstellt, die einen Platform Services Controller-Knoten und einen oder mehrere Verwaltungsknoten aufweist.

In diesem Szenario werden die vorhandenen vCenter Server- und vCenter Single Sign On-Zertifikate beibehalten und als Maschinen-SSL-Zertifikate verwendet. VMCA weist jedem Lösungsbenutzer ein VMCA-signiertes Zertifikat zu (Sammlung von vCenter-Diensten). Ein Lösungsbenutzer verwendet dieses Zertifikat nur zum Authentifizieren bei vCenter Single Sign On, weshalb es möglicherweise nicht notwendig ist, Lösungsbenutzerzertifikate zu ersetzen.

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

vCenter Server-Schnittstellen

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

vSphere Certificate Manager-Dienstprogramm

Führen Sie alle gängigen Zertifikatsverwaltungsaufgaben über die Befehlszeile aus.

Zertifikatsverwaltungs-CLIs

Führen Sie alle Zertifikatsverwaltungsaufgaben mit `dir-cli`, `certool` und `vecs-cli` aus.

vSphere Web Client-Zertifikatsverwaltung

Zeigen Sie Zertifikate einschließlich der Informationen zum Ablauf von Zertifikaten an.

Für ESXi führen Sie die Zertifikatsverwaltung über den vSphere Web Client aus. Zertifikate werden von der VMCA bereitgestellt und nur lokal auf dem ESXi-Host gespeichert, jedoch nicht in vmdir oder VECS. Siehe [Zertifikatsverwaltung für ESXi-Hosts](#).

Unterstützte vCenter-Zertifikate

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

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

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

Übersicht Zertifikatsersetzung

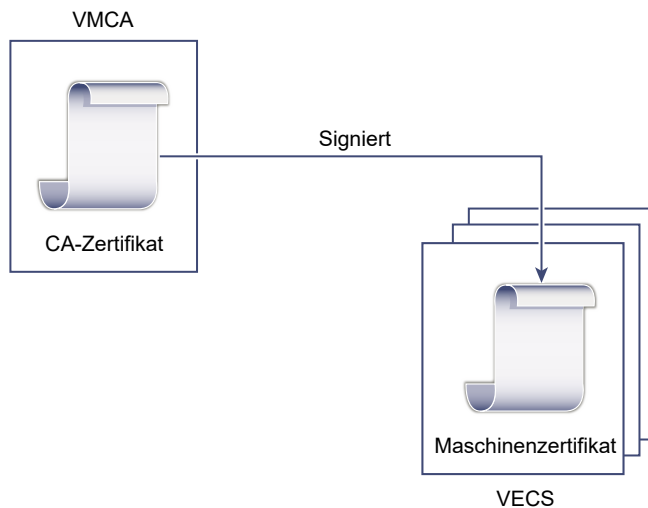
Sie können je nach der Unternehmensrichtlinie und den Anforderungen für das System, das Sie konfigurieren, verschiedene Arten von Zertifikatsersetzungen ausführen. Sie können jede Ersetzung mit dem Dienstprogramm „vSphere Certificate Manager“ oder manuell über die Befehlszeilenschnittstellen durchführen,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

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

Ersetzen durch von VMCA signierte Zertifikate

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

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

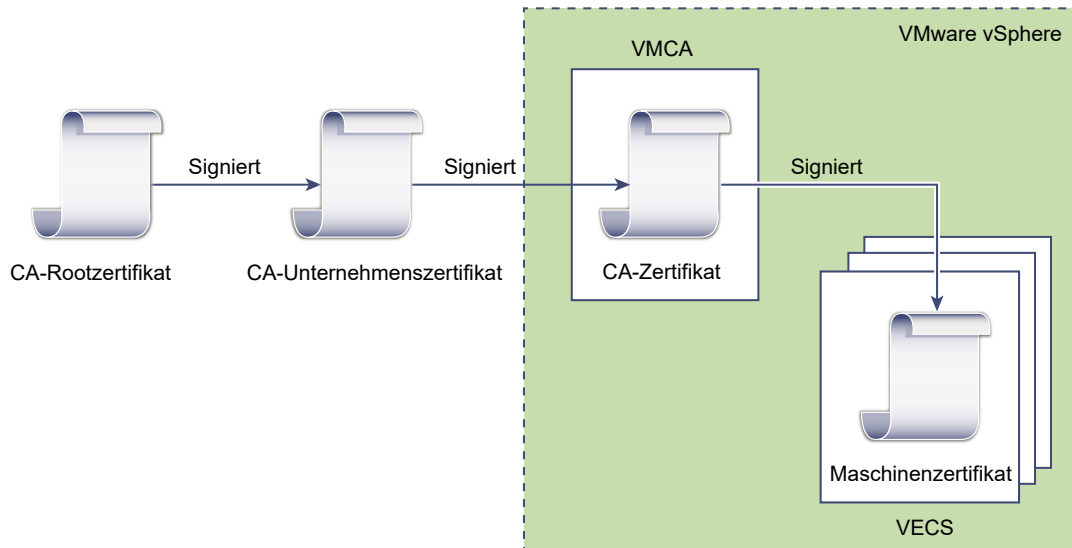


VMCA zu einer Zwischenzertifizierungsstelle machen

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

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

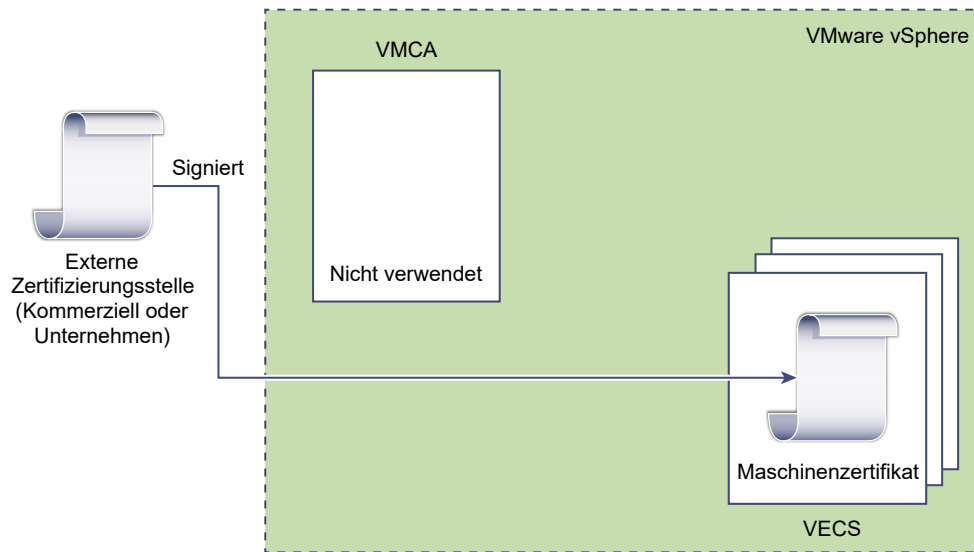
Abbildung 3-2. Zertifikate, die durch eine Zertifizierungsstelle eines Drittanbieters oder Unternehmens signiert wurden, verwenden VMCA als Zwischenzertifizierungsstelle



VMCA nicht verwenden, benutzerdefinierte Zertifikate zur Verfügung stellen

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

Abbildung 3-3. Externe Zertifikate werden direkt in VECS gespeichert



Hybrid-Bereitstellung

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

ESXi-Zertifikatsersetzung

Für ESXi-Hosts können Sie die Methode der Zertifikatsbereitstellung über den vSphere Web Client ändern.

Modus „VMware-Zertifizierungsstelle“ (Standard)

Wenn Sie Zertifikate über den vSphere Web Client erneuern, gibt VMCA die Zertifikate für die Hosts aus. Wenn Sie das VMCA-Rootzertifikat geändert haben, sodass eine Zertifikatskette enthalten ist, enthalten die Hostzertifikate die vollständige Kette.

Modus „Benutzerdefinierte Zertifizierungsstelle“

Damit können Sie Zertifikate, die nicht von VMCA signiert oder ausgegeben wurden, manuell aktualisieren und verwenden.

Fingerabdruckmodus

Kann verwendet werden, um 5.5-Zertifikate beim Aktualisieren beizubehalten. Verwenden Sie diesen Modus nur vorübergehend in Debugging-Situationen.

Verwendung von Zertifikaten in vSphere 6.0

Ab vSphere 6.0 stellt die VMware-Zertifizierungsstelle (VMware Certificate Authority, VMCA) Zertifikate für Ihre Umgebung bereit. Hierzu zählen Maschinen-SSL-Zertifikate für sichere Verbindungen, Lösungsbenutzerzertifikate für die Authentifizierung bei vCenter Single Sign On und Zertifikate für ESXi-Hosts, die zu vCenter Server hinzugefügt werden.

Die folgenden Zertifikate werden verwendet.

Tabelle 3-2. Zertifikate in vSphere 6.0

Zertifikat	Bereitgestellt durch	Speicherort
ESXi-Zertifikate	VMCA (Standard)	Lokal auf ESXi-Host
Maschinen-SSL-Zertifikate	VMCA (Standard)	VECS
Lösungsbenutzerzertifikate	VMCA (Standard)	VECS
vCenter Single Sign On-SSL-Signaturzertifikat	Bereitgestellt während der Installation.	Verwalten Sie dieses Zertifikat über den vSphere Web Client. Warnung Dieses Zertifikat sollten Sie nicht im Dateisystem ändern, da dies zu unvorhersehbarem Verhalten führen kann.
VMware-Verzeichnisdienst (vmdir)-SSL-Zertifikat	Bereitgestellt während der Installation.	In seltenen Fällen müssen Sie dieses Zertifikat möglicherweise ersetzen. Siehe Ersetzen des VMware-Verzeichnisdienstzertifikats .

ESXi

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

Maschinen-SSL-Zertifikate

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

Alle Dienste kommunizieren über den Reverse-Proxy. Aus Kompatibilitätsgründen verwenden Dienste aus früheren Versionen von vSphere auch bestimmte Ports. Beispielsweise verwendet der vpxd-Dienst MACHINE_SSL_CERT, um den Endpoint verfügbar zu machen.

Jeder Knoten (eingebettete Bereitstellung, Verwaltungsknoten oder Platform Services Controller) verwendet ein eigenes Maschinen-SSL-Zertifikat. Alle Dienste, die auf diesem Knoten ausgeführt werden, verwenden dieses Maschinen-SSL-Zertifikat, um die SSL-Endpoints verfügbar zu machen.

Das Maschinen-SSL-Zertifikat wird wie folgt verwendet:

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

VMware-Produkte verwenden X.509 Version 3 (X.509v3)-Standardzertifikate für die Verschlüsselung von Sitzungsinformationen, die per SSL zwischen den Komponenten übertragen werden.

Lösungsbenutzerzertifikate

Ein Lösungsbenutzer kapselt einen oder mehrere vCenter Server-Dienste und verwendet die Zertifikate zum Authentifizieren bei vCenter Single Sign On über den Austausch von SAML-Token. Jeder Lösungsbenutzer muss bei vCenter Single Sign On authentifiziert werden.

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

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

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

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

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

- `vpxd`: vCenter-Dienst-Daemon (vpxd)-Speicher für Verwaltungsknoten und eingebettete Bereitstellungen. vpxd verwendet das in diesem Speicher gespeicherte Lösungsbenutzerzertifikat für die Authentifizierung bei vCenter Single Sign On.
- `vpxd-extensions`: vCenter-Erweiterungsspeicher. Enthält den Auto Deploy-Dienst, den Inventory Service und sonstige Dienste, die nicht Bestandteil anderer Lösungsbenutzer sind.

- `vsphere-webclient`: vSphere Web Client-Speicher. Enthält auch zusätzliche Dienste wie etwa den Leistungsdiagrammdienst.

Der Maschinenspeicher ist ebenfalls in jedem Platform Services Controller-Knoten enthalten.

vCenter Single Sign On-Zertifikate

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

vCenter Single Sign On-Signaturzertifikat

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

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

Dieses Zertifikat können Sie über den vSphere Web Client ersetzen. Siehe [Aktualisieren des Zertifikats für den Security Token Service](#).

VMware-Verzeichnisdienst-SSL-Zertifikat

Bei Verwendung benutzerdefinierter Zertifikate müssen Sie möglicherweise das VMware-Verzeichnisdienst-SSL-Zertifikat explizit ersetzen. Siehe [Ersetzen des VMware-Verzeichnisdienstzertifikats](#).

VMCA- und VMware-Kernidentitätsdienste

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

Zu den VMware-Kernidentitätsdiensten zählen mehrere Komponenten.

Tabelle 3-3. Kernidentitätsdienste

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

VMware Endpoint Certificate Store – Übersicht

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

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

VECS überprüft den VMware-Verzeichnisdienst (vmdir) in bestimmten Abständen auf Aktualisierungen für den TRUSTED_ROOTS-Speicher. Zertifikate und Schlüssel können Sie in VECS auch explizit mithilfe der `vecs-cli`-Befehle verwalten. Siehe [Befehlsreferenz für vecs-cli](#).

VECS enthält die folgenden Speicher.

Tabelle 3-4. Speicher in VECS

Speicher	Beschreibung
Maschinen-SSL-Speicher (MACHINE_SSL_CERT)	<ul style="list-style-type: none"> ■ Wird vom Reverse-Proxy-Dienst auf jedem vSphere-Knoten verwendet. ■ Wird vom VMware-Verzeichnisdienst (vmdir) für eingebettete Bereitstellungen und für jeden Platform Services Controller-Knoten verwendet. <p>Alle Dienste in vSphere 6.0 kommunizieren über einen Reverse-Proxy, der das Maschinen-SSL-Zertifikat verwendet. Aus Gründen der Abwärtskompatibilität verwenden die 5.x-Dienste weiterhin bestimmte Ports. Deshalb ist für bestimmte Dienste wie etwa vpxd ein eigener Port geöffnet.</p>
Vertrauenswürdiger Stammspeicher (TRUSTED_ROOTS)	Enthält alle vertrauenswürdigen Stammzertifikate.
Lösungsbenutzerspeicher <ul style="list-style-type: none"> ■ Maschine ■ vpxd ■ vpxd-extensions ■ vsphere-webclient 	<p>VECS enthält einen Speicher für jeden Lösungsbenutzer. Das Objekt jedes Lösungsbenutzerzertifikats muss eindeutig sein. So darf z. B. das Maschinenzertifikat nicht das gleiche Objekt wie das vpxd-Zertifikat haben.</p> <p>Lösungsbenutzerzertifikate werden für die Authentifizierung mit vCenter Single Sign On verwendet. vCenter Single Sign On überprüft, ob das Zertifikat gültig ist. Andere Zertifikatsattribute werden jedoch nicht überprüft. Bei einer eingebetteten Bereitstellung befinden sich alle Lösungsbenutzerzertifikate im selben System.</p> <p>Die folgenden Lösungsbenutzer-Zertifikatspeicher sind in VECS für jeden Verwaltungsknoten und für jede eingebettete Bereitstellung enthalten:</p> <ul style="list-style-type: none"> ■ machine: Wird vom Komponentenmanager, Lizenzserver und Protokollierungsdienst verwendet. <p>Hinweis Das Lösungsbenutzerzertifikat „machine“ hat nichts mit dem SSL-Zertifikat „machine“ zu tun. Das Lösungsbenutzerzertifikat „machine“ wird für den Austausch von SAML-Tokens verwendet; das SSL-Zertifikat „machine“ wird für sichere SSL-Verbindungen für eine Maschine verwendet.</p> <ul style="list-style-type: none"> ■ vpxd: vCenter-Dienst-Daemon (vpxd)-Speicher für Verwaltungsknoten und eingebettete Bereitstellungen. vpxd verwendet das in diesem Speicher gespeicherte Lösungsbenutzerzertifikat für die Authentifizierung bei vCenter Single Sign On. ■ vpxd-extensions: vCenter-Erweiterungsspeicher. Enthält den Auto Deploy-Dienst, den Inventory Service und sonstige Dienste, die nicht Bestandteil anderer Lösungsbenutzer sind. ■ vsphere-webclient: vSphere Web Client-Speicher. Enthält auch zusätzliche Dienste wie etwa den Leistungsdiagrammdienst. <p>Der Maschinenspeicher ist ebenfalls in jedem Platform Services Controller-Knoten enthalten.</p>

Tabelle 3-4. Speicher in VECS (Fortsetzung)

Speicher	Beschreibung
vSphere Certificate Manager Utility-Backup-Speicher (BACKUP_STORE)	Wird von VMCA (VMware Certificate Manager) für die Unterstützung der Zertifikatwiederherstellung verwendet. Nur der letzte Status wird als Backup gespeichert und Sie können nur den letzten Schritt rückgängig machen.
Weitere Speicher	<p>Weitere Speicher können durch Lösungen hinzugefügt werden. Beispielsweise fügt die VVOL-Lösung einen SMS-Speicher hinzu. Ändern Sie die Zertifikate in diesen Speichern nur, wenn Sie in VMware-Dokumentation oder in einem VMware-Knowledgebase-Artikel dazu aufgefordert werden.</p> <p>Hinweis CRLS werden in vSphere 6.0 nicht unterstützt. Dennoch kann durch das Löschen des TRUSTED_ROOTS_CRLS-Speichers Ihre Zertifikatinfrastruktur beschädigt werden. Den TRUSTED_ROOTS_CRLS-Speicher sollten Sie weder löschen noch ändern.</p>

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

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

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

Verwalten von Zertifikatswiderrufungen

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

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

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

Zertifikatsersetzung bei großen Bereitstellungen

Die Zertifikatsersetzung bei Bereitstellungen, die mehrere Verwaltungsknoten und einen oder mehrere Platform Services Controller-Knoten enthalten, ist mit der Zertifikatsersetzung bei eingebetteten Bereitstellungen vergleichbar. In beiden Fällen können Sie das Dienstprogramm

vSphere Certificate Management verwenden oder die Zertifikate manuell ersetzen. Für die Zertifikatsersetzung gelten bestimmte Best Practices.

Zertifikatsersetzung in High Availability-Umgebungen mit Lastausgleichsdienst

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

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

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

vSphere Certificate Manager

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

Manuelle Zertifikatsersetzung

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

- [Ersetzen der Maschinen-SSL-Zertifikate durch VMCA-signierte Zertifikate](#)
- [Ersetzen der Maschinen-SSL-Zertifikate \(Zwischenzertifizierungsstelle\)](#)
- [Ersetzen der Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate](#)

Ersetzen der Lösungsbenutzerzertifikate in Umgebungen mit mehreren Verwaltungsknoten

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

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

vSphere Certificate Manager

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

Manuelle Zertifikatsersetzung

- 1 Generieren Sie ein Zertifikat oder fordern Sie ein Zertifikat an. Sie benötigen die folgenden Zertifikate:
 - Ein Zertifikat für den Lösungsbenutzer „machine“ auf dem Platform Services Controller.
 - Ein Zertifikat für den Lösungsbenutzer „machine“ auf jedem Verwaltungsknoten.
 - Ein Zertifikat für jeden der folgenden Lösungsbenutzer auf jedem Verwaltungsknoten:
 - vpxd-Lösungsbenutzer
 - vpxd-extension-Lösungsbenutzer
 - vsphere-webclient-Lösungsbenutzer
- 2 Ersetzen Sie die Zertifikate auf jedem Knoten. Die genaue Vorgehensweise hängt vom verwendeten Zertifikatsersetzungstyp ab. Siehe [Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager](#).

Weitere Informationen finden Sie in den folgenden Themen:

- [Ersetzen der Lösungsbenutzerzertifikate durch neue VMCA-signierte Stammzertifikate](#)
- [Ersetzen der Lösungsbenutzerzertifikate \(Zwischenzertifizierungsstelle\)](#)
- [Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate](#)

Wenn die Unternehmensrichtlinien das Ersetzen aller Zertifikate verlangen, müssen Sie auch das Zertifikat für den VMware-Verzeichnisdienst (vmdir) auf dem Platform Services Controller ersetzen. Siehe [Ersetzen des VMware-Verzeichnisdienstzertifikats](#).

Zertifikatsersetzung in Umgebungen mit externen Lösungen

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

Sie können das Skript `ls_update_certs` ausführen, um das Problem zu beheben. Details finden Sie im [VMware-Knowledgebase-Artikel 2109074](#).

Verwalten von Zertifikaten mit der Platform Services Controller-Webschnittstelle

Zertifikate können Sie durch Anmelden bei der Platform Services Controller-Webschnittstelle anzeigen und verwalten. Viele Zertifikatsverwaltungsaufgaben können Sie entweder mit dem Dienstprogramm vSphere Certificate Manager oder mithilfe dieser Webschnittstelle ausführen.

Mit der Platform Services Controller-Webschnittstelle können Sie diese Verwaltungsaufgaben ausführen.

- Anzeigen der aktuellen Zertifikatspeicher sowie Hinzufügen und Entfernen von Zertifikatspeichereinträgen.
- Anzeigen der VMware Certificate Authority (VMCA)-Instanz im Zusammenhang mit diesem Platform Services Controller.
- Anzeigen von durch VMware Certificate Authority generierten Zertifikaten.
- Verlängern vorhandener Zertifikate oder Ersetzen von Zertifikaten.

Die meisten Abschnitte der Workflows zur Zertifikatsersetzung werden von der Platform Services Controller-Webschnittstelle vollständig unterstützt. Für das Generieren von Zertifikatssignieranforderungen (CSRs) können Sie das Dienstprogramm vSphere Certificate Manager verwenden.

Unterstützte Workflows

Nach dem Installieren eines Platform Services Controller stellt die VMware Certificate Authority auf diesem Knoten allen anderen Knoten in der Umgebung standardmäßig Zertifikate bereit. Zum Verlängern oder Ersetzen von Zertifikaten können Sie einen der folgenden Workflows verwenden.

Zertifikate erneuern

Sie können VMCA ein neues Rootzertifikat generieren lassen und alle Zertifikate in Ihrer Umgebung über die Platform Services Controller-Webschnittstelle verlängern.

VMCA zu einer Zwischenzertifizierungsstelle machen

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

Zertifikate durch benutzerdefinierte Zertifikate ersetzen

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

Falls Sie das Rootzertifikat für den VMware Directory Service (vmdir) ersetzen müssen oder falls Unternehmensrichtlinien das Ersetzen des vCenter Single Sign On-Zertifikats in einer Umgebung im gemischten Modus erfordern, können Sie CLI-Befehle zum Ersetzen dieser Zertifikate nach dem Ersetzen der anderen Zertifikate verwenden. Siehe [Ersetzen des VMware-Verzeichnisdienstzertifikats](#) und [Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus](#).

Durchsuchen der Zertifikatspeicher über die Platform Services Controller-Webschnittstelle

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

Weitere Informationen zu den verschiedenen Zertifikatspeichern in VECS finden Sie unter [VMware Endpoint Certificate Store – Übersicht](#).

Voraussetzungen

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

Verfahren

- 1 Stellen Sie über einen Browser eine Verbindung zum Platform Services Controller her, indem Sie folgende URL eingeben:

`https://psc_hostname_or_IP/psc`

In einer eingebetteten Bereitstellung ist der Hostname oder die IP-Adresse von Platform Services Controller identisch mit dem Hostnamen oder der IP-Adresse von vCenter Server.

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

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

- 3 Klicken Sie unter „Zertifikate“ auf **Zertifikatspeicher** und durchsuchen Sie den Zertifikatspeicher.
- 4 Wählen Sie im Pulldown-Menü den Zertifikatspeicher im VMware Endpoint Certificate Store (VECS) aus, den Sie durchsuchen möchten.

In [VMware Endpoint Certificate Store – Übersicht](#) werden die Komponenten der einzelnen Zertifikatspeicher erläutert.

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

- 6 Um einen Eintrag im ausgewählten Zertifikatspeicher zu löschen, klicken Sie auf das Symbol **Eintrag löschen**.

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

Ersetzen von Zertifikaten durch neue VMCA-signierte Zertifikate über die Platform Services Controller-Webschnittstelle

Sie können alle VMCA-signierten Zertifikate durch neue VMCA-signierte Zertifikate ersetzen. Dieser Vorgang wird als Verlängern von Zertifikaten bezeichnet. Sie können einzelne Zertifikate oder alle Zertifikate in Ihrer Umgebung über die Platform Services Controller-Webschnittstelle verlängern.

Voraussetzungen

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

Verfahren

- 1 Stellen Sie über einen Browser eine Verbindung zum Platform Services Controller her, indem Sie folgende URL eingeben:

`https://psc_hostname_or_IP/psc`

In einer eingebetteten Bereitstellung ist der Hostname oder die IP-Adresse von Platform Services Controller identisch mit dem Hostnamen oder der IP-Adresse von vCenter Server.

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

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

- 3 Wählen Sie unter „Zertifikate“ die Option **Zertifikatsverwaltung** aus und geben Sie die IP-Adresse oder den Hostnamen für den Platform Services Controller und den Benutzernamen sowie das Kennwort für den Administrator der lokalen Domäne (standardmäßig administrator@vsphere.local) an. Klicken Sie anschließend auf **Übermitteln**.

- 4 Verlängern Sie das Maschinen-SSL-Zertifikat für das lokale System.

- a Klicken Sie auf die Registerkarte **Maschinenzertifikate**.
- b Wählen Sie das Zertifikat aus, klicken Sie auf **Verlängern** und beantworten Sie die Eingabeaufforderung mit **Ja**.

- 5 (Optional) Verlängern Sie die Lösungsbenutzerzertifikate für das lokale System.
 - a Klicken Sie auf die Registerkarte **Lösungsbenutzerzertifikate**.
 - b Wählen Sie ein Zertifikat aus und klicken Sie auf **Verlängern**, um einzelne ausgewählte Zertifikate zu verlängern, oder klicken Sie auf **Alle verlängern**, um alle Lösungsbenutzerzertifikate zu verlängern.
 - c Beantworten Sie die Eingabeaufforderung mit **Ja**.
- 6 Wenn in Ihrer Umgebung ein externer Platform Services Controller vorhanden ist, können Sie die Zertifikate für jedes vCenter Server-System verlängern.
 - a Klicken Sie im Bereich „Zertifikatsverwaltung“ auf die Schaltfläche **Abmelden**.
 - b Geben Sie, wenn Sie dazu aufgefordert werden, die IP-Adresse oder den FQDN des vCenter Server-Systems und den Benutzernamen und das Kennwort eines vCenter Server-Administrators an, der sich bei vCenter Single Sign On authentifizieren kann.
 - c Verlängern Sie das Maschinen-SSL-Zertifikat auf dem vCenter Server und optional jedes Lösungsbenutzerzertifikat.
 - d Falls mehrere vCenter Server-Systeme in Ihrer Umgebung vorhanden sind, wiederholen Sie den Vorgang für jedes System.

Nächste Schritte

Starten Sie die Dienste auf dem Platform Services Controller neu. Sie können entweder den Platform Services Controller neu starten oder die folgenden Befehle über die Befehlszeile ausführen:

Windows

Unter Windows befindet sich der service-control-Befehl unter `VCENTER_INSTALL_PATH\bin`.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

Festlegen von VMCA über die Platform Services Controller-Webschnittstelle als Zwischenzertifizierungsstelle

Sie können die VMCA-Zertifikate von einer anderen Zertifizierungsstelle signieren lassen, sodass VMCA eine Zwischenzertifizierungsstelle wird. In Zukunft beinhalten alle von VMCA generierten Zertifikate die vollständige Zertifikatskette.

Diese Konfiguration können Sie mit dem Dienstprogramm vSphere Certificate Manager, mit der Befehlszeilenschnittstelle (CLI) oder über die Platform Services Controller-Webschnittstelle ausführen.

Voraussetzungen

- 1 Generieren Sie die Zertifikatsignieranforderung (Certificate Signing Request, CSR).
- 2 Bearbeiten Sie das erhaltene Zertifikat und platzieren Sie das aktuelle VMCA-Rootzertifikat im unteren Bereich.

Im Abschnitt [Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats \(Zwischenzertifizierungsstelle\)](#) werden beide Schritte erläutert.

Verfahren

- 1 Stellen Sie über einen Browser eine Verbindung zum Platform Services Controller her, indem Sie folgende URL eingeben:

`https://psc_hostname_or_IP/psc`

In einer eingebetteten Bereitstellung ist der Hostname oder die IP-Adresse von Platform Services Controller identisch mit dem Hostnamen oder der IP-Adresse von vCenter Server.

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

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

- 3 Um die vorhandenen Zertifikate durch das verkettete Zertifikat zu ersetzen, befolgen Sie diese Schritte:

- a Klicken Sie unter „Zertifikate“ auf **Zertifizierungsstelle** und wählen Sie die Registerkarte **Rootzertifikat** aus.
- b Klicken Sie auf **Zertifikat ersetzen**. Fügen Sie die Datei mit dem privaten Schlüssel und die Zertifikatsdatei (vollständige Zertifikatskette) hinzu und klicken Sie auf **OK**.
- c Klicken Sie im Dialogfeld **Rootzertifikat ersetzen** auf **Durchsuchen** und wählen Sie den privaten Schlüssel aus. Klicken Sie erneut auf **Durchsuchen**, wählen Sie das Zertifikat aus und klicken Sie auf **OK**.

In Zukunft signiert VMCA alle ausgestellten Zertifikate mit dem neuen verketteten Rootzertifikat.

- 4 Verlängern Sie das Maschinen-SSL-Zertifikat für das lokale System.
 - a Klicken Sie unter „Zertifikate“ auf **Zertifikatsverwaltung** und klicken Sie auf die Registerkarte **Maschinenzertifikate**.
 - b Wählen Sie das Zertifikat aus, klicken Sie auf **Verlängern** und beantworten Sie die Eingabeaufforderung mit **Ja**.

VMCA ersetzt das Maschinen-SSL-Zertifikat durch das von der neuen Zertifizierungsstelle signierte Zertifikat.

5 (Optional) Verlängern Sie die Lösungsbenutzerzertifikate für das lokale System.

- a Klicken Sie auf die Registerkarte **Lösungsbenutzerzertifikate**.
- b Wählen Sie ein Zertifikat aus, klicken Sie auf **Verlängern**, um einzelne ausgewählte Zertifikate zu verlängern, oder klicken Sie auf **Alle verlängern**, um alle Zertifikate zu ersetzen, und beantworten Sie die Eingabeaufforderung mit **Ja**.

VMCA ersetzt das Lösungsbenutzerzertifikat bzw. alle Lösungsbenutzerzertifikate durch von der neuen Zertifizierungsstelle signierte Zertifikate.

6 Wenn in Ihrer Umgebung ein externer Platform Services Controller vorhanden ist, können Sie die Zertifikate für jedes vCenter Server-System verlängern.

- a Klicken Sie im Bereich „Zertifikatsverwaltung“ auf die Schaltfläche **Abmelden**.
- b Geben Sie, wenn Sie dazu aufgefordert werden, die IP-Adresse oder den FQDN des vCenter Server-Systems und den Benutzernamen und das Kennwort eines vCenter Server-Administrators an, der sich bei vCenter Single Sign On authentifizieren kann.
- c Verlängern Sie das Maschinen-SSL-Zertifikat auf dem vCenter Server und optional jedes Lösungsbenutzerzertifikat.
- d Falls mehrere vCenter Server-Systeme in Ihrer Umgebung vorhanden sind, wiederholen Sie den Vorgang für jedes System.

Nächste Schritte

Starten Sie die Dienste auf dem Platform Services Controller neu. Sie können entweder den Platform Services Controller neu starten oder die folgenden Befehle über die Befehlszeile ausführen:

Windows

Unter Windows befindet sich der service-control-Befehl unter `VCENTER_INSTALL_PATH\bin`.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

Einrichten Ihres Systems für die Verwendung benutzerdefinierter Zertifikate des Platform Services Controller

Sie können den Platform Services Controller verwenden, um Ihre Umgebung für die Verwendung benutzerdefinierter Zertifikate einzurichten.

Mithilfe des Dienstprogramms Certificate Manager können Sie Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) für jede Maschine und für jeden Lösungsbenutzer generieren. Wenn Sie die CSRs an Ihre interne oder Drittanbieter-Zertifizierungsstelle übermitteln, gibt die Zertifizierungsstelle signierte Zertifikate und das Rootzertifikat zurück. Sie können sowohl das Rootzertifikat als auch die signierten Zertifikate aus der Platform Services Controller-Benutzerschnittstelle hochladen.

Generieren von Zertifikatssignieranforderungen mit vSphere Certificate Manager (benutzerdefinierte Zertifikate)

Mithilfe von vSphere Certificate Manager können Sie Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) generieren, die Sie anschließend mit Ihrer Unternehmenszertifizierungsstelle verwenden oder an eine externe Zertifizierungsstelle senden können. Sie können die Zertifikate mit den unterschiedlichen unterstützten Ersetzungsvorgängen von Zertifikaten verwenden.

Sie können das Certificate Manager-Tool wie folgt über die Befehlszeile ausführen:

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

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

Voraussetzungen

vSphere Certificate Manager fordert Sie zur Eingabe von Informationen auf. Die Eingabeaufforderungen sind abhängig von Ihrer Umgebung und vom Zertifikatstyp, den Sie ersetzen möchten.

- Beim Generieren von Zertifikatssignieranforderungen werden Sie generell aufgefordert, das Kennwort für den Benutzer „administrator@vsphere.local“ bzw. den Administrator für die vCenter Single Sign On-Domäne, mit der Sie eine Verbindung herstellen, einzugeben.
- Wenn Sie eine Zertifikatssignieranforderung in einer Umgebung mit einem externen Platform Services Controller generieren, werden Sie zur Eingabe des Hostnamens oder der IP-Adresse für den Platform Services Controller aufgefordert.
- Zum Generieren einer Zertifikatssignieranforderung für ein Maschinen-SSL-Zertifikat werden Sie zur Eingabe von Zertifikateigenschaften aufgefordert, die in der Datei `certtool.cfg` gespeichert sind. Für die meisten Felder können Sie den Standardwert übernehmen oder aber standortspezifische Werte eingeben. Der FQDN der Maschine ist erforderlich.

Verfahren

- 1 Starten Sie vSphere Certificate Manager auf jeder Maschine in Ihrer Umgebung und wählen Sie Option 1 aus.
- 2 Geben Sie, wenn Sie dazu aufgefordert werden, das Kennwort sowie die IP-Adresse oder den Hostnamen für den Platform Services Controller ein.
- 3 Wählen Sie Option 1 aus, um die Zertifikatssignieranforderung zu generieren, befolgen Sie die Anweisungen und beenden Sie Certificate Manager.

Im Rahmen dieses Vorgangs müssen Sie ein Verzeichnis angeben. Certificate Manager speichert die Zertifikats- und Schlüsseldateien in dem Verzeichnis.

- 4 Wenn Sie alle Lösungsbenutzerzertifikate ersetzen möchten, starten Sie Certificate Manager neu.
- 5 Wählen Sie Option 5 aus.
- 6 Geben Sie, wenn Sie dazu aufgefordert werden, das Kennwort sowie die IP-Adresse oder den Hostnamen für den Platform Services Controller ein.
- 7 Wählen Sie Option 1 aus, um die Zertifikatssignieranforderungen zu generieren, befolgen Sie die Anweisungen und beenden Sie Certificate Manager.

Im Rahmen dieses Vorgangs müssen Sie ein Verzeichnis angeben. Certificate Manager speichert die Zertifikats- und Schlüsseldateien in dem Verzeichnis.

Certificate Manager generiert auf jedem Platform Services Controller-Knoten je ein Zertifikats- und Schlüsselpaar. Certificate Manager generiert auf jedem vCenter Server-Knoten je vier Zertifikats- und Schlüsselpaare.

Nächste Schritte

Führen Sie die Zertifikatsersetzung durch.

Hinzufügen eines vertrauenswürdigen Rootzertifikats zum Zertifikatspeicher

Wenn Sie in Ihrer Umgebung Drittanbieterzertifikate verwenden möchten, müssen Sie ein vertrauenswürdiges Rootzertifikat zum Zertifikatspeicher hinzufügen.

Voraussetzungen

Beziehen Sie das benutzerdefinierte Rootzertifikat von Ihrer Drittanbieter- oder internen Zertifizierungsstelle.

Verfahren

- 1 Stellen Sie über einen Browser eine Verbindung zum Platform Services Controller her, indem Sie folgende URL eingeben:

`https://psc_hostname_or_IP/psc`

In einer eingebetteten Bereitstellung ist der Hostname oder die IP-Adresse von Platform Services Controller identisch mit dem Hostnamen oder der IP-Adresse von vCenter Server.

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

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

- 3 Wählen Sie unter „Zertifikate“ die Option **Zertifikatsverwaltung** aus und geben Sie die IP-Adresse oder den Hostnamen für den Platform Services Controller und den Benutzernamen sowie das Kennwort für den Administrator der lokalen Domäne (standardmäßig administrator@vsphere.local) an. Klicken Sie anschließend auf **Übermitteln**.
- 4 Wählen Sie **Vertrauenswürdige Rootzertifikate** aus und klicken Sie auf **Zertifikat hinzufügen**.
- 5 Klicken Sie auf **Durchsuchen** und wählen Sie den Speicherort der Zertifikatskette aus.
Sie können Dateien des Typs CER, PEM oder CRT verwenden.

Nächste Schritte

Ersetzen Sie die Maschinen-SSL-Zertifikate und optional auch die Lösungsbenutzerzertifikate durch die Zertifikate, die von dieser Zertifizierungsstelle signiert wurden.

Hinzufügen benutzerdefinierter Zertifikate aus dem Platform Services Controller

Sie können benutzerdefinierte Maschinen-SSL-Zertifikate und benutzerdefinierte Lösungsbenutzerzertifikate zum Zertifikatspeicher des Platform Services Controller hinzufügen.

In den meisten Fällen ist es ausreichend, das Maschinen-SSL-Zertifikat für jede Komponente zu ersetzen. Das Lösungsbenutzerzertifikat bleibt hinter einem Proxy-Server.

Voraussetzungen

Generieren Sie Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) für jedes zu ersetzende Zertifikat. Sie können die CSRs mit dem Dienstprogramm Certificate Manager generieren. Speichern Sie das Zertifikat und den privaten Schlüssel an einem Speicherort, auf den der Platform Services Controller zugreifen kann.

Verfahren

- 1 Stellen Sie über einen Browser eine Verbindung zum Platform Services Controller her, indem Sie folgende URL eingeben:

`https://psc_hostname_or_IP/psc`

In einer eingebetteten Bereitstellung ist der Hostname oder die IP-Adresse von Platform Services Controller identisch mit dem Hostnamen oder der IP-Adresse von vCenter Server.

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

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

- 3 Wählen Sie unter „Zertifikate“ die Option **Zertifikatsverwaltung** aus und geben Sie die IP-Adresse oder den Hostnamen für den Platform Services Controller und den Benutzernamen sowie das Kennwort für den Administrator der lokalen Domäne (standardmäßig administrator@vsphere.local) an. Klicken Sie anschließend auf **Übermitteln**.
- 4 Befolgen Sie zum Ersetzen eines Maschinenzertifikats diese Schritte:
 - a Wählen Sie die Registerkarte **Maschinenzertifikate** aus und klicken Sie auf das zu ersetzende Zertifikat.
 - b Klicken Sie auf **Ersetzen** und auf **Durchsuchen**, um die Zertifikatskette zu ersetzen. Klicken Sie anschließend auf **Durchsuchen**, um den privaten Schlüssel zu ersetzen.
- 5 Befolgen Sie zum Ersetzen von Lösungsbenutzerzertifikaten diese Schritte:
 - a Wählen Sie die Registerkarte **Lösungsbenutzerzertifikate** aus und klicken Sie auf das erste der vier Zertifikate für eine Komponente, z. B. **Maschine**.
 - b Klicken Sie auf **Ersetzen** und auf **Durchsuchen**, um die Zertifikatskette zu ersetzen. Klicken Sie anschließend auf **Durchsuchen**, um den privaten Schlüssel zu ersetzen.
 - c Wiederholen Sie den Vorgang für die anderen drei Zertifikate derselben Komponente.

Nächste Schritte

Starten Sie die Dienste auf dem Platform Services Controller neu. Sie können entweder den Platform Services Controller neu starten oder die folgenden Befehle über die Befehlszeile ausführen:

Windows

Unter Windows befindet sich der service-control-Befehl unter `VCENTER_INSTALL_PATH\bin`.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager

Mit dem Dienstprogramm vSphere Certificate Manager können Sie die meisten Zertifikatsverwaltungsaufgaben interaktiv über die Befehlszeile ausführen. vSphere Certificate Manager fordert Sie zur Eingabe der auszuführenden Aufgabe, der Zertifikatspeicherorte und

etwaiger sonstiger Informationen auf und beendet und startet dann Dienste und ersetzt Zertifikate.

Bei Verwendung von vSphere Certificate Manager müssen Sie die Zertifikate nicht in VECS (VMware Endpoint Certificate Store) platzieren und müssen die Dienste nicht starten und beenden.

Bevor Sie vSphere Certificate Manager ausführen, sollten Sie sich unbedingt mit dem Ersetzungsvorgang vertraut machen und die Zertifikate suchen, die Sie verwenden möchten.

Vorsicht Mit vSphere Certificate Manager kann nur eine Ausführungsebene rückgängig gemacht werden. Wenn Sie vSphere Certificate Manager zweimal ausführen und feststellen, dass Sie Ihre Umgebung versehentlich beschädigt haben, kann mit dem Tool die erste der beiden Ausführungsinstanzen nicht rückgängig gemacht werden.

Sie können das Tool wie folgt in der Befehlszeile ausführen:

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

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

Verfahren

1 Rückgängigmachen des zuletzt ausgeführten Vorgangs durch die erneute Veröffentlichung alter Zertifikate

Wenn Sie einen Zertifikatverwaltungsvorgang mithilfe von vSphere Certificate Manager durchführen, wird der aktuelle Zertifikatsstatus im BACKUP_STORE-Speicher in VECS gespeichert, bevor Zertifikate ersetzt werden. Sie können den zuletzt ausgeführten Vorgang rückgängig machen und den vorherigen Status wiederherstellen.

2 Alle Zertifikate zurücksetzen

Verwenden Sie die Option `Alle Zertifikate zurücksetzen`, wenn Sie alle vorhandenen vCenter-Zertifikate durch VMCA-signierte Zertifikate ersetzen möchten.

3 Neugenerieren eines neuen VMCA-Rootzertifikats und Ersetzen aller Zertifikate

Sie können das VMCA-Rootzertifikat neu generieren und das lokale Maschinen-SSL-Zertifikat sowie die lokalen Lösungsbenutzerzertifikate durch VMCA-signierte Zertifikate ersetzen. Bei Bereitstellungen mit mehreren Knoten führen Sie vSphere Certificate Manager mit dieser Option auf dem Platform Services Controller aus. Anschließend führen Sie dieses Dienstprogramm erneut auf allen anderen Knoten aus und wählen `Maschinen-SSL-Zertifikat durch VMCA-Zertifikat ersetzen` und `Lösungsbenutzerzertifikate durch VMCA-Zertifikate ersetzen` aus.

4 Festlegen von VMCA als Zwischenzertifizierungsstelle (Certificate Manager)

Sie können VMCA als Zwischenzertifizierungsstelle festlegen, indem Sie den Eingabeaufforderungen des Dienstprogramms Certificate Manager folgen. Nachdem Sie diesen Vorgang durchgeführt haben, signiert VMCA alle neuen Zertifikate mit der vollständigen Zertifikatskette. Wenn Sie möchten, können Sie Certificate Manager zum Ersetzen aller vorhandenen Zertifikate durch neue VMCA-signierte Zertifikate verwenden.

5 Ersetzen aller Zertifikate durch benutzerdefinierte Zertifikate (Certificate Manager)

Sie können das Dienstprogramm vSphere Certificate Manager verwenden, um alle Zertifikate durch benutzerdefinierte Zertifikate zu ersetzen. Bevor Sie den Vorgang starten, müssen Sie Zertifikatssignieranforderungen (CSRs) an Ihre Zertifizierungsstelle (CA) senden. Sie können Certificate Manager zum Generieren der CSRs verwenden.

Rückgängigmachen des zuletzt ausgeführten Vorgangs durch die erneute Veröffentlichung alter Zertifikate

Wenn Sie einen Zertifikatverwaltungsvorgang mithilfe von vSphere Certificate Manager durchführen, wird der aktuelle Zertifikatstatus im BACKUP_STORE-Speicher in VECS gespeichert, bevor Zertifikate ersetzt werden. Sie können den zuletzt ausgeführten Vorgang rückgängig machen und den vorherigen Status wiederherstellen.

Hinweis Beim Rückgängigmachen wird der im BACKUP_STORE gespeicherte Status wiederhergestellt. Wenn Sie vSphere Certificate Manager für zwei unterschiedliche Optionen ausführen und rückgängig zu machen versuchen, wird nur der letzte Vorgang rückgängig gemacht.

Alle Zertifikate zurücksetzen

Verwenden Sie die Option `Alle Zertifikate zurücksetzen`, wenn Sie alle vorhandenen vCenter-Zertifikate durch VMCA-signierte Zertifikate ersetzen möchten.

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

- Auf einem Platform Services Controller-Knoten kann vSphere Certificate Manager das Stammzertifikat neu generieren und das Maschinen-SSL-Zertifikat („machine“) und das Lösungsbenutzerzertifikat „machine“ ersetzen.
- Auf einem Verwaltungsknoten kann vSphere Certificate Manager das Maschinen-SSL-Zertifikat und alle Lösungsbenutzerzertifikate ersetzen.
- Bei einer eingebetteten Bereitstellung kann vSphere Certificate Manager alle Zertifikate ersetzen.

Welche Zertifikate ersetzt werden, hängt von den von Ihnen ausgewählten Optionen ab.

Neugenerieren eines neuen VMCA-Rootzertifikats und Ersetzen aller Zertifikate

Sie können das VMCA-Rootzertifikat neu generieren und das lokale Maschinen-SSL-Zertifikat sowie die lokalen Lösungsbenutzerzertifikate durch VMCA-signierte Zertifikate ersetzen. Bei Bereitstellungen mit mehreren Knoten führen Sie vSphere Certificate Manager mit dieser Option auf dem Platform Services Controller aus. Anschließend führen Sie dieses Dienstprogramm erneut auf allen anderen Knoten aus und wählen `Maschinen-SSL-Zertifikat` durch `VMCA-Zertifikat` ersetzen und `Lösungsbenutzerzertifikate` durch `VMCA-Zertifikate` ersetzen aus.

Bei der Ausführung dieses Befehls werden Sie von vSphere Certificate Manager aufgefordert, das Kennwort und Zertifikatsinformationen einzugeben. Alle Informationen mit Ausnahme des Kennworts werden in der Datei `certtool.cfg` gespeichert. Das Beenden von Diensten, das Ersetzen aller Zertifikate und das Neustarten von Prozessen erfolgt danach automatisch. Sie werden zur Eingabe der folgenden Informationen aufgefordert:

- Kennwort für „administrator@vsphere.local“.
- Aus zwei Buchstaben bestehender Ländercode
- Name des Unternehmens
- Organisationsname
- Organisationseinheit
- Zustand
- Ort
- IP-Adresse (optional)
- E-Mail
- Hostname, d. h., der vollqualifizierte Domänenname der Maschine, für die Sie das Zertifikat ersetzen möchten
- IP-Adresse des Platform Services Controller, falls Sie den Befehl auf einem Verwaltungsknoten ausführen

Voraussetzungen

Sie müssen den FQDN der Maschine kennen, für die Sie ein neues VMCA-signiertes Zertifikat generieren möchten. Für alle anderen Eigenschaften werden standardmäßig die vordefinierten Werte verwendet. Die IP-Adresse ist optional.

Nächste Schritte

Nach dem Ersetzen des Rootzertifikats bei einer Bereitstellung mit mehreren Knoten müssen Sie die Dienste für alle vCenter Server-Knoten mit externem Platform Services Controller neu starten.

Festlegen von VMCA als Zwischenzertifizierungsstelle (Certificate Manager)

Sie können VMCA als Zwischenzertifizierungsstelle festlegen, indem Sie den Eingabeaufforderungen des Dienstprogramms Certificate Manager folgen. Nachdem Sie diesen Vorgang durchgeführt haben, signiert VMCA alle neuen Zertifikate mit der vollständigen Zertifikatskette. Wenn Sie möchten, können Sie Certificate Manager zum Ersetzen aller vorhandenen Zertifikate durch neue VMCA-signierte Zertifikate verwenden.

Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats (Zwischenzertifizierungsstelle)

Mithilfe von vSphere Certificate Manager können Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) generiert werden. Übermitteln Sie diese CSRs zur Unterzeichnung an Ihre Unternehmenszertifizierungsstelle oder an eine externe Zertifizierungsstelle. Sie können die signierten Zertifikate mit den unterschiedlichen unterstützten Zertifikatersetzungsvorgängen verwenden.

- Sie können vSphere Certificate Manager zum Generieren der CSR verwenden.
- Wenn Sie die CSR manuell erstellen möchten, muss das Zertifikat, das Sie zum Signieren senden, die folgenden Anforderungen erfüllen.
 - Schlüsselgröße: mindestens 2.048 Bit
 - PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
 - x509 Version 3
 - Wenn Sie benutzerdefinierte Zertifikate verwenden, muss die Zertifizierungsstellenerweiterung für Stammzertifikate auf „true“ festgelegt werden, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.
 - CRL-Signatur muss aktiviert sein.
 - „Erweiterte Schlüsselverwendung“ darf keine Clientauthentifizierung oder Serverauthentifizierung enthalten.
 - Keine explizite Beschränkung der Zertifikatskettenlänge. VMCA verwendet den OpenSSL-Standardwert von 10 Zertifikaten.
 - Zertifikate mit Platzhalterzeichen oder mehr als einem DNS-Namen werden nicht unterstützt.
 - Untergeordnete Zertifizierungsstellen von VMCA können nicht erstellt werden.

Im VMware Knowledge Base-Artikel 2112009, „Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0“, finden Sie ein Beispiel für die Verwendung der Microsoft-Zertifizierungsstelle.

Voraussetzungen

vSphere Certificate Manager fordert Sie zur Eingabe von Informationen auf. Die Eingabeaufforderungen sind abhängig von Ihrer Umgebung und vom Zertifikatstyp, den Sie ersetzen möchten.

Beim Generieren von Zertifikatssignieranforderungen werden Sie generell aufgefordert, das Kennwort für den Benutzer „administrator@vsphere.local“ bzw. den Administrator für die vCenter Single Sign On-Domäne, mit der Sie eine Verbindung herstellen, einzugeben.

Verfahren

- 1 Starten Sie vSphere Certificate Manager und wählen Sie Option 2 aus.
Anfänglich verwenden Sie diese Option zum Generieren der CSR, nicht zum Ersetzen von Zertifikaten.
- 2 Geben Sie, wenn Sie dazu aufgefordert werden, das Kennwort sowie die IP-Adresse oder den Hostnamen für den Platform Services Controller ein.
- 3 Wählen Sie Option 1 aus, um die Zertifikatssignieranforderung zu generieren, und befolgen Sie die Anweisungen.
Im Rahmen dieses Vorgangs müssen Sie ein Verzeichnis angeben. Certificate Manager fügt das zu signierende Zertifikat (*.csr-Datei) und die entsprechende Schlüsseldatei (*.key-Datei) in das Verzeichnis ein.
- 4 Senden Sie das Zertifikat zur Unterzeichnung an die Unternehmenszertifizierungsstelle oder die externe Zertifizierungsstelle und legen Sie für die Datei folgenden Namen fest:
root_signing_cert.cer.
- 5 Kombinieren Sie in einem Texteditor die Zertifikate wie folgt.

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

- 6 Speichern Sie die Datei unter dem Namen root_signing_chain.cer.

Nächste Schritte

Ersetzen Sie das vorhandene Rootzertifikat durch das verkettete Rootzertifikat. Weitere Informationen hierzu finden Sie unter [Ersetzen des VMCA-Rootzertifikats durch benutzerdefiniertes Signierungszertifikat und Ersetzen aller Zertifikate](#).

Ersetzen des VMCA-Rootzertifikats durch benutzerdefiniertes Signierungszertifikat und Ersetzen aller Zertifikate

Das VMCA-Stammzertifikat können Sie durch ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat ersetzen, das VMCA als Zwischenzertifikat in der Zertifikatskette beinhaltet. In Zukunft beinhalten alle von VMCA generierten Zertifikate die Zertifikatskette.

vSphere Certificate Manager führen Sie für eine eingebettete Installation oder einen externen Platform Services Controller aus, um das VMCA-Rootzertifikat durch ein benutzerdefiniertes Signaturzertifikat zu ersetzen.

vSphere Certificate Manager fordert Sie zur Eingabe der folgenden Informationen auf:

Voraussetzungen

- Generieren Sie die Zertifikatsignieranforderung (Certificate Signing Request, CSR).
 - Sie können vSphere Certificate Manager zum Generieren der CSR verwenden. Siehe [Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats \(Zwischenzertifizierungsstelle\)](#).
 - Wenn Sie die CSR lieber manuell erstellen, muss das Zertifikat, das Sie zum Signieren senden, die folgenden Anforderungen erfüllen:
 - Schlüsselgröße: mindestens 2.048 Bit
 - PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
 - x509 Version 3
 - Wenn Sie benutzerdefinierte Zertifikate verwenden, muss die Zertifizierungsstellenerweiterung für Stammzertifikate auf „true“ festgelegt werden, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.
 - CRL-Signatur muss aktiviert sein.
 - „Erweiterte Schlüsselerwendung“ darf keine Clientauthentifizierung oder Serverauthentifizierung enthalten.
 - Keine explizite Beschränkung der Zertifikatskettenlänge. VMCA verwendet den OpenSSL-Standardwert von 10 Zertifikaten.
 - Zertifikate mit Platzhalterzeichen oder mehr als einem DNS-Namen werden nicht unterstützt.
 - Untergeordnete Zertifizierungsstellen von VMCA können nicht erstellt werden.
- Im VMware Knowledge Base-Artikel 2112009, „Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0“, finden Sie ein Beispiel für die Verwendung der Microsoft-Zertifizierungsstelle.

- Nachdem Sie das Zertifikat von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle erhalten haben, kombinieren Sie es mit dem anfänglichen VMCA-Stammzertifikat, um eine vollständige Zertifikatskette mit dem VMCA-Rootzertifikat im unteren Bereich zu erstellen. Siehe [Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats \(Zwischenzertifizierungsstelle\)](#).
- Sammeln Sie die erforderlichen Informationen.
 - Kennwort für „administrator@vsphere.local“.
 - Gültiges benutzerdefiniertes Zertifikat für Root (.crt-Datei).
 - Gültiger benutzerdefinierter Schlüssel für Root (.key-Datei).

Verfahren

- 1 Starten Sie vSphere Certificate Manager in einer eingebetteten Installation oder auf einem externen Platform Services Controller und wählen Sie Option 2 aus.
- 2 Wählen Sie Option 2 aus, um die Zertifikatsersetzung zu starten, und befolgen Sie die Anweisungen.
 - a Geben Sie, wenn Sie dazu aufgefordert werden, den vollständigen Pfad zum Stammzertifikat an.
 - b Falls Sie Zertifikate erstmalig ersetzen, werden Sie zur Eingabe von Informationen für das Maschinen-SSL-Zertifikat aufgefordert.

Diese Informationen beinhalten den erforderlichen FQDN der Maschine und werden in der Datei `certtool.cfg` gespeichert.
- 3 Falls Sie das Stammzertifikat für eine Bereitstellung mit mehreren Knoten ersetzen, müssen Sie die Dienste für alle vCenter Server-Instanzen neu starten.
- 4 Bei Bereitstellungen mit mehreren Knoten verwenden Sie für die Neugenerierung aller Zertifikate in jeder vCenter Server-Instanz die Optionen 3 (Maschinen-SSL-Zertifikat durch VMCA-Zertifikat ersetzen) und 6 (Lösungsbutzerzertifikate durch VMCA-Zertifikate ersetzen).

Beim Ersetzen der Zertifikate signiert VMCA mit der vollständigen Zertifikatskette.

Nächste Schritte

Abhängig von Ihrer Umgebung müssen Sie möglicherweise zusätzliche Zertifikate explizit ersetzen.

- Wenn die Unternehmensrichtlinien das Ersetzen aller Zertifikate verlangen, ersetzen Sie das vmdir-Rootzertifikat. Siehe [Ersetzen des VMware-Verzeichnisdienstzertifikats](#).
- Wenn Sie das Upgrade von einer vSphere 5.x-Umgebung aus vornehmen, müssen Sie möglicherweise das vCenter Single Sign On-Zertifikat innerhalb von vmdir ersetzen. Siehe [Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus](#).

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

In einer Bereitstellung mit mehreren Knoten, die VMCA als Zwischenzertifizierungsstelle verwendet, müssen Sie das Maschinen-SSL-Zertifikat explizit ersetzen. Zuerst ersetzen Sie das VMCA-Stammzertifikat auf dem Platform Services Controller-Knoten; dann können Sie die Zertifikate auf den vCenter Server-Knoten ersetzen, damit die Zertifikate in der gesamte Kette signiert sind. Sie können diese Option auch verwenden, um beschädigte oder in Kürze ablaufende Maschinen-SSL-Zertifikate zu ersetzen.

Wenn Sie das vorhandene Maschinen-SSL-Zertifikat durch ein neues VMCA-signiertes Zertifikat ersetzen, werden Sie von vSphere Certificate Manager zur Eingabe von Informationen aufgefordert. vSphere Certificate Manager gibt alle Werte mit Ausnahme des Kennworts und der IP-Adresse des Platform Services Controller in die Datei `certtool.cfg` ein.

- Kennwort für „administrator@vsphere.local“.
- Aus zwei Buchstaben bestehender Ländercode
- Name des Unternehmens
- Organisationsname
- Organisationseinheit
- Zustand
- Ort
- IP-Adresse (optional)
- E-Mail
- Hostname, d. h., der vollqualifizierte Domänenname der Maschine, für die Sie das Zertifikat ersetzen möchten. Wenn der Hostname nicht mit dem FQDN übereinstimmt, wird die Zertifikatersetzung nicht ordnungsgemäß abgeschlossen und Ihre Umgebung weist möglicherweise einen instabilen Status auf.
- IP-Adresse des Platform Services Controller, wenn Sie den Befehl auf einem Verwaltungsknoten ausführen

Voraussetzungen

- Starten Sie alle vCenter Server-Knoten explizit neu, falls Sie das VMCA-Stammzertifikat in einer Bereitstellung mit mehreren Knoten ersetzt haben.
- Sie müssen die folgenden Informationen kennen, um den Zertifikatsmanager mit dieser Option auszuführen.
 - Kennwort für „administrator@vsphere.local“.
 - Der FQDN der Maschine, für die Sie ein neues VMCA-signiertes Zertifikat generieren möchten. Für alle anderen Eigenschaften werden standardmäßig die vordefinierten Werte verwendet, die Sie jedoch ändern können.

- Hostname oder IP-Adresse des Platform Services Controller, falls Sie sich auf einem vCenter Server-System mit einem externen Platform Services Controller befinden.

Verfahren

1 Starten Sie vSphere Certificate Manager und wählen Sie Option 3 aus.

2 Beantworten Sie die Eingabeaufforderungen.

Certificate Manager speichert die Informationen in der Datei `certtool.cfg`.

Ergebnisse

vSphere Certificate Manager ersetzt das Maschinen-SSL-Zertifikat.

Ersetzen der Lösungsbenutzerzertifikate durch VMCA-Zertifikate (Zwischenzertifizierungsstelle)

Bei einem Mehrfachknoten, der VMCA als Zwischenzertifizierungsstelle verwendet, müssen Sie die Lösungsbenutzerzertifikate explizit ersetzen. Zuerst ersetzen Sie das VMCA-Stammzertifikat auf dem Platform Services Controller-Knoten; dann können Sie die Zertifikate auf den vCenter Server-Knoten ersetzen, damit die Zertifikate in der gesamte Kette signiert sind. Sie können diese Option auch verwenden, um Lösungsbenutzerzertifikate zu ersetzen, die beschädigt sind oder im Begriff sind abzulaufen.

Voraussetzungen

- Starten Sie alle vCenter Server-Knoten explizit neu, falls Sie das VMCA-Stammzertifikat in einer Bereitstellung mit mehreren Knoten ersetzt haben.
- Sie müssen die folgenden Informationen kennen, um den Zertifikatsmanager mit dieser Option auszuführen.
 - Kennwort für „administrator@vsphere.local“.
 - Hostname oder IP-Adresse des Platform Services Controller, falls Sie sich auf einem vCenter Server-System mit einem externen Platform Services Controller befinden.

Verfahren

1 Starten Sie vSphere Certificate Manager und wählen Sie Option 6 aus.

2 Beantworten Sie die Eingabeaufforderungen.

Ergebnisse

vSphere Certificate Manager ersetzt alle Lösungsbenutzerzertifikate.

Ersetzen aller Zertifikate durch benutzerdefinierte Zertifikate (Certificate Manager)

Sie können das Dienstprogramm vSphere Certificate Manager verwenden, um alle Zertifikate durch benutzerdefinierte Zertifikate zu ersetzen. Bevor Sie den Vorgang starten, müssen Sie

Zertifikatssignieranforderungen (CSRs) an Ihre Zertifizierungsstelle (CA) senden. Sie können Certificate Manager zum Generieren der CSRs verwenden.

Eine Option besteht darin, nur das Maschinen-SSL-Zertifikat zu ersetzen und die durch VMCA bereitgestellten Lösungsbenutzerzertifikate zu verwenden. Lösungsbenutzerzertifikate werden nur für die Kommunikation zwischen vSphere-Komponenten verwendet.

Wenn Sie benutzerdefinierte Zertifikate verwenden, sind Sie dafür verantwortlich, dass Sie jedem zu Ihrer Umgebung hinzugefügten Knoten benutzerdefinierte Zertifikate zur Verfügung stellen. VMCA stellt noch immer VMCA-signierte Zertifikate zur Verfügung, und Sie sind für das Ersetzen dieser Zertifikate verantwortlich. Sie können das Dienstprogramm vSphere Certificate Manager oder aber Befehlszeilenschnittstellen für die manuelle Zertifikatsersetzung verwenden. Zertifikate werden in VECS gespeichert.

Generieren von Zertifikatssignieranforderungen mit vSphere Certificate Manager (benutzerdefinierte Zertifikate)

Mithilfe von vSphere Certificate Manager können Sie Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) generieren, die Sie anschließend mit Ihrer Unternehmenszertifizierungsstelle verwenden oder an eine externe Zertifizierungsstelle senden können. Sie können die Zertifikate mit den unterschiedlichen unterstützten Ersetzungsvorgängen von Zertifikaten verwenden.

Sie können das Certificate Manager-Tool wie folgt über die Befehlszeile ausführen:

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

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

Voraussetzungen

vSphere Certificate Manager fordert Sie zur Eingabe von Informationen auf. Die Eingabeaufforderungen sind abhängig von Ihrer Umgebung und vom Zertifikatstyp, den Sie ersetzen möchten.

- Beim Generieren von Zertifikatssignieranforderungen werden Sie generell aufgefordert, das Kennwort für den Benutzer „administrator@vsphere.local“ bzw. den Administrator für die vCenter Single Sign On-Domäne, mit der Sie eine Verbindung herstellen, einzugeben.
- Wenn Sie eine Zertifikatssignieranforderung in einer Umgebung mit einem externen Platform Services Controller generieren, werden Sie zur Eingabe des Hostnamens oder der IP-Adresse für den Platform Services Controller aufgefordert.

- Zum Generieren einer Zertifikatssignieranforderung für ein Maschinen-SSL-Zertifikat werden Sie zur Eingabe von Zertifikateigenschaften aufgefordert, die in der Datei `certtool.cfg` gespeichert sind. Für die meisten Felder können Sie den Standardwert übernehmen oder aber standortspezifische Werte eingeben. Der FQDN der Maschine ist erforderlich.

Verfahren

- 1 Starten Sie vSphere Certificate Manager auf jeder Maschine in Ihrer Umgebung und wählen Sie Option 1 aus.
- 2 Geben Sie, wenn Sie dazu aufgefordert werden, das Kennwort sowie die IP-Adresse oder den Hostnamen für den Platform Services Controller ein.
- 3 Wählen Sie Option 1 aus, um die Zertifikatssignieranforderung zu generieren, befolgen Sie die Anweisungen und beenden Sie Certificate Manager.

Im Rahmen dieses Vorgangs müssen Sie ein Verzeichnis angeben. Certificate Manager speichert die Zertifikats- und Schlüsseldateien in dem Verzeichnis.

- 4 Wenn Sie alle Lösungsbenutzerzertifikate ersetzen möchten, starten Sie Certificate Manager neu.
- 5 Wählen Sie Option 5 aus.
- 6 Geben Sie, wenn Sie dazu aufgefordert werden, das Kennwort sowie die IP-Adresse oder den Hostnamen für den Platform Services Controller ein.
- 7 Wählen Sie Option 1 aus, um die Zertifikatssignieranforderungen zu generieren, befolgen Sie die Anweisungen und beenden Sie Certificate Manager.

Im Rahmen dieses Vorgangs müssen Sie ein Verzeichnis angeben. Certificate Manager speichert die Zertifikats- und Schlüsseldateien in dem Verzeichnis.

Certificate Manager generiert auf jedem Platform Services Controller-Knoten je ein Zertifikats- und Schlüsselpaar. Certificate Manager generiert auf jedem vCenter Server-Knoten je vier Zertifikats- und Schlüsselpaare.

Nächste Schritte

Führen Sie die Zertifikatsersetzung durch.

Ersetzen des Maschinen-SSL-Zertifikats durch ein benutzerdefiniertes Zertifikat

Das Maschinen-SSL-Zertifikat wird vom Reverse-Proxy-Dienst für jeden Verwaltungsknoten, Platform Services Controller und jede eingebettete Bereitstellung verwendet. Für jede Maschine ist ein Maschinen-SSL-Zertifikat für die sichere Kommunikation mit anderen Diensten erforderlich. Sie können dieses Zertifikat für jeden Knoten durch ein benutzerdefiniertes Zertifikat ersetzen.

Voraussetzungen

Bevor Sie beginnen, benötigen Sie eine Zertifikatssignieranforderung (CSR) für jede Maschine in Ihrer Umgebung. Sie können die CSR mit vSphere Certificate Manager oder explizit generieren.

- 1 Weitere Informationen zum Generieren einer CSR mit vSphere Certificate Manager finden Sie unter [Generieren von Zertifikatssignieranforderungen mit vSphere Certificate Manager \(benutzerdefinierte Zertifikate\)](#).
- 2 Um die CSR explizit zu generieren, fordern Sie für jede Maschine ein Zertifikat von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle an. Das Zertifikat muss die folgenden Anforderungen erfüllen:
 - Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
 - CRT-Format
 - x509 Version 3
 - „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten
 - Enthält die folgenden Schlüsselverwendungen: Digitale Signatur, Unleugbarkeit, Schlüsselverschlüsselung

Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel [2112014, Beziehen von vSphere-Zertifikaten von einer Microsoft-Zertifizierungsstelle](#).

Verfahren

- 1 Starten Sie vSphere Certificate Manager und wählen Sie Option 1 aus.
- 2 Wählen Sie Option 2 aus, um die Zertifikatsersetzung zu starten, und befolgen Sie die Anweisungen.

vSphere Certificate Manager fordert Sie zur Eingabe der folgenden Informationen auf:

- Kennwort für „administrator@vsphere.local“.
- Gültiges benutzerdefiniertes Maschinen-SSL-Zertifikat (.crt-Datei).
- Gültiger benutzerdefinierter Maschinen-SSL-Schlüssel (.key-Datei).
- Gültiges Signaturzertifikat für das benutzerdefinierte Maschinen-SSL-Zertifikat (.crt-Datei).
- Die IP-Adresse des Platform Services Controller, wenn Sie den Befehl für einen Verwaltungsknoten in einer Bereitstellung mit mehreren Knoten ausführen.

Nächste Schritte

Abhängig von Ihrer Umgebung müssen Sie möglicherweise zusätzliche Zertifikate explizit ersetzen.

- Wenn die Unternehmensrichtlinien das Ersetzen aller Zertifikate verlangen, ersetzen Sie das vmdir-Rootzertifikat. Siehe [Ersetzen des VMware-Verzeichnisdienstzertifikats](#).

- Wenn Sie das Upgrade von einer vSphere 5.x-Umgebung aus vornehmen, müssen Sie möglicherweise das vCenter Single Sign On-Zertifikat innerhalb von vmdir ersetzen. Siehe [Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus](#).

Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate

Viele Unternehmen möchten lediglich Zertifikate zu Diensten ersetzen lassen, die extern zugänglich sind. Certificate Manager unterstützt jedoch auch das Ersetzen von Lösungsbenutzerzertifikaten. Lösungsbenutzer sind Sammlungen von Diensten. So ersetzen beispielsweise alle mit dem vSphere Web Client verbundene Dienste in Bereitstellungen mit mehreren Knoten das Lösungsbenutzerzertifikat „machine“ im Platform Services Controller sowie sämtliche Lösungsbenutzer auf allen Verwaltungsknoten.

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

Das Format sollte so oder ähnlich aussehen:

```
-----BEGIN CERTIFICATE-----
Signing certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

Voraussetzungen

Bevor Sie beginnen, benötigen Sie eine Zertifikatssignieranforderung (CSR) für jede Maschine in Ihrer Umgebung. Sie können die CSR mit vSphere Certificate Manager oder explizit generieren.

- 1 Weitere Informationen zum Generieren einer CSR mit vSphere Certificate Manager finden Sie unter [Generieren von Zertifikatssignieranforderungen mit vSphere Certificate Manager \(benutzerdefinierte Zertifikate\)](#).
- 2 Fordern Sie von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle ein Zertifikat für jeden Benutzer der Lösung auf jedem Knoten an. Sie können die CSR mit vSphere Certificate Manager oder selbst generieren. DIE CSR muss die folgenden Anforderungen erfüllen:
 - Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
 - CRT-Format
 - x509 Version 3
 - „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten
 - Für jedes Lösungsbenutzerzertifikat ist ein unterschiedlicher Wert für `Subject` erforderlich. Geben Sie beispielsweise den Lösungsbenutzernamen (z. B. vpxd) oder einen anderen eindeutigen Bezeichner an.

- Enthält die folgenden Schlüsselverwendungen: Digitale Signatur, Unleugbarkeit, Schlüsselverschlüsselung

Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel [2112014](#), [Beziehen von vSphere-Zertifikaten von einer Microsoft-Zertifizierungsstelle](#).

Verfahren

- 1 Starten Sie vSphere Certificate Manager und wählen Sie Option 5 aus.
- 2 Wählen Sie Option 2 aus, um die Zertifikatsersetzung zu starten, und befolgen Sie die Anweisungen.

vSphere Certificate Manager fordert Sie zur Eingabe der folgenden Informationen auf:

- Kennwort für „administrator@vsphere.local“.
- Zertifikat und Schlüssel für Lösungsbenutzer „machine“.
- Wenn Sie vSphere Certificate Manager für einen Platform Services Controller-Knoten ausführen, werden Sie zur Eingabe des Zertifikats und des Schlüssels (`vpzd.crt` und `vpzd.key`) für den Lösungsbenutzer „machine“ aufgefordert.
- Wenn Sie vSphere Certificate Manager für einen Verwaltungsknoten oder eine eingebettete Bereitstellung ausführen, werden Sie zur Eingabe aller Zertifikate und Schlüssel (`vpzd.crt` und `vpzd.key`) für alle Lösungsbenutzer aufgefordert.

Nächste Schritte

Wenn Sie das Upgrade von einer vSphere 5.x-Umgebung aus vornehmen, müssen Sie möglicherweise das vCenter Single Sign On-Zertifikat innerhalb von `vmdir` ersetzen. Weitere Informationen hierzu finden Sie unter [Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus](#).

Manuelle Zertifikatsersetzung

Es kann vorkommen, dass Sie nur einen Lösungsbenutzerzertifikatstyp ersetzen möchten und deshalb nicht das Dienstprogramm vSphere Certificate Manager verwenden können. In diesem Fall verwenden Sie die Befehlszeilenschnittstellen (CLIs) Ihrer Installation zum Ersetzen von Zertifikaten.

Grundlegende Informationen zum Starten und Stoppen von Diensten

Für bestimmte Bereiche der manuellen Zertifikatsersetzung müssen Sie alle Dienste beenden und dann nur jene Dienste starten, die die Zertifikatinfrastruktur verwalten. Wenn Sie Dienste nur bei Bedarf beenden, können Sie die Ausfallzeit minimieren.

Halten Sie sich an die folgenden Faustregeln.

- Beenden Sie die Dienste nicht, um neue öffentliche/private Schlüsselpaare oder neue Zertifikate zu generieren.

- Wenn Sie der einzige Administrator sind, müssen Sie die Dienste beim Hinzufügen eines neuen Stammzertifikats nicht beenden. Das alte Stammzertifikat bleibt verfügbar, und alle Dienste können weiterhin mit diesem Zertifikat authentifiziert werden. Beenden Sie alle Dienste und starten Sie sie sofort neu, nachdem Sie das Stammzertifikat hinzugefügt haben, um Probleme mit Ihren Hosts zu vermeiden.
- Wenn es in Ihrer Umgebung mehrere Administratoren gibt, beenden Sie die Dienste, bevor Sie ein neues Stammzertifikat hinzufügen, und starten Sie die Dienste neu, nachdem Sie ein neues Zertifikat hinzugefügt haben.
- Beenden Sie die Dienste, bevor Sie die folgenden Aufgaben ausführen:
 - Löschen Sie ein Maschinen-SSL-Zertifikat bzw. jedes Lösungsbenutzerzertifikat in VECS.
 - Ersetzen Sie ein Lösungsbenutzerzertifikat im VMware-Verzeichnisdienst (vmdir).

Ersetzen vorhandener VMCA-signierter Zertifikate durch neue VMCA-signierte Zertifikate

Wenn das VMCA-Rootzertifikat in naher Zukunft abläuft oder wenn Sie es aus anderen Gründen ersetzen möchten, können Sie ein neues Rootzertifikat generieren und zum VMware-Verzeichnisdienst hinzufügen. Anschließend können Sie neue Maschinen-SSL-Zertifikate und Lösungsbenutzerzertifikate mithilfe des neuen Rootzertifikats generieren.

In den meisten Fällen können Sie das Dienstprogramm vSphere Certificate Manager zum Ersetzen von Zertifikaten verwenden.

Für die detailliertere Kontrolle finden Sie in diesem Szenario ausführliche schrittweise Anleitungen zum Ersetzen aller Zertifikate mithilfe von CLI-Befehlen. Mit der Vorgehensweise für die entsprechende Aufgabe können Sie stattdessen auch nur einzelne Zertifikate ersetzen.

Voraussetzungen

Nur „administrator@vsphere.local“ oder andere Benutzer in der Gruppe „CAAdmins“ können Zertifikatverwaltungsaufgaben durchführen. Siehe [Hinzufügen von Mitgliedern zu einer vCenter Single Sign On-Gruppe](#).

Verfahren

1 Generieren eines neuen VMCA-signierten Stammzertifikats

Neue VMCA-signierte Zertifikate erstellen Sie mit der `certool`-Befehlszeilenschnittstelle (CLI) und veröffentlichen sie in vmdir.

2 Ersetzen der Maschinen-SSL-Zertifikate durch VMCA-signierte Zertifikate

Nachdem Sie ein neues VMCA-signiertes Rootzertifikat generiert haben, können Sie alle Maschinen-SSL-Zertifikate in Ihrer Umgebung ersetzen.

3 Ersetzen der Lösungsbenutzerzertifikate durch neue VMCA-signierte Stammzertifikate

Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie alle Lösungsbenutzerzertifikate ersetzen. Lösungsbenutzerzertifikate müssen gültig sein (also nicht abgelaufen), aber die anderen Informationen des Zertifikats werden nicht von der Zertifikatsinfrastruktur verwendet.

4 Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

Generieren eines neuen VMCA-signierten Stammzertifikats

Neue VMCA-signierte Zertifikate erstellen Sie mit der `certtool`-Befehlszeilenschnittstelle (CLI) und veröffentlichen sie in `vmdir`.

Bei einer Bereitstellung mit mehreren Knoten führen Sie Befehle zum Generieren von Stammzertifikaten im Platform Services Controller aus.

Verfahren

- 1 Generieren Sie ein neues selbstsigniertes Zertifikat und einen privaten Schlüssel.

```
certtool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config <config_file>
```

- 2 Ersetzen Sie das vorhandene Stammzertifikat durch das neue Zertifikat.

```
certtool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

Mit diesem Befehl wird das Zertifikat generiert und zu `vmdir` sowie zu VECS hinzugefügt.

- 3 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

- 4 (Optional) Veröffentlichen Sie das neue Stammzertifikat in vmdir.

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

Wenn Sie diesen Befehl ausführen, werden alle vmdir-Instanzen sofort aktualisiert. Andernfalls kann die Weitergabe an alle Instanzen eine Weile dauern.

- 5 Starten Sie alle Dienste neu.

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

Beispiel: Generieren eines neuen VMCA-signierten Stammzertifikats

Das folgende Beispiel veranschaulicht alle Schritte, um die Informationen zur aktuellen Stammzertifizierungsstelle zu überprüfen und das Stammzertifikat neu zu generieren.

- 1 (Optional) Listen Sie das VMCA-Stammzertifikat auf, um sicherzustellen, dass es sich im Zertifikatspeicher befindet.

- In einem Platform Services Controller-Knoten oder einer eingebetteten Installation:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca
```

- In einem Verwaltungsknoten (externe Installation):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca --server=<psc-
ip-or-fqdn>
```

Die Ausgabe sieht so oder ähnlich aus:

```
output:
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      cf:2d:ff:49:88:50:e5:af
    ...
```

- 2 (Optional) Listen Sie den VECS TRUSTED_ROOTS-Speicher auf und vergleichen Sie die Seriennummer des Zertifikats mit der Ausgabe aus Schritt 1.

Dieser Befehl kann sowohl für Platform Services Controller als auch für Verwaltungsknoten verwendet werden, da VECS eine Abfrage für vmdir ausführt.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry list --store TRUSTED_ROOTS
--text
```

Im einfachsten Fall mit nur einem Stammzertifikat sieht die Ausgabe wie folgt aus:

```
Number of entries in store :    1
Alias : 960d43f31eb95211ba3a2487ac840645a02894bd
Entry type :    Trusted Cert
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      cf:2d:ff:49:88:50:e5:af
```

- 3 Generieren Sie ein neues VMCA-Stammzertifikat. Das Zertifikat wird zum TRUSTED_ROOTS-Speicher in VECS und im VMware-Verzeichnisdienst (vmdir) hinzugefügt.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program
Files\VMware\vCenter Server\vmcad\certool.cfg"
```

Unter Windows ist `--config` optional, da der Befehl die Standarddatei `certool.cfg` verwendet.

Ersetzen der Maschinen-SSL-Zertifikate durch VMCA-signierte Zertifikate

Nachdem Sie ein neues VMCA-signiertes Rootzertifikat generiert haben, können Sie alle Maschinen-SSL-Zertifikate in Ihrer Umgebung ersetzen.

Für jede Maschine ist ein Maschinen-SSL-Zertifikat für die sichere Kommunikation mit anderen Diensten erforderlich. Bei einer Bereitstellung mit mehreren Knoten müssen Sie die Befehle zum Generieren von Maschinen-SSL-Zertifikaten auf jedem Knoten ausführen. Verwenden Sie den Parameter `--server`, um von einem vCenter Server mit externem Platform Services Controller aus auf den Platform Services Controller zu verweisen.

Voraussetzungen

Sie sollten darauf vorbereitet sein, alle Dienste zu beenden und die Dienste für die Weitergabe und Speicherung von Zertifikaten zu starten.

Verfahren

- 1 Erstellen Sie eine Kopie von `certtool.cfg` für jede Maschine, für die ein neues Zertifikat erforderlich ist.

`certtool.cfg` finden Sie in den folgenden Speicherorten:

Betriebssystem	Pfad
Windows	C:\Program Files\VMware\vCenter Server\vmcad
Linux	/usr/lib/vmware-vmca/share/config/

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

Führen Sie `NSLookup` für die IP-Adresse der Maschine aus, um die DNS-Liste für den Namen anzuzeigen, und verwenden Sie diesen Namen für das Feld „Hostname“ in der Datei.

- 3 Generieren Sie für jede Datei ein öffentliches/privates Schlüsselpaar sowie ein Zertifikat und übergeben Sie die Konfigurationsdatei, die Sie soeben angepasst haben.

Beispiel:

```
certtool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certtool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --
config machine1.cfg
```

- 4 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Fügen Sie VECS das neue Zertifikat hinzu.

Alle Maschinen benötigen das neue Zertifikat im lokalen Zertifikatspeicher für die Kommunikation über SSL. Zunächst löschen Sie den vorhandenen Eintrag und fügen dann den neuen Eintrag hinzu.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

6 Starten Sie alle Dienste neu.

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

Beispiel: Ersetzen der Maschinenzertifikate durch VMCA-signierte Zertifikate

- 1 Erstellen Sie eine Konfigurationsdatei für das SSL-Zertifikat und speichern Sie sie unter dem Namen `ssl-config.cfg` im aktuellen Verzeichnis.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

- 2 Generieren Sie ein Schlüsselpaar für das Maschinen-SSL-Zertifikat. Führen Sie diesen Befehl auf jedem Verwaltungsknoten und Platform Services Controller-Knoten aus. Die Option `--server` ist dabei nicht erforderlich.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

Die Dateien `ssl-key.priv` und `ssl-key.pub` werden im aktuellen Verzeichnis erstellt.

- 3 Generieren Sie das neue Maschinen-SSL-Zertifikat. Dieses Zertifikat ist VMCA-signiert. Falls Sie das VMCA-Rootzertifikat durch ein benutzerdefiniertes Zertifikat ersetzt haben, signiert VMCA alle Zertifikate mit der vollständigen Zertifikatskette.

- In einem Platform Services Controller-Knoten oder einer eingebetteten Installation:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- Auf einem vCenter Server (externe Installation):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

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

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

```
"C:\Program Files\VMware\VMware vCenter Server\vmaddd\vecs-cli store list
```

- Ausgabe auf Platform Services Controller:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Ausgabe auf vCenter Server:

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

5 Ersetzen Sie das Maschinen-SSL-Zertifikat in VECS durch das neue Maschinen-SSL-Zertifikat. Die Werte `--store` und `--alias` müssen genau mit den Standardnamen übereinstimmen.

- Führen Sie auf dem Platform Services Controller den folgenden Befehl aus, um das Maschinen-SSL-Zertifikat im MACHINE_SSL_CERT-Speicher zu aktualisieren.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmaddd\vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmaddd\vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- Führen Sie auf jedem Verwaltungsknoten oder für jede eingebettete Bereitstellung den folgenden Befehl aus, um das Maschinen-SSL-Zertifikat im MACHINE_SSL_CERT-Speicher zu aktualisieren. Sie müssen das Zertifikat für jede Maschine separat aktualisieren, da jedes Zertifikat einen unterschiedlichen FQDN aufweist.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmaddd\vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmaddd\vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Nächste Schritte

Sie können auch die Zertifikate für Ihre ESXi-Hosts ersetzen. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

Nach dem Ersetzen des Rootzertifikats bei einer Bereitstellung mit mehreren Knoten müssen Sie die Dienste für alle vCenter Server-Knoten mit externem Platform Services Controller neu starten.

Ersetzen der Lösungsbenutzerzertifikate durch neue VMCA-signierte Stammzertifikate

Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie alle Lösungsbenutzerzertifikate ersetzen. Lösungsbenutzerzertifikate müssen gültig sein (also nicht abgelaufen), aber die anderen Informationen des Zertifikats werden nicht von der Zertifikatinfrastruktur verwendet.

Sie ersetzen das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten und auf jedem Platform Services Controller-Knoten. Die anderen Lösungsbenutzerzertifikate ersetzen Sie nur auf jedem Verwaltungsknoten. Verwenden Sie den Parameter `--server`, um auf den Platform Services Controller zu verweisen, wenn Sie Befehle auf einem Verwaltungsknoten mit einem externen Platform Services Controller ausführen.

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

Voraussetzungen

Sie sollten darauf vorbereitet sein, alle Dienste zu beenden und die Dienste für die Weitergabe und Speicherung von Zertifikaten zu starten.

Verfahren

- 1 Erstellen Sie eine Kopie von `certtool.cfg`, entfernen Sie die Felder für den Namen, die IP-Adresse, den DNS-Namen und die E-Mail-Adresse und benennen Sie die Datei z. B. in `sol_usr.cfg` um.

Sie können die Zertifikate im Rahmen des Generierungsvorgangs über die Befehlszeile benennen. Die restlichen Informationen sind für Lösungsbenutzer nicht erforderlich. Wenn Sie die Standardinformationen unverändert lassen, könnten die generierten Zertifikate für Verwirrung sorgen.

- 2 Generieren Sie für jeden Lösungsbenutzer ein öffentliches/privates Schlüsselpaar sowie ein Zertifikat und übergeben Sie die Konfigurationsdatei, die Sie soeben angepasst haben.

Beispiel:

```
certtool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certtool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

- 3 Suchen Sie den Namen für jeden Lösungsbenutzer.

```
dir-cli service list
```

Sie können die eindeutige ID verwenden, die beim Ersetzen der Zertifikate zurückgegeben wird. Die Ein- und Ausgabe könnte so oder ähnlich wie im Folgenden aussehen.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

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

- 4 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

- 5 Ersetzen Sie für jeden Lösungsbenutzer das vorhandene Zertifikat in `vmdir` und anschließend in `VECS`.

Das folgende Beispiel veranschaulicht, wie die Zertifikate für den `vpxd`-Dienst ersetzt werden.

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

Hinweis Lösungsbenutzer können sich nur bei vCenter Single Sign On authentifizieren, wenn Sie das Zertifikat in `vmdir` ersetzen.

- 6 Starten Sie alle Dienste neu.

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

Beispiel: Verwenden von VMCA-signierten Lösungsbenutzerzertifikaten

- 1 Generieren Sie für jeden Lösungsbenutzer ein öffentliches/privates Schlüsselpaar. Dies beinhaltet ein Schlüsselpaar für den Lösungsbenutzer „machine“ auf jedem Platform Services Controller und jedem Verwaltungsknoten sowie ein Schlüsselpaar für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient) auf jedem Verwaltungsknoten.

- a Generieren Sie für den Lösungsbenutzer „machine“ einer eingebetteten Bereitstellung oder für den Lösungsbenutzer „machine“ des Platform Services Controller ein Schlüsselpaar.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- b (Optional) Generieren Sie für Bereitstellungen mit einem externen Platform Services Controller für den Lösungsbenutzer „machine“ ein Schlüsselpaar auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- c Generieren Sie für den vpxd-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

- d Generieren Sie für den vpxd-extension-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

- e Generieren Sie für den vsphere-webclient-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```


- 2 Generieren Sie vom neuen VMCA-Rootzertifikat signierte Lösungsbenutzerzertifikate für den Lösungsbenutzer „machine“ auf jedem Platform Services Controller und jedem Verwaltungsknoten sowie für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient) auf jedem Verwaltungsknoten.

Hinweis Der Parameter `--Name` muss eindeutig sein. Durch die Angabe des Namens des Lösungsbenutzerspeichers (z. B. vpxd oder vpxd-extension) ist auf einfache Weise erkennbar, welches Zertifikat welchem Lösungsbenutzer zugeordnet ist.

- a Führen Sie den folgenden Befehl auf dem Platform Services Controller-Knoten aus, um für den Lösungsbenutzer „machine“ auf diesem Knoten ein Lösungsbenutzerzertifikat zu generieren.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

- c Generieren Sie für den vpxd-Lösungsbenutzer auf jedem Verwaltungsknoten ein Zertifikat.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

- d Generieren Sie für den vpxd-extensions-Lösungsbenutzer auf jedem Verwaltungsknoten ein Zertifikat.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

- 3 Ersetzen Sie die Lösungsbenutzerzertifikate in VECS durch die neuen Lösungsbenutzerzertifikate.

Hinweis Die Parameter `--store` und `--alias` müssen genau mit den Standardnamen für die Dienste übereinstimmen.

- a Führen Sie auf dem Platform Services Controller-Knoten den folgenden Befehl aus, um das Lösungsbenutzerzertifikat „machine“ zu ersetzen:

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b Ersetzen Sie das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten:

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c Ersetzen Sie das vpxd-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

- d Ersetzen Sie das vpxd-extension-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

- e Ersetzen Sie das vsphere-webclient-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

- 4 Aktualisieren Sie den VMware-Verzeichnisdienst (vmdir) mit den neuen Lösungsbenutzerzertifikaten. Sie werden zur Eingabe eines vCenter Single Sign On-Administratorkennworts aufgefordert.
- a Führen Sie `dir-cli service list` aus, um für jeden Lösungsbenutzer das eindeutige Dienst-ID-Suffix abzurufen. Sie können diesen Befehl auf einem Platform Services Controller oder für ein vCenter Server-System ausführen.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

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

- b Ersetzen Sie das Maschinenzertifikat in vmdir auf dem Platform Services Controller. Wenn beispielsweise „machine-29a45d00-60a7-11e4-96ff-00505689639a“ der Lösungsbenutzer „machine“ auf dem Platform Services Controller ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

- c Ersetzen Sie das Maschinenzertifikat in vmdir auf jedem Verwaltungsknoten. Wenn beispielsweise „machine-6fd7f140-60a9-11e4-9e28-005056895a69“ der Lösungsbenutzer „machine“ auf dem vCenter Server ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

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

```
C:\>"C:\Program Files\VMware\VCenter Server\vmadd\dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

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

```
C:\>"C:\Program Files\VMware\VCenter Server\vmadd\dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

Nächste Schritte

Starten Sie alle Dienste auf jedem Platform Services Controller-Knoten und jedem Verwaltungsknoten neu.

Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

Das SSL-Zertifikat des VMware Directory Service wird von vmdir für Handshakes zwischen Platform Services Controller-Knoten verwendet, die die vCenter Single Sign On-Replizierung durchführen.

Diese Schritte sind für Umgebungen im gemischten Modus, die Knoten mit vSphere 6.0 und vSphere 6.5 enthalten, nicht erforderlich. Diese Schritte sind nur in folgenden Fällen erforderlich:

- In Ihrer Umgebung sind sowohl vCenter Single Sign On 5.5- als auch vCenter Single Sign On 6.x-Dienste vorhanden.
- Die vCenter Single Sign On-Dienste sind für die Replizierung von vmdir-Daten eingerichtet.
- Sie können die standardmäßigen VMCA-signierten Zertifikate für den Knoten, auf dem der vCenter Single Sign On 6.x-Dienst ausgeführt wird, durch benutzerdefinierte Zertifikate ersetzen.

Hinweis Es empfiehlt sich, vor dem Neustart der Dienste ein Upgrade der kompletten Umgebung durchzuführen. Vom Ersetzen des VMware Directory Service-Zertifikats wird in der Regel abgeraten.

Verfahren

- 1 Ersetzen Sie auf dem Knoten, auf dem der vCenter Single Sign On 6.x-Dienst ausgeführt wird, das vmdird-SSL-Zertifikat und den Schlüssel.

Weitere Informationen hierzu finden Sie unter [Ersetzen des VMware-Verzeichnisdienstzertifikats](#).

- 2 Richten Sie auf dem Knoten, auf dem der vCenter Single Sign On 5.5-Dienst ausgeführt wird, die Umgebung so ein, dass der vCenter Single Sign On 6.x-Dienst bekannt ist.
 - a Sichern Sie alle Dateien im Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmldird`.
 - b Erstellen Sie eine Kopie der Datei `vmldircert.pem` auf dem Knoten der Version 6.x und benennen Sie sie in `<sso_node2.domain.com>.pem` um, wobei `<sso_node2.domain.com>` der FQDN des Knotens der Version 6.x ist.
 - c Kopieren Sie das umbenannte Zertifikat in das Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmldird`, um das vorhandene Replizierungszertifikat zu ersetzen.

- 3 Starten Sie den VMware Directory Service auf allen Maschinen neu, auf denen Sie Zertifikate ersetzt haben.

Sie können den Dienst über den vSphere Web Client oder mithilfe des Befehls `service-control` neu starten.

Verwenden von VMCA als Zwischenzertifizierungsstelle

Das VMCA-Rootzertifikat können Sie durch ein von einer Zertifizierungsstelle (CA) signiertes Drittanbieterzertifikat ersetzen, das VMCA in der Zertifikatskette beinhaltet. In Zukunft beinhalten alle von VMCA generierten Zertifikate die Zertifikatskette. Vorhandene Zertifikate können Sie durch neu generierte Zertifikate ersetzen. Diese Vorgehensweise kombiniert die Sicherheit eines von einer Zertifizierungsstelle signierten Drittanbieterzertifikats mit der Bequemlichkeit der automatisierten Zertifikatsverwaltung.

Verfahren

- 1 [Ersetzen des Rootzertifikats \(Zwischenzertifizierungsstelle\)](#)

Der erste Schritt beim Ersetzen des VMCA-Zertifikats durch benutzerdefinierte Zertifikate besteht im Generieren einer Zertifikatsignieranforderung (Certificate Signing Request, CSR) und im Hinzufügen des Zertifikats, das als Root-Zertifikat an VMCA zurückgesendet wird.

- 2 [Ersetzen der Maschinen-SSL-Zertifikate \(Zwischenzertifizierungsstelle\)](#)

Nachdem Sie das signierte Zertifikat von der Zertifizierungsstelle erhalten und zum VMCA-Rootzertifikat gemacht haben, können Sie alle Maschinen-SSL-Zertifikate ersetzen.

- 3 [Ersetzen der Lösungsbenutzerzertifikate \(Zwischenzertifizierungsstelle\)](#)

Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie die Lösungsbenutzerzertifikate ersetzen.

4 Ersetzen des VMware-Verzeichnisdienstzertifikats

Wenn Sie ein neues VMCA-Root-Zertifikat verwenden möchten und die Veröffentlichung des VMCA-Root-Zertifikats, das bei der Bereitstellung Ihrer Umgebung verwendet wurde, rückgängig machen, müssen Sie die Maschinen-SSL-Zertifikate, Lösungsbenutzerzertifikate und Zertifikate für bestimmte interne Dienste ersetzen.

5 Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

Ersetzen des Rootzertifikats (Zwischenzertifizierungsstelle)

Der erste Schritt beim Ersetzen des VMCA-Zertifikats durch benutzerdefinierte Zertifikate besteht im Generieren einer Zertifikatsignieranforderung (Certificate Signing Request, CSR) und im Hinzufügen des Zertifikats, das als Root-Zertifikat an VMCA zurückgesendet wird.

Das Zertifikat, das Sie zum Signieren senden, muss die folgenden Anforderungen erfüllen:

- Schlüsselgröße: mindestens 2.048 Bit
- PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
- x509 Version 3
- Wenn Sie benutzerdefinierte Zertifikate verwenden, muss die Zertifizierungsstellenerweiterung für Stammzertifikate auf „true“ festgelegt werden, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.
- CRL-Signatur muss aktiviert sein.
- „Erweiterte Schlüsselverwendung“ darf keine Clientauthentifizierung oder Serverauthentifizierung enthalten.
- Keine explizite Beschränkung der Zertifikatskettenlänge. VMCA verwendet den OpenSSL-Standardwert von 10 Zertifikaten.
- Zertifikate mit Platzhalterzeichen oder mehr als einem DNS-Namen werden nicht unterstützt.
- Untergeordnete Zertifizierungsstellen von VMCA können nicht erstellt werden.

Im VMware Knowledge Base-Artikel 2112009, „Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0“, finden Sie ein Beispiel für die Verwendung der Microsoft-Zertifizierungsstelle.

VMCA überprüft beim Ersetzen des Root-Zertifikats die folgenden Zertifikatsattribute:

- Schlüsselgröße von mindestens 2.048 Bit
- Schlüsselnutzung: „Cert Sign“

- Basiseinschränkung: „Subject Type CA“

Verfahren

- 1 Generieren Sie eine Zertifikatsignieranforderung und senden Sie sie an Ihre Zertifizierungsstelle.

Befolgen Sie die Anweisungen Ihrer Zertifizierungsstelle.

- 2 Bereiten Sie eine Zertifikatsdatei vor, die das signierte VMCA-Zertifikat sowie die vollständige Zertifikatskette Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle enthält, und speichern Sie die Datei beispielsweise unter dem Namen `rootca1.crt`.

Zu diesem Zweck können Sie alle Zertifizierungsstellenzertifikate im PEM-Format in eine einzige Datei kopieren. Sie müssen mit dem VMCA-Root-Zertifikat beginnen und mit dem PEM-Zertifikat der Root-Zertifizierungsstelle enden. Beispiel:

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

- 3 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

- 4 Ersetzen Sie die vorhandene VMCA-Root-Zertifizierungsstelle.

```
certool --rootca --cert=rootca1.crt --privkey=root1.key
```

Bei der Ausführung dieses Befehls passiert Folgendes:

- Das neue benutzerdefinierte Root-Zertifikat wird dem Zertifikatspeicherort im Dateisystem hinzugefügt.
 - Das benutzerdefinierte Root-Zertifikat wird an den TRUSTED_ROOTS-Speicher in VECS angehängt (nach einer Verzögerung).
 - Das benutzerdefinierte Root-Zertifikat wird zu vmdir hinzugefügt (nach einer Verzögerung).
- 5 (Optional) Zur Weitergabe der Änderung an alle Instanzen von vmdir (VMware-Verzeichnisdienst) veröffentlichen Sie das neue Root-Zertifikat in vmdir und geben Sie dabei für jede Datei den vollständigen Dateipfad an.

Beispiel:

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

Die Replizierung zwischen vmdir-Knoten erfolgt alle 30 Sekunden. Sie müssen das Root-Zertifikat nicht explizit zu VECS hinzufügen, da vmdir von VECS alle fünf Minuten auf neue Root-Zertifikatsdateien überprüft wird.

- 6 (Optional) Bei Bedarf können Sie die Aktualisierung von VECS erzwingen.

```
vecs-cli force-refresh
```

- 7 Starten Sie alle Dienste neu.

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

Beispiel: Ersetzen des Root-Zertifikats

Ersetzen Sie das VMCA-Root-Zertifikat durch das benutzerdefinierte Root-Zertifikat der Zertifizierungsstelle, indem Sie den certool-Befehl mit der Option `--rootca` verwenden.

```
C:\>"C:\Programme\VMware\vCenter Server\vmcad\certool" --rootca --cert=C:\custom-  
certs\root.pem --privkey=C:\custom-certs\root.key
```

Bei der Ausführung dieses Befehls passiert Folgendes:

- Das neue benutzerdefinierte Root-Zertifikat wird dem Zertifikatspeicherort im Dateisystem hinzugefügt.
- Das benutzerdefinierte Root-Zertifikat wird an den TRUSTED_ROOTS-Speicher in VECS angehängt.
- Das benutzerdefinierte Root-Zertifikat wird zu vmdir hinzugefügt.

Nächste Schritte

Sie können das ursprüngliche VMCA-Root-Zertifikat aus dem Zertifikatspeicher entfernen, wenn die Unternehmensrichtlinien dies verlangen. In diesem Fall müssen Sie diese internen Zertifikate aktualisieren:

- Ersetzen des vCenter Single Sign On-Signaturzertifikats. Siehe [Aktualisieren des Zertifikats für den Security Token Service](#).
- Ersetzen des VMware-Verzeichnisdienstzertifikats. Siehe [Ersetzen des VMware-Verzeichnisdienstzertifikats](#).

Ersetzen der Maschinen-SSL-Zertifikate (Zwischenzertifizierungsstelle)

Nachdem Sie das signierte Zertifikat von der Zertifizierungsstelle erhalten und zum VMCA-Rootzertifikat gemacht haben, können Sie alle Maschinen-SSL-Zertifikate ersetzen.

Diese Schritte sind im Wesentlichen mit den Schritten zum Ersetzen durch ein Zertifikat, das VMCA als Zertifizierungsstelle verwendet, identisch. In diesem Fall signiert jedoch VMCA alle Zertifikate mit der vollständigen Zertifikatskette.

Für jede Maschine ist ein Maschinen-SSL-Zertifikat für die sichere Kommunikation mit anderen Diensten erforderlich. Bei einer Bereitstellung mit mehreren Knoten müssen Sie die Befehle zum Generieren von Maschinen-SSL-Zertifikaten auf jedem Knoten ausführen. Verwenden Sie den Parameter `--server`, um von einem vCenter Server mit externem Platform Services Controller aus auf den Platform Services Controller zu verweisen.

Voraussetzungen

`SubjectAltName` muss für jedes Maschinen-SSL-Zertifikat `DNS Name=<Machine FQDN>` enthalten.

Verfahren

- 1 Erstellen Sie eine Kopie von `certtool.cfg` für jede Maschine, für die ein neues Zertifikat erforderlich ist.

`certtool.cfg` finden Sie in den folgenden Speicherorten:

Windows

`C:\Programme\VMware\vCenter Server\vmcad`

Linux

`/usr/lib/vmware-vmca/share/config/`

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

Führen Sie `NSLookup` für die IP-Adresse der Maschine aus, um die DNS-Liste für den Namen anzuzeigen, und verwenden Sie diesen Namen für das Feld „Hostname“ in der Datei.

- 3 Generieren Sie für jede Maschine ein öffentliches/privates Schlüsselpaar sowie ein Zertifikat und übergeben Sie die Konfigurationsdatei, die Sie soeben angepasst haben.

Beispiel:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

- 4 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

- 5 Fügen Sie VECS das neue Zertifikat hinzu.

Alle Maschinen benötigen das neue Zertifikat im lokalen Zertifikatspeicher für die Kommunikation über SSL. Zunächst löschen Sie den vorhandenen Eintrag und fügen dann den neuen Eintrag hinzu.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

- 6 Starten Sie alle Dienste neu.

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

Beispiel: Ersetzen der Maschinen-SSL-Zertifikate (VMCA ist die Zwischenzertifizierungsstelle)

- 1 Erstellen Sie eine Konfigurationsdatei für das SSL-Zertifikat und speichern Sie sie unter dem Namen `ssl-config.cfg` im aktuellen Verzeichnis.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = VMware
```

```
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

- 2 Generieren Sie ein Schlüsselpaar für das Maschinen-SSL-Zertifikat. Führen Sie diesen Befehl auf jedem Verwaltungsknoten und Platform Services Controller-Knoten aus. Die Option `--server` ist dabei nicht erforderlich.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

Die Dateien `ssl-key.priv` und `ssl-key.pub` werden im aktuellen Verzeichnis erstellt.

- 3 Generieren Sie das neue Maschinen-SSL-Zertifikat. Dieses Zertifikat ist VMCA-signiert. Falls Sie das VMCA-Rootzertifikat durch ein benutzerdefiniertes Zertifikat ersetzt haben, signiert VMCA alle Zertifikate mit der vollständigen Zertifikatskette.

- In einem Platform Services Controller-Knoten oder einer eingebetteten Installation:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- Auf einem vCenter Server (externe Installation):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

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

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

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli store list
```

- Ausgabe auf Platform Services Controller:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Ausgabe auf vCenter Server:

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

- 5 Ersetzen Sie das Maschinen-SSL-Zertifikat in VECS durch das neue Maschinen-SSL-Zertifikat. Die Werte `--store` und `--alias` müssen genau mit den Standardnamen übereinstimmen.

- Führen Sie auf dem Platform Services Controller den folgenden Befehl aus, um das Maschinen-SSL-Zertifikat im MACHINE_SSL_CERT-Speicher zu aktualisieren.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- Führen Sie auf jedem Verwaltungsknoten oder für jede eingebettete Bereitstellung den folgenden Befehl aus, um das Maschinen-SSL-Zertifikat im MACHINE_SSL_CERT-Speicher zu aktualisieren. Sie müssen das Zertifikat für jede Maschine separat aktualisieren, da jedes Zertifikat einen unterschiedlichen FQDN aufweist.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Nächste Schritte

Sie können auch die Zertifikate für Ihre ESXi-Hosts ersetzen. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

Nach dem Ersetzen des Rootzertifikats bei einer Bereitstellung mit mehreren Knoten müssen Sie die Dienste für alle vCenter Server-Knoten mit externem Platform Services Controller neu starten.

Ersetzen der Lösungsbenutzerzertifikate (Zwischenzertifizierungsstelle)

Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie die Lösungsbenutzerzertifikate ersetzen.

Sie ersetzen das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten und auf jedem Platform Services Controller-Knoten. Die anderen Lösungsbenutzerzertifikate ersetzen Sie nur auf jedem Verwaltungsknoten. Verwenden Sie den Parameter `--server`, um auf den Platform Services Controller zu verweisen, wenn Sie Befehle auf einem Verwaltungsknoten mit einem externen Platform Services Controller ausführen.

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

Voraussetzungen

Für jedes Lösungsbenutzerzertifikat ist ein unterschiedlicher Wert für `Subject` erforderlich. Geben Sie beispielsweise den Lösungsbenutzernamen (z. B. `vpzd`) oder einen anderen eindeutigen Bezeichner an.

Verfahren

- 1 Erstellen Sie eine Kopie von `certool.cfg`, entfernen Sie die Felder für den Namen, die IP-Adresse, den DNS-Namen und die E-Mail-Adresse und benennen Sie die Datei z. B. in `sol_usr.cfg` um.

Sie können die Zertifikate im Rahmen des Generierungsvorgangs über die Befehlszeile benennen. Die restlichen Informationen sind für Lösungsbenutzer nicht erforderlich. Wenn Sie die Standardinformationen unverändert lassen, könnten die generierten Zertifikate für Verwirrung sorgen.

- 2 Generieren Sie für jeden Lösungsbenutzer ein öffentliches/privates Schlüsselpaar sowie ein Zertifikat und übergeben Sie die Konfigurationsdatei, die Sie soeben angepasst haben.

Beispiel:

```
certool --genkey --privkey=vpzd.priv --pubkey=vpzd.pub
certool --gencert --privkey=vpzd.priv --cert vpzd.crt --Name=VPXD_1 --config sol_usr.cfg
```

- 3 Suchen Sie den Namen für jeden Lösungsbenutzer.

```
dir-cli service list
```

Sie können die eindeutige ID verwenden, die beim Ersetzen der Zertifikate zurückgegeben wird. Die Ein- und Ausgabe könnte so oder ähnlich wie im Folgenden aussehen.

```
C:\Program Files\VMware\VMware Server\vmaddd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpzd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpzd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

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

- 4 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

- 5 Ersetzen Sie das vorhandene Zertifikat in vmdir und anschließend in VECS.

Für Lösungsbenutzer müssen Sie die Zertifikate in dieser Reihenfolge hinzufügen. Beispiel:

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

Hinweis Lösungsbenutzer können sich nur bei vCenter Single Sign On anmelden, wenn Sie das Zertifikat in vmdir ersetzen.

- 6 Starten Sie alle Dienste neu.

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

Beispiel: Ersetzen der Lösungsbenutzerzertifikate (Zwischenzertifizierungsstelle)

- 1 Generieren Sie für jeden Lösungsbenutzer ein öffentliches/privates Schlüsselpaar. Dies beinhaltet ein Schlüsselpaar für den Lösungsbenutzer „machine“ auf jedem Platform Services Controller und jedem Verwaltungsknoten sowie ein Schlüsselpaar für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient) auf jedem Verwaltungsknoten.
 - a Generieren Sie für den Lösungsbenutzer „machine“ einer eingebetteten Bereitstellung oder für den Lösungsbenutzer „machine“ des Platform Services Controller ein Schlüsselpaar.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-
key.priv --pubkey=machine-key.pub
```

- b (Optional) Generieren Sie für Bereitstellungen mit einem externen Platform Services Controller für den Lösungsbenutzer „machine“ ein Schlüsselpaar auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- c Generieren Sie für den vpxd-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

- d Generieren Sie für den vpxd-extension-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

- e Generieren Sie für den vsphere-webclient-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

- 2 Generieren Sie vom neuen VMCA-Rootzertifikat signierte Lösungsbenutzerzertifikate für den Lösungsbenutzer „machine“ auf jedem Platform Services Controller und jedem Verwaltungsknoten sowie für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient) auf jedem Verwaltungsknoten.

Hinweis Der Parameter --Name muss eindeutig sein. Durch die Angabe des Namens des Lösungsbenutzerspeichers (z. B. vpxd oder vpxd-extension) ist auf einfache Weise erkennbar, welches Zertifikat welchem Lösungsbenutzer zugeordnet ist.

- a Führen Sie den folgenden Befehl auf dem Platform Services Controller-Knoten aus, um für den Lösungsbenutzer „machine“ auf diesem Knoten ein Lösungsbenutzerzertifikat zu generieren.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<pvc-ip-or-fqdn>
```

- c Generieren Sie für den vpxd-Lösungsbenutzer auf jedem Verwaltungsknoten ein Zertifikat.

```
C:\>"C:\Program Files\VMware\VCServer\vmcad\certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

- d Generieren Sie für den vpxd-extensions-Lösungsbenutzer auf jedem Verwaltungsknoten ein Zertifikat.

```
C:\>"C:\Program Files\VMware\VCServer\vmcad\certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\VCServer\vmcad\certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

- 3 Ersetzen Sie die Lösungsbenutzerzertifikate in VECS durch die neuen Lösungsbenutzerzertifikate.

Hinweis Die Parameter `--store` und `--alias` müssen genau mit den Standardnamen für die Dienste übereinstimmen.

- a Führen Sie auf dem Platform Services Controller-Knoten den folgenden Befehl aus, um das Lösungsbenutzerzertifikat „machine“ zu ersetzen:

```
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b Ersetzen Sie das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten:

```
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c Ersetzen Sie das vpxd-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```


- d Ersetzen Sie das vpxd-extension-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

- e Ersetzen Sie das vsphere-webclient-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

- 4 Aktualisieren Sie den VMware-Verzeichnisdienst (vmdir) mit den neuen Lösungsbenutzerzertifikaten. Sie werden zur Eingabe eines vCenter Single Sign On-Administratorkennworts aufgefordert.
- a Führen Sie `dir-cli service list` aus, um für jeden Lösungsbenutzer das eindeutige Dienst-ID-Suffix abzurufen. Sie können diesen Befehl auf einem Platform Services Controller oder für ein vCenter Server-System ausführen.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

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

- b Ersetzen Sie das Maschinenzertifikat in vmdir auf dem Platform Services Controller. Wenn beispielsweise „machine-29a45d00-60a7-11e4-96ff-00505689639a“ der Lösungsbenutzer „machine“ auf dem Platform Services Controller ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"dir-cli service update --name machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

- c Ersetzen Sie das Maschinenzertifikat in vmdir auf jedem Verwaltungsknoten. Wenn beispielsweise „machine-6fd7f140-60a9-11e4-9e28-005056895a69“ der Lösungsbenutzer „machine“ auf dem vCenter Server ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

Ersetzen des VMware-Verzeichnisdienstzertifikats

Wenn Sie ein neues VMCA-Root-Zertifikat verwenden möchten und die Veröffentlichung des VMCA-Root-Zertifikats, das bei der Bereitstellung Ihrer Umgebung verwendet wurde, rückgängig machen, müssen Sie die Maschinen-SSL-Zertifikate, Lösungsbenutzerzertifikate und Zertifikate für bestimmte interne Dienste ersetzen.

Wenn Sie die Veröffentlichung des VMCA-Root-Zertifikats rückgängig machen, müssen Sie das von vCenter Single Sign On verwendete SSL-Signaturzertifikat ersetzen. Siehe [Aktualisieren des Zertifikats für den Security Token Service](#). Darüber hinaus müssen Sie das Zertifikat für den VMware-Verzeichnisdienst (vmdir) ersetzen.

Voraussetzungen

Fordern Sie ein Zertifikat für vmdir für Ihre Drittanbieter- oder Unternehmenszertifizierungsstelle an.

Verfahren

- 1 Beenden Sie vmdir.

Linux

```
service-control --stop vmdird
```

Windows

```
service-control --stop VMWareDirectoryService
```

- 2 Kopieren Sie das Zertifikat und den Schlüssel, die Sie soeben generiert haben, in den vmdir-Speicherort.

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 Starten Sie vmdir über den vSphere Web Client oder mithilfe des Befehls `service-control` neu.

Linux

```
service-control --start vmdird
```

Windows

```
service-control --start VMWareDirectoryService
```

Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

Das SSL-Zertifikat des VMware Directory Service wird von vmdir für Handshakes zwischen Platform Services Controller-Knoten verwendet, die die vCenter Single Sign On-Replizierung durchführen.

Diese Schritte sind für Umgebungen im gemischten Modus, die Knoten mit vSphere 6.0 und vSphere 6.5 enthalten, nicht erforderlich. Diese Schritte sind nur in folgenden Fällen erforderlich:

- In Ihrer Umgebung sind sowohl vCenter Single Sign On 5.5- als auch vCenter Single Sign On 6.x-Dienste vorhanden.
- Die vCenter Single Sign On-Dienste sind für die Replizierung von vmdir-Daten eingerichtet.
- Sie können die standardmäßigen VMCA-signierten Zertifikate für den Knoten, auf dem der vCenter Single Sign On 6.x-Dienst ausgeführt wird, durch benutzerdefinierte Zertifikate ersetzen.

Hinweis Es empfiehlt sich, vor dem Neustart der Dienste ein Upgrade der kompletten Umgebung durchzuführen. Vom Ersetzen des VMware Directory Service-Zertifikats wird in der Regel abgeraten.

Verfahren

- 1 Ersetzen Sie auf dem Knoten, auf dem der vCenter Single Sign On 6.x-Dienst ausgeführt wird, das vmdir-SSL-Zertifikat und den Schlüssel.

Weitere Informationen hierzu finden Sie unter [Ersetzen des VMware-Verzeichnisdienstzertifikats](#).

- 2 Richten Sie auf dem Knoten, auf dem der vCenter Single Sign On 5.5-Dienst ausgeführt wird, die Umgebung so ein, dass der vCenter Single Sign On 6.x-Dienst bekannt ist.
 - a Sichern Sie alle Dateien im Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmdir`.
 - b Erstellen Sie eine Kopie der Datei `vmdircert.pem` auf dem Knoten der Version 6.x und benennen Sie sie in `<sso_node2.domain.com>.pem` um, wobei `<sso_node2.domain.com>` der FQDN des Knotens der Version 6.x ist.
 - c Kopieren Sie das umbenannte Zertifikat in das Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmdir`, um das vorhandene Replizierungszertifikat zu ersetzen.
- 3 Starten Sie den VMware Directory Service auf allen Maschinen neu, auf denen Sie Zertifikate ersetzt haben.

Sie können den Dienst über den vSphere Web Client oder mithilfe des Befehls `service-control` neu starten.

Verwenden von Drittanbieterzertifikaten mit vSphere

Wenn die Unternehmensrichtlinien es verlangen, können Sie alle in vSphere verwendeten Zertifikate durch Zertifikate ersetzen, die von einer Zertifizierungsstelle eines Drittanbieters signiert wurden. In diesem Fall befindet sich VMCA nicht in Ihrer Zertifikatskette, aber alle vCenter-Zertifikate müssen in VECS gespeichert werden.

Sie können alle Zertifikate ersetzen oder eine Hybridlösung verwenden. Ersetzen Sie beispielsweise alle Zertifikate, die für Netzwerkdatenverkehr verwendet werden, und belassen Sie VMCA-signierte Lösungsbenutzerzertifikate. Lösungsbenutzerzertifikate werden nur für die Authentifizierung bei vCenter Single Sign On verwendet.

Hinweis Wenn Sie VMCA nicht verwenden möchten, müssen Sie selbst alle Zertifikate ersetzen, neue Komponenten mit Zertifikaten bereitstellen und den Ablauf von Zertifikaten nachverfolgen.

Verfahren

1 Anfordern von Zertifikaten und Importieren eines benutzerdefinierten Rootzertifikats

Wenn die Unternehmensrichtlinien keine Zwischenzertifizierungsstelle zulassen, können die Zertifikate nicht von VMCA generiert werden. Sie verwenden benutzerdefinierte Zertifikate von einer Unternehmens- oder Drittanbieter-Zertifizierungsstelle.

2 Ersetzen der Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate

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

3 Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate

Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie die VMCA-signierten Lösungsbenutzerzertifikate durch Drittanbieter- oder Unternehmenszertifikate ersetzen.

4 Ersetzen des VMware-Verzeichnisdienstzertifikats

Wenn Sie ein neues VMCA-Root-Zertifikat verwenden möchten und die Veröffentlichung des VMCA-Root-Zertifikats, das bei der Bereitstellung Ihrer Umgebung verwendet wurde, rückgängig machen, müssen Sie die Maschinen-SSL-Zertifikate, Lösungsbenutzerzertifikate und Zertifikate für bestimmte interne Dienste ersetzen.

5 Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

Anfordern von Zertifikaten und Importieren eines benutzerdefinierten Rootzertifikats

Wenn die Unternehmensrichtlinien keine Zwischenzertifizierungsstelle zulassen, können die Zertifikate nicht von VMCA generiert werden. Sie verwenden benutzerdefinierte Zertifikate von einer Unternehmens- oder Drittanbieter-Zertifizierungsstelle.

Voraussetzungen

Das Zertifikat muss die folgenden Anforderungen erfüllen:

- Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)

- PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
- x509 Version 3
- Für Stammzertifikate muss die Zertifizierungsstellenerweiterung auf „true“ festgelegt sein, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.
- „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten
- CRT-Format
- Enthält die folgenden Schlüsselverwendungen: Digitale Signatur, 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.

Verfahren

- 1 Senden Sie Zertifikatssignieranforderung (CSRs) für die folgenden Zertifikate an Ihren Unternehmens- oder Drittanbieter-Zertifikatanbieter.

- Ein Maschinen-SSL-Zertifikat für jede Maschine. Für das Maschinen-SSL-Zertifikat muss das Feld „SubjectAltName“ den vollqualifizierten Domännennamen (DNS NAME= *Maschinen-FQDN*) enthalten.
- Optional vier Lösungsbenutzerzertifikate für jedes eingebettete System bzw. jeden Verwaltungsknoten. Lösungsbenutzerzertifikate sollten keine IP-Adresse, keinen Hostnamen und keine E-Mail-Adresse enthalten. Für jedes Zertifikat ist ein unterschiedlicher Zertifikatantragsteller erforderlich.

Das Ergebnis sind in der Regel eine PEM-Datei für die Vertrauenskette sowie die signierten SSL-Zertifikate für jeden Platform Services Controller bzw. jeden Verwaltungsknoten.

- 2 Listen Sie die TRUSTED_ROOTS- und Maschinen-SSL-Speicher auf.

```
vecs-cli store list
```

- a Stellen Sie sicher, dass das aktuelle Rootzertifikat und alle Maschinen-SSL-Zertifikate von VMCA signiert wurden.
- b Notieren Sie sich den Inhalt der Felder „Seriennummer“, „Aussteller“ und „Subjektnamen“.
- c (Optional) Stellen Sie mithilfe eines Webbrowsers eine HTTPS-Verbindung zu einem Knoten her, auf dem das Zertifikat platziert werden soll. Überprüfen Sie die Zertifikatsinformationen und stellen Sie sicher, dass sie mit dem Maschinen-SSL-Zertifikat übereinstimmen.

- 3 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

- 4 Veröffentlichen Sie das benutzerdefinierte Rootzertifikat, bei dem es sich um das Signaturzertifikat der Drittanbieter-Zertifizierungsstelle handelt.

```
dir-cli trustedcert publish --cert <my_custom_root>
```

Wenn Sie in der Befehlszeile keinen Benutzernamen und kein Kennwort eingeben, werden Sie zur Eingabe dieser Informationen aufgefordert.

- 5 Starten Sie alle Dienste neu.

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

Nächste Schritte

Sie können das ursprüngliche VMCA-Stammzertifikat aus dem Zertifikatspeicher entfernen, falls die Unternehmensrichtlinien dies verlangen. In diesem Fall müssen Sie diese internen Zertifikate aktualisieren:

- Ersetzen Sie das vCenter Single Sign On-Signaturzertifikat. Siehe [Aktualisieren des Zertifikats für den Security Token Service](#).
- Ersetzen des VMware-Verzeichnisdienstzertifikats. Siehe [Ersetzen des VMware-Verzeichnisdienstzertifikats](#).

Ersetzen der Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate

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

Für jede Maschine ist ein Maschinen-SSL-Zertifikat für die sichere Kommunikation mit anderen Diensten erforderlich. Bei einer Bereitstellung mit mehreren Knoten müssen Sie die Befehle zum Generieren von Maschinen-SSL-Zertifikaten auf jedem Knoten ausführen. Verwenden Sie den Parameter `--server`, um von einem vCenter Server mit externem Platform Services Controller aus auf den Platform Services Controller zu verweisen.

Sie benötigen die folgenden Informationen, bevor Sie mit dem Ersetzen der Zertifikate beginnen können:

- Kennwort für „administrator@vsphere.local“.
- Gültiges benutzerdefiniertes Maschinen-SSL-Zertifikat (.crt-Datei).
- Gültiger benutzerdefinierter Maschinen-SSL-Schlüssel (.key-Datei).
- Gültiges benutzerdefiniertes Zertifikat für Root (.crt-Datei).
- Die IP-Adresse des Platform Services Controller, wenn Sie den Befehl für einen vCenter Server mit externem Platform Services Controller in einer Bereitstellung mit mehreren Knoten ausführen.

Voraussetzungen

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

- Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
- CRT-Format
- x509 Version 3
- „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten
- Enthält die folgenden Schlüsselverwendungen: Digitale Signatur, Unleugbarkeit, Schlüsselverschlüsselung

Verfahren

- 1 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

- 2 Melden Sie sich bei jedem Knoten an und fügen Sie die neuen Maschinenzertifikate, die Sie von der Zertifizierungsstelle erhalten haben, zu VECS hinzu.

Alle Maschinen benötigen das neue Zertifikat im lokalen Zertifikatspeicher für die Kommunikation über SSL.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-path>
--key <key-file-path>
```

- 3 Starten Sie alle Dienste neu.

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

Beispiel: Ersetzen der Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate

Sie können das Maschinen-SSL-Zertifikat für jeden Knoten auf dieselbe Weise ersetzen.

- 1 Löschen Sie zunächst das vorhandene Zertifikat in VECS.

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
```

- 2 Fügen Sie anschließend das Ersatzzertifikat hinzu.

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-wl-
vim-cat-dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-
cat-dhcp-1128.vmware.com.priv
```

Nächste Schritte

Sie können auch die Zertifikate für Ihre ESXi-Hosts ersetzen. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

Nach dem Ersetzen des Rootzertifikats bei einer Bereitstellung mit mehreren Knoten müssen Sie die Dienste für alle vCenter Server-Knoten mit externem Platform Services Controller neu starten.

Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate

Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie die VMCA-signierten Lösungsbenutzerzertifikate durch Drittanbieter- oder Unternehmenszertifikate ersetzen.

Lösungsbenutzer verwenden Zertifikate für die Authentifizierung bei vCenter Single Sign On. Wenn das Zertifikat gültig ist, weist vCenter Single Sign On dem Lösungsbenutzer ein SAML-Token zu, und der Lösungsbenutzer verwendet das SAML-Token für die Authentifizierung bei anderen vCenter-Komponenten.

Überlegen Sie sich, ob Lösungsbenutzerzertifikate in Ihrer Umgebung ersetzt werden müssen. Da sich Lösungsbenutzer hinter einem Proxy-Server befinden und das Maschinen-SSL-Zertifikat für den Schutz des SSL-Datenverkehrs verwendet wird, stellen die Lösungsbenutzerzertifikate möglicherweise ein geringeres Sicherheitsrisiko dar.

Sie ersetzen das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten und auf jedem Platform Services Controller-Knoten. Die anderen Lösungsbenutzerzertifikate ersetzen Sie nur auf jedem Verwaltungsknoten. Verwenden Sie den Parameter `--server`, um auf den Platform Services Controller zu verweisen, wenn Sie Befehle auf einem Verwaltungsknoten mit einem externen Platform Services Controller ausführen.

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

Voraussetzungen

- Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
- CRT-Format
- x509 Version 3
- „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten
- Für jedes Lösungsbenutzerzertifikat ist ein unterschiedlicher Wert für `Subject` erforderlich. Geben Sie beispielsweise den Lösungsbenutzernamen (z. B. `vpxd`) oder einen anderen eindeutigen Bezeichner an.
- Enthält die folgenden Schlüsselverwendungen: Digitale Signatur, Unleugbarkeit, Schlüsselverschlüsselung

Verfahren

- 1 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmca
```

- 2 Suchen Sie den Namen für jeden Lösungsbenutzer.

```
dir-cli service list
```

Sie können die eindeutige ID verwenden, die beim Ersetzen der Zertifikate zurückgegeben wird. Die Ein- und Ausgabe könnte so oder ähnlich wie im Folgenden aussehen.

```
C:\Program Files\VMware\vCenter Server\vmafd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

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

- 3 Ersetzen Sie für jeden Lösungsbenutzer das vorhandene Zertifikat in VECS und anschließend in vmdir.

Sie müssen die Zertifikate in dieser Reihenfolge hinzufügen.

```
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
dir-cli service update --name <vpxd-xxxx-xxx-xxxxxx> --cert vpxd.crt
```

Hinweis Lösungsbenutzer können sich nur bei vCenter Single Sign On authentifizieren, wenn Sie das Zertifikat in vmdir ersetzen.

- 4 Starten Sie alle Dienste neu.

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

Ersetzen des VMware-Verzeichnisdienstzertifikats

Wenn Sie ein neues VMCA-Root-Zertifikat verwenden möchten und die Veröffentlichung des VMCA-Root-Zertifikats, das bei der Bereitstellung Ihrer Umgebung verwendet wurde, rückgängig

machen, müssen Sie die Maschinen-SSL-Zertifikate, Lösungsbenutzerzertifikate und Zertifikate für bestimmte interne Dienste ersetzen.

Wenn Sie die Veröffentlichung des VMCA-Root-Zertifikats rückgängig machen, müssen Sie das von vCenter Single Sign On verwendete SSL-Signaturzertifikat ersetzen. Siehe [Aktualisieren des Zertifikats für den Security Token Service](#). Darüber hinaus müssen Sie das Zertifikat für den VMware-Verzeichnisdienst (vmdir) ersetzen.

Voraussetzungen

Fordern Sie ein Zertifikat für vmdir für Ihre Drittanbieter- oder Unternehmenszertifizierungsstelle an.

Verfahren

- 1 Beenden Sie vmdir.

Linux

```
service-control --stop vmdird
```

Windows

```
service-control --stop VMWareDirectoryService
```

- 2 Kopieren Sie das Zertifikat und den Schlüssel, die Sie soeben generiert haben, in den vmdir-Speicherort.

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 Starten Sie vmdir über den vSphere Web Client oder mithilfe des Befehls `service-control` neu.

Linux

```
service-control --start vmdird
```

Windows

```
service-control --start VMWareDirectoryService
```

Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

Das SSL-Zertifikat des VMware Directory Service wird von vmdir für Handshakes zwischen Platform Services Controller-Knoten verwendet, die die vCenter Single Sign On-Replizierung durchführen.

Diese Schritte sind für Umgebungen im gemischten Modus, die Knoten mit vSphere 6.0 und vSphere 6.5 enthalten, nicht erforderlich. Diese Schritte sind nur in folgenden Fällen erforderlich:

- In Ihrer Umgebung sind sowohl vCenter Single Sign On 5.5- als auch vCenter Single Sign On 6.x-Dienste vorhanden.
- Die vCenter Single Sign On-Dienste sind für die Replizierung von vmdir-Daten eingerichtet.
- Sie können die standardmäßigen VMCA-signierten Zertifikate für den Knoten, auf dem der vCenter Single Sign On 6.x-Dienst ausgeführt wird, durch benutzerdefinierte Zertifikate ersetzen.

Hinweis Es empfiehlt sich, vor dem Neustart der Dienste ein Upgrade der kompletten Umgebung durchzuführen. Vom Ersetzen des VMware Directory Service-Zertifikats wird in der Regel abgeraten.

Verfahren

- 1 Ersetzen Sie auf dem Knoten, auf dem der vCenter Single Sign On 6.x-Dienst ausgeführt wird, das vmdird-SSL-Zertifikat und den Schlüssel.

Weitere Informationen hierzu finden Sie unter [Ersetzen des VMware-Verzeichnisdienstzertifikats](#).

- 2 Richten Sie auf dem Knoten, auf dem der vCenter Single Sign On 5.5-Dienst ausgeführt wird, die Umgebung so ein, dass der vCenter Single Sign On 6.x-Dienst bekannt ist.
 - a Sichern Sie alle Dateien im Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmdird`.
 - b Erstellen Sie eine Kopie der Datei `vmdircert.pem` auf dem Knoten der Version 6.x und benennen Sie sie in `<sso_node2.domain.com>.pem` um, wobei `<sso_node2.domain.com>` der FQDN des Knotens der Version 6.x ist.
 - c Kopieren Sie das umbenannte Zertifikat in das Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmdird`, um das vorhandene Replizierungszertifikat zu ersetzen.

- 3 Starten Sie den VMware Directory Service auf allen Maschinen neu, auf denen Sie Zertifikate ersetzt haben.

Sie können den Dienst über den vSphere Web Client oder mithilfe des Befehls `service-control` neu starten.

Verwalten von Zertifikaten und Diensten mit CLI-Befehlen

Mit einer Reihe von Befehlszeilenschnittstellen (CLIs) können Sie VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store) und den VMware Directory Service (vmdir) verwalten. Das Dienstprogramm vSphere Certificate Manager unterstützt zwar auch viele verwandte Aufgaben, für die manuelle Zertifikatsverwaltung sind jedoch Befehlszeilenschnittstellen erforderlich.

Tabelle 3-5. CLI-Tools für die Verwaltung von Zertifikaten und zugehörigen Diensten

Befehlszeilenschnittstelle	Beschreibung	Informationen hierzu unter
<code>certool</code>	Generieren und verwalten Sie Zertifikate und Schlüssel. Bestandteil von VMCA.	Befehlsreferenz für die certool-Initialisierung
<code>vecs-cli</code>	Verwalten Sie die Inhalte von VMware-Zertifikatspeicherinstanzen. Bestandteil von VMAFD.	Befehlsreferenz für vecs-cli
<code>dir-cli</code>	Erstellen und aktualisieren Sie Zertifikate im VMware Directory Service. Bestandteil von VMAFD.	Befehlsreferenz für dir-cli
<code>service-control</code>	Starten oder Stoppen von Diensten, zum Beispiel als Teil eines Workflows zur Zertifikatsersetzung.	

Speicherorte der Zertifikatsverwaltungstools

Die Tools finden Sie standardmäßig in den folgenden Speicherorten auf jedem Knoten.

Windows

```
C:\Programme\VMware\vCenter Server\vmafdd\vecs-cli.exe
C:\Programme\VMware\vCenter Server\vmafdd\dir-cli.exe
C:\Programme\VMware\vCenter Server\vmcad\certool.exe
VCENTER_INSTALL_PATH\bin\service-control
```

Linux

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

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

Wenn Sie Befehle von einem Verwaltungsknoten aus mit einem externen Platform Services Controller ausführen, können Sie den Platform Services Controller mit dem Parameter `--server` angeben.

Erforderliche Rechte für Zertifikatsverwaltungsvorgänge

Für die meisten vCenter-Zertifikatsverwaltungsvorgänge müssen Sie Mitglied der Gruppe „CAAdmins“ in der Domäne „vsphere.local“ sein. Der Benutzer „administrator@vsphere.local“ gehört der Gruppe „CAAdmins“ an. Manche Vorgänge sind für alle Benutzer zulässig.

Bei Ausführung des Dienstprogramms vCenter Certificate Manager werden Sie zur Eingabe des Kennworts von „administrator@vsphere.local“ aufgefordert. Wenn Sie Zertifikate manuell ersetzen, erfordern die verschiedenen Optionen für die verschiedenen Zertifikatsverwaltungs-CLIs unterschiedliche Rechte.

dir-cli

Sie müssen ein Mitglied der Gruppe „CAAdmins“ in der Domäne „vsphere.local“ sein. Sie werden bei jeder Ausführung eines `dir-cli`-Befehls zur Eingabe eines Benutzernamens und Kennworts aufgefordert.

vecs-cli

Zunächst hat nur der Inhaber eines Speichers Zugriff auf den Speicher. Der Inhaber des Speichers ist der Administratorbenutzer auf Windows-Systemen bzw. der Rootbenutzer auf Linux-Systemen. Der Inhaber des Speichers kann anderen Benutzern den Zugriff ermöglichen.

Bei den Speichern `MACHINE_SSL_CERT` und `TRUSTED_ROOTS` handelt es sich um spezielle Speicher. In Abhängigkeit vom Installationstyp hat nur der Rootbenutzer oder Administratorbenutzer vollständigen Zugriff.

certool

Für die meisten `certool`-Befehle muss der Benutzer der Gruppe „CAAdmins“ angehören. Der Benutzer „administrator@vsphere.local“ gehört der Gruppe „CAAdmins“ an. Alle Benutzer können die folgenden Befehle ausführen:

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`
- `waitVMCA`
- `genkey`

■ viewcert

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

Ändern der certool-Konfiguration

Wenn Sie `certool --gencert` und bestimmte andere Zertifikatinitialisierungs- oder Verwaltungsbefehle ausführen, liest die Befehlszeilenschnittstelle (CLI) alle Werte aus einer Konfigurationsdatei ein. Sie können die vorhandene Datei bearbeiten, die Standardkonfigurationsdatei (`certool.cfg`) mithilfe der Option `--config=<Dateiname>` außer Kraft setzen oder verschiedene Werte in der Befehlszeile überschreiben.

Die Konfigurationsdatei weist mehrere Felder mit den folgenden Standardwerten auf:

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

Die Konfigurationswerte können Sie wie folgt ändern:

- Erstellen Sie eine Sicherungskopie der Konfigurationsdatei und bearbeiten Sie die Datei. Falls Sie die Standardkonfigurationsdatei verwenden, müssen Sie die Datei nicht angeben. Andernfalls verwenden Sie die Befehlszeilenoption `--config`, falls Sie beispielsweise den Namen der Konfigurationsdatei geändert haben.
- Überschreiben Sie den Wert für die Konfigurationsdatei in der Befehlszeile. Führen Sie beispielsweise den folgenden Befehl aus, um „Locality“ zu überschreiben:

```
certool --gencert --privkey=private.key --Locality="Mountain View"
```

Geben Sie `--Name` an, um das Feld „CN“ für den Objektnamen des Zertifikats zu ersetzen.

- Für Lösungsbenutzerzertifikate lautet der Name laut Konvention `<Lösungsbenutzername>@<Domäne>`, aber Sie können den Namen ändern, falls in Ihrer Umgebung eine andere Konvention verwendet wird.
- Für Maschinen-SSL-Zertifikate wird der FQDN der Maschine verwendet, da der SSL-Client bei der Verifizierung des Hostnamens der Maschine das Feld „CN“ für den Objektnamen des Zertifikats überprüft. Eine Maschine kann mehrere Aliase aufweisen, weshalb Zertifikate das erweiterte Feld „Alternativnamen für Betreff“ enthalten, in dem Sie andere Namen angeben können (DNS-Namen, IP-Adressen usw.). VMCA erlaubt allerdings nur einen einzigen DNSName-Wert (im Feld `Hostname`) und keine anderen Aliasoptionen. Wenn die IP-Adresse vom Benutzer angegeben wird, wird sie ebenfalls in „SubAltName“ gespeichert.

Mithilfe des Parameters `--Hostname` wird der `DNSName`-Wert für „SubAltName“ des Zertifikats angegeben.

Befehlsreferenz für die certool-Initialisierung

Mit den Befehlen zur `certool`-Initialisierung können Sie Zertifikatsignieranforderungen generieren, VMCA-signierte Zertifikate und Schlüssel anzeigen und generieren, Stammzertifikate importieren und weitere Zertifikatsverwaltungsvorgänge durchführen.

In vielen Fällen übergeben Sie mit einem `certool`-Befehl eine Konfigurationsdatei. Siehe [Ändern der certool-Konfiguration](#). Einige Beispiele für die Verwendung finden Sie unter [Ersetzen vorhandener VMCA-signierter Zertifikate durch neue VMCA-signierte Zertifikate](#).

certool --initcsr

Generiert eine Zertifikatsignieranforderung (Certificate Signing Request, CSR). Der Befehl generiert eine PKCS10-Datei und einen privaten Schlüssel.

Option	Beschreibung
<code>--initcsr</code>	Erforderlich zum Generieren von CSRs
<code>--privkey <Schlüsseldatei></code>	Name der privaten Schlüsseldatei
<code>--pubkey <Schlüsseldatei></code>	Name der öffentlichen Schlüsseldatei
<code>--csrfile <CSR-Datei></code>	Dateinamen der CSR-Datei, die an den Anbieter der Zertifizierungsstelle gesendet werden soll
<code>--config <Konfigurationsdatei></code>	Optional Name der Konfigurationsdatei. <code>certool.cfg</code> ist die Standardeinstellung.

Beispiel:

```
certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

Erstellt ein selbstsigniertes Zertifikat und stattet den VMCA-Server mit einer selbstsignierten Stammzertifizierungsstelle aus. Diese Option ist eine der einfachsten Methoden zur Bereitstellung von Zertifikaten für den VMCA-Server. Sie können dem VMCA-Server auch ein Stammzertifikat eines Drittanbieters zur Verfügung stellen, wobei VMCA als Zwischenzertifizierungsstelle fungiert. Siehe [Verwenden von VMCA als Zwischenzertifizierungsstelle](#).

Dieser Befehl generiert ein um drei Tage rückdatiertes Zertifikat, um Zeitonenkonflikte zu vermeiden.

Option	Beschreibung
<code>--selfca</code>	Erforderlich zum Generieren eines selbstsignierten Zertifikats.
<code>--predate <Anzahl_der_Minuten></code>	Ermöglicht im Feld „Gültig nicht vor“ des Stammzertifikats die Eingabe einer Anzahl von Minuten vor der aktuellen Uhrzeit. Mit dieser Option können Sie potenzielle Probleme aufgrund von Zeitverschiebungen vermeiden. Der Maximalwert beträgt drei Tage.
<code>--config <Konfigurationsdatei></code>	Optionaler Name der Konfigurationsdatei. <code>certool.cfg</code> ist die Standardeinstellung.
<code>--server <Server></code>	Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“.

Beispiel:

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280 --selfca --server=
192.0.2.24 --srp-upn=administrator@vsphere.local
```

certool --rootca

Importiert ein Stammzertifikat. Fügt das Zertifikat und den privaten Schlüssel der VMCA hinzu. VMCA verwendet zur Signierung stets das aktuellste Stammzertifikat, aber andere Zertifikate stehen nach wie vor zur Verfügung. Das bedeutet, dass Sie Ihre Infrastruktur schrittweise aktualisieren und zum Schluss alle nicht mehr benötigten Zertifikate löschen können.

Option	Beschreibung
<code>--rootca</code>	Erforderlich zum Importieren einer Stammzertifizierungsstelle.
<code>--cert <Zertifikatsdatei></code>	Optionaler Name der Konfigurationsdatei. <code>certool.cfg</code> ist die Standardeinstellung.
<code>--privkey <Schlüsseldatei></code>	Name der privaten Schlüsseldatei. Die Datei muss im kodierten PEM-Format vorliegen.
<code>--server <Server></code>	Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“.

Beispiel:

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

Gibt den Standarddomännennamen zurück, der vom vmdir verwendet wird.

Option	Beschreibung
<code>--server <Server></code>	Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“.
<code>--port <Portnummer></code>	Optionale Portnummer. Die Standardeinstellung ist Port 389.

Beispiel:

```
certool --getdc
```

certool --waitVMDIR

Warten Sie, bis der VMware-Verzeichnisdienst ausgeführt wird oder die durch `--wait` angegebene Zeitüberschreitungsdauer abgelaufen ist. Verwenden Sie diese Option zusammen mit anderen Optionen zur Planung gewisser Aufgaben, z. B. der Rückgabe des Standarddomännennamens.

Option	Beschreibung
<code>--wait</code>	Optionale Anzahl von Minuten, die gewartet werden soll. Die Standardeinstellung lautet 3.
<code>--server <Server></code>	Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“.
<code>--port <Portnummer></code>	Optionale Portnummer. Die Standardeinstellung ist Port 389.

Beispiel:

```
certool --waitVMDIR --wait 5
```

certool --waitVMCA

Warten Sie, bis der VMCA-Dienst ausgeführt wird oder die angegebene Zeitüberschreitungsdauer abgelaufen ist. Verwenden Sie diese Option zusammen mit anderen Optionen zur Planung gewisser Aufgaben, z. B. der Generierung von Zertifikaten.

Option	Beschreibung
<code>--wait</code>	Optionale Anzahl von Minuten, die gewartet werden soll. Die Standardeinstellung lautet 3.
<code>--server <Server></code>	Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“.
<code>--port <Portnummer></code>	Optionale Portnummer. Die Standardeinstellung ist Port 389.

Beispiel:

```
certool --waitVMCA --selfca
```

certool --publish-roots

Erzwingt ein Update der Stammzertifikate. Für diesen Befehl sind Administratorrechte erforderlich.

Option	Beschreibung
<code>--server <Server></code>	Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“.

Beispiel:

```
certool --publish-roots
```

Befehlsreferenz für die certool-Verwaltung

Mit den `certool`-Verwaltungsbefehlen können Sie Zertifikate anzeigen, generieren und widerrufen sowie Informationen zu Zertifikaten anzeigen.

certool --genkey

Erstellt ein privates und öffentliches Schlüsselpaar. Diese Dateien können dann zum Generieren eines Zertifikats verwendet werden, das durch VMCA signiert wird. Sie können das Zertifikat für Systeme oder Lösungsbenutzer bereitstellen.

Option	Beschreibung
<code>--genkey</code>	Ist zum Erstellen eines privaten und öffentlichen Schlüssels erforderlich.
<code>--privkey <Schlüsseldatei></code>	Name der privaten Schlüsseldatei
<code>--pubkey <Schlüsseldatei></code>	Name der öffentlichen Schlüsseldatei
<code>--server <Server></code>	Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“.

Beispiel:

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

certool --gencert

Erstellt ein Zertifikat vom VMCA-Server. Dieser Befehl verwendet die Information in `certool.cfg` oder in der festgelegten Konfigurationsdatei.

Option	Beschreibung
<code>--gencert</code>	Ist zum Erstellen eines Zertifikats erforderlich.
<code>--cert <Zertifikatsdatei></code>	Name der Zertifikatsdatei. Die Datei muss im kodierten PEM-Format vorliegen.

Option	Beschreibung
<code>--privkey <Schlüsseldatei></code>	Name der privaten Schlüsseldatei. Die Datei muss im kodierten PEM-Format vorliegen.
<code>--config <Konfigurationsdatei></code>	Optionaler Name der Konfigurationsdatei. <code>certool.cfg</code> ist die Standardeinstellung.
<code>--server <Server></code>	Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“.

Beispiel:

```
certool --gencert --privkey=<filename> --cert=<filename>
```

certool --getrootca

Druckt das aktuelle Root-CA-Zertifikat in für Benutzer lesbarer Form. Wenn Sie diesen Befehl über einen Verwaltungsknoten ausführen, verwenden Sie den Maschinennamen des Platform Services Controller-Knotens zum Laden der Root-Zertifizierungsstelle. Diese Ausgabe ist nicht als Zertifikat nutzbar, sie wurde geändert, damit sie von Benutzern gelesen werden kann.

Option	Beschreibung
<code>--getrootca</code>	Ist zum Drucken des Rootzertifikats erforderlich.
<code>--server <Server></code>	Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“.

Beispiel:

```
certool --getrootca --server=remoteserver
```

certool --viewcert

Druckt alle Felder in einem Zertifikat in für Benutzer lesbarer Form.

Option	Beschreibung
<code>--viewcert</code>	Ist zum Anzeigen eines Zertifikats erforderlich.
<code>--cert <Zertifikatsdatei></code>	Optionaler Name der Konfigurationsdatei. <code>certool.cfg</code> ist die Standardeinstellung.

Beispiel:

```
certool --viewcert --cert=<filename>
```

certool --enumcert

Listet alle Zertifikate auf, die der VMCA-Server kennt. Mit der erforderlichen `Filter`-Option können Sie alle Zertifikate oder nur widerrufene, aktive oder abgelaufene Zertifikate auflisten.

Option	Beschreibung
<code>--enumcert</code>	Ist zum Auflisten aller Zertifikate erforderlich.
<code>--filter [all active]</code>	Erforderlicher Filter. Geben Sie „all“ oder „active“ an. Die Optionen „revoked“ und „expired“ werden derzeit nicht unterstützt.

Beispiel:

```
certool --enumcert --filter=active
```

certool --status

Sendet ein festgelegtes Zertifikat zum VMCA-Server, um zu prüfen, ob das Zertifikat widerrufen wurde. Druckt Zertifikat: WIDERRUFEN, wenn das Zertifikat widerrufen wurde, und ansonsten Zertifikat: AKTIV.

Option	Beschreibung
<code>--status</code>	Ist zum Prüfen des Status eines Zertifikats erforderlich.
<code>--cert <Zertifikatsdatei></code>	Optional Name der Konfigurationsdatei. <code>certool.cfg</code> ist die Standardeinstellung.
<code>--server <Server></code>	Optional Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“.

Beispiel:

```
certool --status --cert=<filename>
```

certool --genselfcert

Erstellt ein selbstsigniertes Zertifikat basierend auf den Werten in der Konfigurationsdatei. Dieser Befehl generiert ein um drei Tage rückdatiertes Zertifikat, um Zeitonenkonflikte zu vermeiden.

Option	Beschreibung
<code>--genselfcert</code>	Erforderlich zum Generieren eines selbstsignierten Zertifikats.
<code>--outcert <Zertifikatsdatei></code>	Name der Zertifikatsdatei. Die Datei muss im kodierten PEM-Format vorliegen.
<code>--outprivkey <Schlüsseldatei></code>	Name der privaten Schlüsseldatei. Die Datei muss im kodierten PEM-Format vorliegen.
<code>--config <Konfigurationsdatei></code>	Optional Name der Konfigurationsdatei. <code>certool.cfg</code> ist die Standardeinstellung.

Beispiel:

```
certool --genselfcert --privkey=<filename> --cert=<filename>
```

Befehlsreferenz für vecs-cli

Mit dem Befehlssatz `vecs-cli` können Sie die Instanzen des VMware-Zertifikatspeichers (VMware Certificate Store, VECS) verwalten. Verwenden Sie diese Befehle zusammen mit `dir-cli` und `certool`, um Ihre Zertifikatinfrastruktur zu verwalten.

vecs-cli store create

Erstellt einen Zertifikatspeicher.

Option	Beschreibung
<code>--name <name></code>	Der Name des Zertifikatspeichers.

Beispiel:

```
vecs-cli store create --name <store>
```

vecs-cli store delete

Löscht einen Zertifikatspeicher. Vom System vordefinierte Zertifikatspeicher können nicht gelöscht werden.

Option	Beschreibung
<code>--name <name></code>	Name des zu löschenden Zertifikatspeichers.

Beispiel:

```
vecs-cli store delete --name <store>
```

vecs-cli store list

Listet Zertifikatspeicher auf.

VECS enthält die folgenden Speicher.

Tabelle 3-6. Speicher in VECS

Speicher	Beschreibung
Maschinen-SSL-Speicher (MACHINE_SSL_CERT)	<ul style="list-style-type: none"> ■ Wird vom Reverse-Proxy-Dienst auf jedem vSphere-Knoten verwendet. ■ Wird vom VMware-Verzeichnisdienst (vmdir) für eingebettete Bereitstellungen und für jeden Platform Services Controller-Knoten verwendet. <p>Alle Dienste in vSphere 6.0 kommunizieren über einen Reverse-Proxy, der das Maschinen-SSL-Zertifikat verwendet. Aus Gründen der Abwärtskompatibilität verwenden die 5.x-Dienste weiterhin bestimmte Ports. Deshalb ist für bestimmte Dienste wie etwa vpxd ein eigener Port geöffnet.</p>
Vertrauenswürdiger Stammspeicher (TRUSTED_ROOTS)	Enthält alle vertrauenswürdigen Stammzertifikate.
Lösungsbenutzerspeicher <ul style="list-style-type: none"> ■ Maschine ■ vpxd ■ vpxd-extensions ■ vsphere-webclient 	<p>VECS enthält einen Speicher für jeden Lösungsbenutzer. Das Objekt jedes Lösungsbenutzerzertifikats muss eindeutig sein. So darf z. B. das Maschinenzertifikat nicht das gleiche Objekt wie das vpxd-Zertifikat haben.</p> <p>Lösungsbenutzerzertifikate werden für die Authentifizierung mit vCenter Single Sign On verwendet. vCenter Single Sign On überprüft, ob das Zertifikat gültig ist. Andere Zertifikatsattribute werden jedoch nicht überprüft. Bei einer eingebetteten Bereitstellung befinden sich alle Lösungsbenutzerzertifikate im selben System.</p> <p>Die folgenden Lösungsbenutzer-Zertifikatspeicher sind in VECS für jeden Verwaltungsknoten und für jede eingebettete Bereitstellung enthalten:</p> <ul style="list-style-type: none"> ■ <code>machine</code>: Wird vom Komponentenmanager, Lizenzserver und Protokollierungsdienst verwendet. <p>Hinweis Das Lösungsbenutzerzertifikat „machine“ hat nichts mit dem SSL-Zertifikat „machine“ zu tun. Das Lösungsbenutzerzertifikat „machine“ wird für den Austausch von SAML-Tokens verwendet; das SSL-Zertifikat „machine“ wird für sichere SSL-Verbindungen für eine Maschine verwendet.</p> <ul style="list-style-type: none"> ■ <code>vpxd</code>: vCenter-Dienst-Daemon (vpxd)-Speicher für Verwaltungsknoten und eingebettete Bereitstellungen. vpxd verwendet das in diesem Speicher gespeicherte Lösungsbenutzerzertifikat für die Authentifizierung bei vCenter Single Sign On. ■ <code>vpxd-extensions</code>: vCenter-Erweiterungsspeicher. Enthält den Auto Deploy-Dienst, den Inventory Service und sonstige Dienste, die nicht Bestandteil anderer Lösungsbenutzer sind. ■ <code>vsphere-webclient</code>: vSphere Web Client-Speicher. Enthält auch zusätzliche Dienste wie etwa den Leistungsdiagrammdienst. <p>Der Maschinenspeicher ist ebenfalls in jedem Platform Services Controller-Knoten enthalten.</p>

Tabelle 3-6. Speicher in VECS (Fortsetzung)

Speicher	Beschreibung
vSphere Certificate Manager Utility-Backup-Speicher (BACKUP_STORE)	Wird von VMCA (VMware Certificate Manager) für die Unterstützung der Zertifikatwiederherstellung verwendet. Nur der letzte Status wird als Backup gespeichert und Sie können nur den letzten Schritt rückgängig machen.
Weitere Speicher	<p>Weitere Speicher können durch Lösungen hinzugefügt werden. Beispielsweise fügt die VVOL-Lösung einen SMS-Speicher hinzu. Ändern Sie die Zertifikate in diesen Speichern nur, wenn Sie in VMware-Dokumentation oder in einem VMware-Knowledgebase-Artikel dazu aufgefordert werden.</p> <p>Hinweis CRLS werden in vSphere 6.0 nicht unterstützt. Dennoch kann durch das Löschen des TRUSTED_ROOTS_CRLS-Speichers Ihre Zertifikatinfrastruktur beschädigt werden. Den TRUSTED_ROOTS_CRLS-Speicher sollten Sie weder löschen noch ändern.</p>

Beispiel:

```
vecs-cli store list
```

vecs-cli store permissions

Erteilt oder widerruft die Berechtigungen für den Speicher. Verwenden Sie entweder die Option `--grant` (erteilen) oder die Option `--revoke` (widerrufen).

Der Besitzer des Speichers hat umfassende Kontrolle über seinen Speicher. Dazu gehört auch das Recht zum Erteilen und Widerrufen von Berechtigungen. Der Administrator besitzt Berechtigungen für alle Speicher, einschließlich des Rechts zum Erteilen und Widerrufen von Berechtigungen.

Mit `vecs-cli get-permissions --name <store-name>` können Sie die aktuellen Einstellungen des Speichers abrufen.

Option	Beschreibung
<code>--name <name></code>	Der Name des Zertifikatspeichers.
<code>--user <username></code>	Eindeutiger Name des Benutzers, dem Berechtigungen erteilt werden
<code>--grant [read write]</code>	Berechtigung, die erteilt wird: read (Lesen) oder write (Schreiben)
<code>--revoke [read write]</code>	Berechtigung, die widerrufen wird: read (Lesen) oder write (Schreiben). Wird derzeit nicht unterstützt.

vecs-cli entry create

Erstellen Sie einen Eintrag in VECS. Verwenden Sie diesen Befehl, um einen privaten Schlüssel in ein Zertifikat oder einen Speicher einzufügen.

Option	Beschreibung
--store <Zertifikatspeichername>	Der Name des Zertifikatspeichers.
--alias <Alias>	Der optionale Alias für das Zertifikat. Diese Option wird für den vertrauenswürdigen Stammzertifikatspeicher ignoriert.
--cert <Dateipfad_des_Zertifikats>	Der vollständige Pfad der Zertifikatsdatei.
--key <Dateipfad_des_Schlüssels>	Der vollständige Pfad des Schlüssels, der dem Zertifikat entspricht. Optional.

vecs-cli entry list

Listet alle Einträge im angegebenen Speicher auf.

Option	Beschreibung
--store <Zertifikatspeichername>	Der Name des Zertifikatspeichers.
--text	Zeigt eine von Benutzern lesbare Version des Zertifikats an.

vecs-cli entry getcert

Ruft ein Zertifikat aus dem VECS ab. Sie können das Zertifikat an eine Ausgabedatei senden oder als von Benutzern lesbaren Text anzeigen.

Option	Beschreibung
--store <Zertifikatspeichername>	Der Name des Zertifikatspeichers.
--alias <Alias>	Alias des Zertifikats
--output <output_file_path>	Datei, in die das Zertifikat geschrieben wird.
--text	Zeigt eine von Benutzern lesbare Version des Zertifikats an.

vecs-cli entry getkey

Ruft einen im VECS gespeicherten Schlüssel ab. Sie können das Zertifikat an eine Ausgabedatei senden oder als von Benutzern lesbaren Text anzeigen.

Option	Beschreibung
<code>--store <Zertifikatspeichername></code>	Der Name des Zertifikatspeichers.
<code>--alias <Alias></code>	Alias des Schlüssels
<code>--output <output_file_path></code>	Ausgabedatei, in die der Schlüssel geschrieben wird.
<code>--text</code>	Zeigt eine von Benutzern lesbare Version des Schlüssels an.

vecs-cli entry delete

Löscht einen Eintrag in einem Zertifikatspeicher. Wenn ein Eintrag aus dem VECS gelöscht wird, wird er dauerhaft aus dem VECS entfernt. Die einzige Ausnahme ist das aktuelle Stammzertifikat. VECS ruft ein Rootzertifikat aus vmdir ab.

Option	Beschreibung
<code>--store <Zertifikatspeichername></code>	Der Name des Zertifikatspeichers.
<code>--alias <Alias></code>	Alias des Eintrags, der gelöscht werden soll

vecs-cli force-refresh

Erzwingt die Aktualisierung von `vecs-cli`. Dabei wird `vecs-cli` aktualisiert, damit die aktuellsten Daten in vmdir genutzt werden. Standardmäßig sieht der VECS alle 5 Minuten im vmdir nach, ob ein neues Stammzertifikat vorliegt. Mit diesem Befehl wird der VECS sofort aus dem vmdir aktualisiert.

Befehlsreferenz für dir-cli

Mit dem Dienstprogramm `dir-cli` können Sie Lösungsbenutzer erstellen und aktualisieren, andere Benutzerkonten erstellen und Zertifikate und Kennwörter in vmdir verwalten. Verwenden Sie dieses Dienstprogramm zusammen mit `vecs-cli` und `certool`, um Ihre Zertifikatinfrastruktur zu verwalten.

dir-cli service create

Erstellt einen Lösungsbenutzer. Wird hauptsächlich für Lösungen von Drittanbietern verwendet.

Option	Beschreibung
<code>--name <name></code>	Name des zu erstellenden Lösungsbenutzers
<code>--cert <cert file></code>	Pfad zur Zertifikatdatei. Dies kann ein von VMCA signiertes Zertifikat oder ein Drittanbieterzertifikat sein.

Option	Beschreibung
<code>--login <Admin-Benutzer-ID></code>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
<code>--password <Admin-Kennwort></code>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli service list

Listet die Lösungsbenutzer auf, die `dir-cli` bekannt sind.

Option	Beschreibung
<code>--login <Admin-Benutzer-ID></code>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
<code>--password <Admin-Kennwort></code>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli service delete

Löscht einen Lösungsbenutzer in `vmdir`. Wenn Sie den Lösungsbenutzer löschen, sind alle zugehörigen Dienste für alle Verwaltungsknoten, die diese `vmdir`-Instanz verwenden, nicht mehr verfügbar.

Option	Beschreibung
<code>--name</code>	Name des zu löschenden Lösungsbenutzers.
<code>--login <Admin-Benutzer-ID></code>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
<code>--password <Admin-Kennwort></code>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli service update

Aktualisiert das Zertifikat für einen angegebenen Lösungsbenutzer, d. h. eine Sammlung von Diensten. Nach Ausführen dieses Befehls übernimmt VECS die Änderung nach 5 Minuten, oder Sie können `vecs-cli force-refresh` verwenden, um eine Aktualisierung zu erzwingen.

Option	Beschreibung
<code>--name <name></code>	Name des zu aktualisierenden Lösungsbenutzers
<code>--cert <cert_file></code>	Name des Zertifikats, das dem Dienst zugewiesen wird.

Option	Beschreibung
<code>--login <Admin-Benutzer-ID></code>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
<code>--password <Admin-Kennwort></code>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli user create

Erstellt einen regulären Benutzer innerhalb von vmdir. Dieser Befehl kann für Personen verwendet werden, die sich bei vCenter Single Sign On mit einem Benutzernamen und Kennwort authentifizieren. Verwenden Sie diesen Befehl beim Erstellen von Prototypen.

Option	Beschreibung
<code>--account <name></code>	Name des zu erstellenden vCenter Single Sign On-Benutzers
<code>--user-password <password></code>	Anfängliches Kennwort des Benutzers.
<code>--first-name <name></code>	Vorname des Benutzers.
<code>--last-name <name></code>	Nachname des Benutzers.
<code>--login <Admin-Benutzer-ID></code>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
<code>--password <Admin-Kennwort></code>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli user delete

Löscht den angegebenen Benutzer in vmdir.

Option	Beschreibung
<code>--account <name></code>	Name des zu löschenden vCenter Single Sign On-Benutzers
<code>--login <Admin-Benutzer-ID></code>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
<code>--password <Admin-Kennwort></code>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli group modify

Fügt einer vorhandenen Gruppe einen Benutzer oder eine Gruppe hinzu.

Option	Beschreibung
--name <name>	Name der Gruppe in vmdir.
--add <benutzer_oder_gruppenname>	Name des hinzuzufügenden Benutzers oder der Gruppe.
--login <Admin-Benutzer-ID>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
--password <Admin-Kennwort>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli group list

Listet eine angegebene vmdir-Gruppe auf.

Option	Beschreibung
--name <name>	Optionaler Name der Gruppe in vmdir. Mit dieser Option können Sie prüfen, ob eine Gruppe vorhanden ist.
--login <Admin-Benutzer-ID>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
--password <Admin-Kennwort>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli trustedcert publish

Veröffentlicht ein vertrauenswürdiges Root-Zertifikat in vmdir.

Option	Beschreibung
--cert <datei>	Pfad zur Zertifikatdatei.
--login <Admin-Benutzer-ID>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
--password <Admin-Kennwort>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli trustedcert unpublish

Hebt die Veröffentlichung eines vertrauenswürdigen Root-Zertifikats in vmdir auf. Verwenden Sie diesen Befehl beispielsweise, wenn Sie ein anderes Root-Zertifikat zu vmdir hinzugefügt haben, das jetzt das Root-Zertifikat für alle anderen Zertifikate in der Umgebung ist. Das Aufheben der Veröffentlichung von nicht mehr verwendeten Zertifikaten ist Bestandteil der Sicherung Ihrer Umgebung.

Option	Beschreibung
<code>--cert-file <datei></code>	Pfad zur Zertifikatsdatei, deren Veröffentlichung aufgehoben werden soll.
<code>--crl <datei></code>	Pfad zur diesem Zertifikat zugeordneten CRL-Datei. Wird derzeit nicht verwendet.
<code>--login <Admin-Benutzer-ID></code>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
<code>--password <Admin-Kennwort></code>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli trustedcert list

Listet alle vertrauenswürdigen Root-Zertifikate und deren IDs auf. Sie benötigen die Zertifikat-IDs, um ein Zertifikat mit `dir-cli trustedcert get` abzurufen.

Option	Beschreibung
<code>--login <Admin-Benutzer-ID></code>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
<code>--password <Admin-Kennwort></code>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli trustedcert get

Ruft ein vertrauenswürdiges Stammzertifikat aus vmdir ab und schreibt es in eine angegebene Datei.

Option	Beschreibung
<code>--id <zert_ID></code>	ID des abzurufenden Zertifikats. Die ID wird im Befehl <code>dir-cli trustedcert list</code> angezeigt.
<code>--outcert <pfad></code>	Pfad, in den die Zertifikatsdatei geschrieben wird.
<code>--outcrl <pfad></code>	Pfad, in den die CRL-Datei geschrieben wird. Wird derzeit nicht verwendet.
<code>--login <Admin-Benutzer-ID></code>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
<code>--password <Admin-Kennwort></code>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli password create

Erstellt ein zufälliges Kennwort, das die Kennwortanforderungen erfüllt. Dieser Befehl kann von Benutzern von Drittanbieterlösungen verwendet werden.

Option	Beschreibung
<code>--login <Admin-Benutzer-ID></code>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
<code>--password <Admin-Kennwort></code>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli password reset

Damit kann ein Administrator ein Benutzerkennwort zurücksetzen. Wenn Sie kein Administratorbenutzer sind und ein Kennwort zurücksetzen möchten, verwenden Sie stattdessen `dir-cli password change`.

Option	Beschreibung
<code>--account</code>	Name des Kontos, dem ein neues Kennwort zugewiesen werden soll.
<code>--new</code>	Neues Kennwort für den angegebenen Benutzer.
<code>--login <Admin-Benutzer-ID></code>	Standardmäßig administrator@vsphere.local. Dieser Administrator kann andere Benutzer zur vCenter Single Sign On-Gruppe „CAAdmins“ hinzufügen, um ihnen Administratorrechte zu erteilen.
<code>--password <Admin-Kennwort></code>	Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert.

dir-cli password change

Damit kann ein Benutzer sein Kennwort ändern. Sie können diese Änderung nur vornehmen, wenn Sie der Besitzer des Benutzerkontos sind. Administratoren können jedes beliebige Kennwort mit `dir-cli password reset` zurücksetzen.

Option	Beschreibung
<code>--account</code>	Kontoname.
<code>--current</code>	Aktuelles Kennwort des Benutzers, der Besitzer des Kontos ist.
<code>--new</code>	Neues Kennwort des Benutzers, der Besitzer des Kontos ist.

Anzeigen von vCenter-Zertifikaten mit dem vSphere Web Client

Sie können die der VMware-Zertifizierungsstelle (VMCA) bekannten Zertifikate anzeigen, um festzustellen, ob aktive Zertifikate demnächst ablaufen, um abgelaufene Zertifikate zu überprüfen und um den Status des Rootzertifikats anzuzeigen. Alle Zertifikatsverwaltungsaufgaben führen Sie mit den Zertifikatsverwaltungs-CLIs aus.

Sie zeigen Zertifikate für die VMCA-Instanz an, die in Ihrer eingebetteten Bereitstellung oder im Platform Services Controller enthalten ist. Zertifikatsinformationen werden für die Instanzen des VMware-Verzeichnisdiensts (vmdir) repliziert.

Wenn Sie versuchen, Zertifikate im vSphere Web Client anzuzeigen, werden Sie zur Eingabe eines Benutzernamens und eines Kennworts aufgefordert. Geben Sie den Benutzernamen und das Kennwort eines Benutzers mit Rechten für die VMware-Zertifizierungsstelle an, d. h., eines Benutzers in der vCenter Single Sign On-Gruppe „CAAdmins“.

Verfahren

- 1 Melden Sie sich bei vCenter Server als „administrator@vsphere.local“ oder als ein anderer Benutzer der vCenter Single Sign On-Gruppe „CAAdmins“ an.
- 2 Wählen Sie **Verwaltung** aus, klicken Sie auf **Bereitstellung** und klicken Sie dann auf **Systemkonfiguration**.
- 3 Klicken Sie auf **Knoten** und wählen Sie den Knoten aus, für den Sie Zertifikate anzeigen oder verwalten möchten.
- 4 Klicken Sie auf die Registerkarte **Verwalten** und klicken Sie anschließend auf **Zertifizierungsstelle**.
- 5 Klicken Sie auf den Zertifikatstyp, für den Sie Zertifikatsinformation anzeigen möchten.

Option	Beschreibung
Aktive Zertifikate	Zeigt aktive Zertifikate einschließlich der Validierungsinformationen an. Das grüne Symbol „Gültig bis“ wird geändert, wenn das Zertifikat demnächst abläuft.
Widerrufene Zertifikate	Zeigt die Liste der widerrufenen Zertifikate an. Dies wird in dieser Version nicht unterstützt.
Abgelaufene Zertifikate	Listet abgelaufene Zertifikate auf.
Rootzertifikate	Zeigt die für diese Instanz der VMware-Zertifizierungsstelle verfügbaren Rootzertifikate an.

- 6 Wählen Sie ein Zertifikat aus und klicken Sie auf die Schaltfläche **Zertifikatsdetails anzeigen**, um die Zertifikatsdetails anzuzeigen.

Zu den Details gehören der Subjektnamen, der Aussteller, die Gültigkeit und der Algorithmus.

Festlegen des Schwellenwerts für Warnungen zum Ablauf von vCenter-Zertifikaten

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

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie das vCenter Server-Objekt aus und klicken Sie dann auf die Registerkarte **Verwalten** und auf die Unterregisterkarte **Einstellungen**.
- 3 Klicken Sie auf **Erweiterte Einstellungen**, wählen Sie **Bearbeiten** aus und filtern Sie nach dem Schwellenwert.
- 4 Ändern Sie die Einstellung von „vpzd.cert.threshold“ auf den gewünschten Wert und klicken Sie auf **OK**.

vSphere-Berechtigungen und Benutzerverwaltungsaufgaben

4

vCenter Single Sign On unterstützt die Authentifizierung, d. h., es wird bestimmt, ob ein Benutzer überhaupt auf vSphere-Komponenten zugreifen kann. Darüber hinaus muss jeder Benutzer autorisiert werden, um vSphere-Objekte anzeigen oder bearbeiten zu können.

vSphere unterstützt verschiedene Autorisierungsmechanismen, die im Abschnitt [Grundlegende Informationen zur Autorisierung in vSphere](#) behandelt werden. Den Schwerpunkt der Informationen in diesem Abschnitt bilden das vCenter Server-Berechtigungsmodell und 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.

Anfangs ist nur der Benutzer „administrator@vsphere.local“ berechtigt, sich beim vCenter Server-System anzumelden. Dieser Benutzer kann dann folgende Schritte ausführen:

- 1 Hinzufügen einer Identitätsquelle, in der zusätzliche Benutzer und Gruppen definiert sind, zu vCenter Single Sign On. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer vCenter Single Sign On-Identitätsquelle](#).
- 2 Erteilen von Rechten für einen Benutzer oder eine Gruppe, indem er ein Objekt wie etwa eine virtuelle Maschine oder ein vCenter Server-System auswählt und für dieses Objekt dem Benutzer oder der Gruppe eine Rolle zuweist.



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](#)
- [Grundlegendes zum vCenter Server-Berechtigungsmodell](#)
- [Hierarchische Vererbung von Berechtigungen](#)
- [Einstellungen für Mehrfachberechtigungen](#)
- [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

Die Hauptmethode zur Autorisierung eines Benutzers oder einer Gruppe in vSphere sind vCenter Server-Berechtigungen. Je nach geplanter Aufgabe benötigen Sie möglicherweise weitere Autorisierungen.

vSphere 6.0 und höher erlauben berechtigten Benutzern, anderen Benutzern Berechtigungen zur Ausführung von Aufgaben zu erteilen, und zwar wie unten angegeben. Diese Ansätze schließen sich zum Großteil gegenseitig aus, aber mit globalen Berechtigungen können Sie bestimmte Benutzer für alle Lösungen autorisieren. Mit lokalen vCenter Server-Berechtigungen autorisieren Sie andere Benutzer für einzelne vCenter Server-Systeme.

vCenter Server-Berechtigungen

Das Berechtigungsmodell für vCenter Server-Systeme basiert auf der Zuweisung von Berechtigungen zu Objekten in der Objekthierarchie von vCenter Server. Jede Berechtigung erteilt einem Benutzer oder einer Gruppe eine Reihe von Berechtigungen (d. h. eine Rolle) für das ausgewählte Objekt. Sie können beispielsweise einen ESXi-Host auswählen und einer Benutzergruppe eine Rolle zuweisen, um diesen Benutzern die entsprechenden Berechtigungen für den betreffenden Host zu erteilen.

Globale Berechtigungen

Globale Berechtigungen werden auf ein globales Stammobjekt angewendet, das für mehrere Lösungen verwendet wird. Wenn z. B. vCenter Server und vCenter Orchestrator installiert sind, können Sie Berechtigungen für alle Objekte in beiden Objekthierarchien erteilen.

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. Siehe [Globale Berechtigungen](#).

Gruppenmitgliedschaft in vsphere.local-Gruppen

Der Benutzer „administrator@vsphere.local“ kann alle Aufgaben im Zusammenhang mit den Diensten im Platform Services Controller ausführen. Die Mitglieder einer vsphere.local-Gruppe haben das Recht, die der Gruppe zugehörigen Aufgaben durchzuführen. Wenn Sie beispielsweise Mitglied der Gruppe „LicenseService.Administrators“ sind, dürfen Sie Lizenzen verwalten. Siehe [Gruppen in der Domäne „vsphere.local“](#).

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 *vSphere-Verwaltung mit dem vSphere Client*.

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.

Mit den folgenden Konzepten sollten Sie 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.

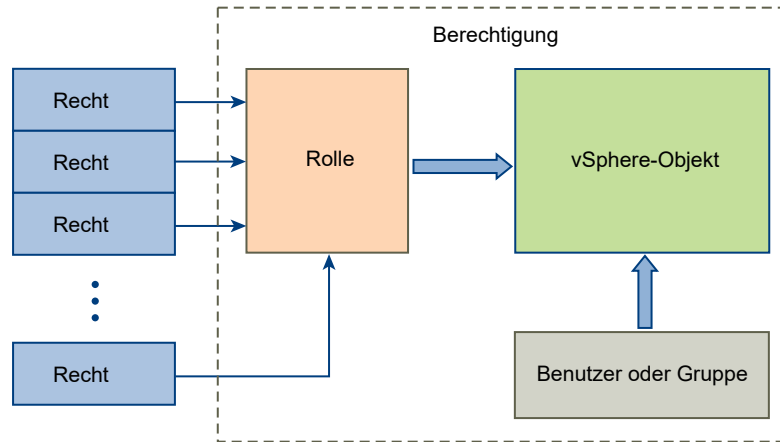
Rollen

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.

Rechte

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

Abbildung 4-1. vSphere-Berechtigungen



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

- 1 Wählen Sie das Objekt in der vCenter-Objekthierarchie aus, auf die Sie die Berechtigung 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 die Rolle (d. h. die Gruppe von Rechten) aus, die Sie der Gruppe oder Benutzer für das Objekt erteilen möchten. Berechtigungen werden standardmäßig weitergegeben, d. h., die Gruppe oder der Benutzer verfügt über die ausgewählte Rolle für das ausgewählte Objekt und dessen untergeordnete Objekte.

Das Berechtigungsmodell vereinfacht und beschleunigt das Arbeiten mithilfe vordefinierter Rollen. Sie können auch Rechte zusammenfassen, um benutzerdefinierte Rollen zu erstellen. In [Kapitel 11 Definierte Rechte](#) finden Sie Informationen zu allen Rechten und zu den Objekten, auf die Sie die Rechte anwenden können. Unter [Erforderliche Berechtigungen für allgemeine Aufgaben](#) finden Sie Beispiele zu den Rechten, die Sie zum Ausführen dieser Aufgaben benötigen.

In vielen Fällen müssen Berechtigungen sowohl für ein Quellobjekt 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.

Das Berechtigungsmodell für eigenständige ESXi-Hosts ist einfacher. Siehe [Zuweisen der Berechtigungen für ESXi](#).

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. Wenn beispielsweise dem Benutzer „Schmidt“ eine Rolle für mehrere Objekte zugewiesen wurde und der Benutzername in der Domäne in „Schmidt2“ geändert wird, schließt der Host daraus, dass der Benutzer „Schmidt“ nicht mehr vorhanden ist, und entfernt die Berechtigungen für diesen Benutzer bei der nächsten Validierung 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 ein neuer Benutzer „Schmidt“ vor der nächsten Validierung zur Domäne hinzugefügt wird, ersetzt der neue Benutzer in den Berechtigungen für alle Objekte den alten Benutzer.

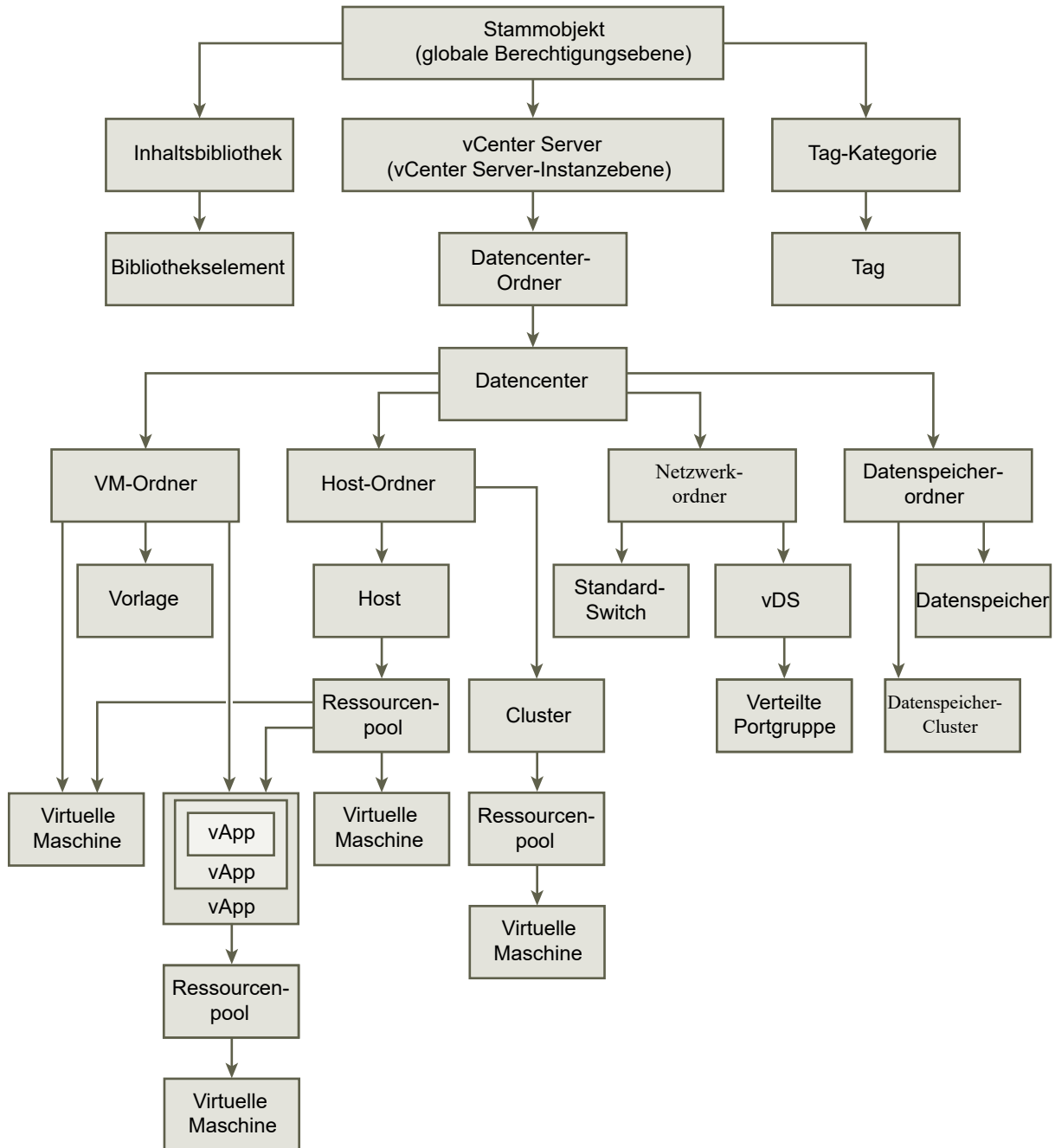
Hierarchische Vererbung von Berechtigungen

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 4-2. vSphere-Bestandslistenhierarchie



Die meisten Bestandslistenobjekte übernehmen Berechtigungen von einem einzelnen übergeordneten Objekt in der Hierarchie. Beispielsweise 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. Beispielsweise könnte eine Berechtigung festlegen, dass die Gruppe A über Administratorrechte für ein Objekt verfügt. Eine weitere Berechtigung könnte festlegen, dass Gruppe B über VM-Administratorrechte für dasselbe Objekt verfügt.

Wenn ein Objekt Berechtigungen von zwei übergeordneten Objekten erbt, werden die Berechtigungen für ein Objekt zu den Berechtigungen für das andere Objekt hinzugefügt. Wenn sich beispielsweise eine virtuelle Maschine in einem VM-Ordner befindet und außerdem zu einem Ressourcenpool gehört, erbt diese virtuelle Maschine 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:

- Wenn dem Benutzer für dieses Objekt keine Berechtigungen gewährt wurden, wird dem Benutzer der Satz an Berechtigungen zugewiesen, der den Gruppen für dieses Objekt zugewiesen wurden.
- Wenn dem Benutzer eine Berechtigung für das Objekt gewährt wurde, hat diese Berechtigung Vorrang vor allen Gruppenberechtigungen.

Beispiel 1: Vererbung von mehreren Berechtigungen

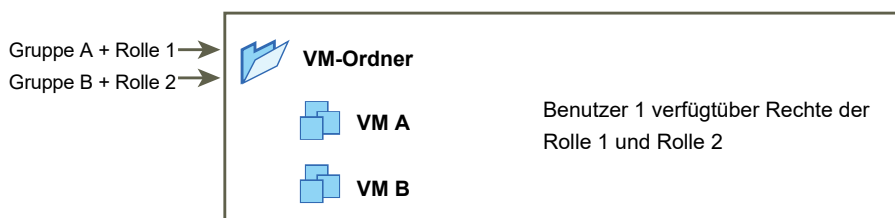
Dieses Beispiel zeigt, wie ein Objekt mehrere Berechtigungen von Gruppen übernehmen kann, die auf einem übergeordneten Objekt Berechtigungen erhalten haben.

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 4-3. Beispiel 1: Vererbung von mehreren Berechtigungen



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

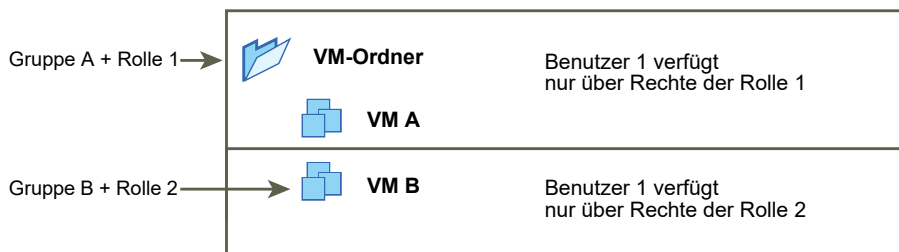
Dieses Beispiel zeigt, wie Berechtigungen, die einem untergeordneten Objekt zugewiesen wurden, die Berechtigungen, die einem übergeordneten Objekt zugewiesen wurden, außer Kraft setzen. Sie können dieses Verhalten dazu verwenden, um den Benutzerzugriff auf bestimmte Bereiche der Bestandsliste einzuschränken.

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 4-4. Beispiel 2: Untergeordnete Berechtigungen, die übergeordnete Berechtigungen außer Kraft setzen



Beispiel 3: Überschreiben der Gruppenrolle durch die Benutzerrolle

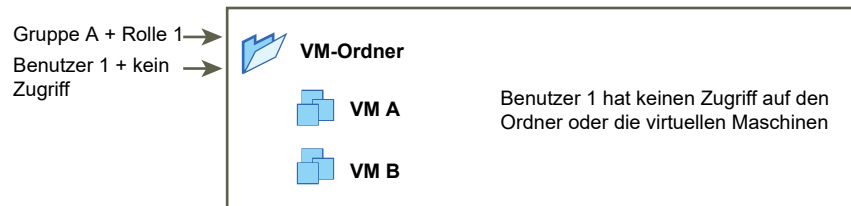
Dieses Beispiel zeigt, wie die einem individuellen Benutzer direkt zugewiesene Rolle die Rechte einer Rolle überschreibt, die einer Gruppe zugeordnet ist.

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 4-5. 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.

Rollen

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.

Rechte

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

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 Wählen Sie die Registerkarte **Verwalten** aus und klicken Sie auf **Berechtigungen**.
- 3 Klicken Sie auf das Symbol „Hinzufügen“ und klicken Sie dann auf **Hinzufügen**.

- 4 Identifizieren Sie den Benutzer oder die Gruppe, für den die Rechte mithilfe der ausgewählten Rolle definiert werden.
 - a Wählen Sie im Dropdown-Menü **Domäne** die Domäne aus, in der sich der Benutzer oder die Gruppe befindet.
 - b Geben Sie einen Namen im Feld „Suchen“ ein oder wählen Sie einen Namen aus der Liste aus.
Das System sucht 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 Berechtigungen, 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 Wählen Sie die Registerkarte **Verwalten** aus und klicken Sie auf **Berechtigungen**.
- 3 Klicken Sie auf das entsprechende Element, um die Kombination aus Rolle und Benutzer oder Gruppe auszuwählen.
- 4 Klicken Sie auf **Rolle für Berechtigung ändern**.
- 5 Wählen Sie aus dem Dropdown-Menü **Zugewiesene Rolle** die entsprechende Rolle für den Benutzer oder die Gruppe aus.
- 6 Um die Rechte für die untergeordneten Elemente des zugewiesenen Bestandslistenobjekts zu übernehmen, aktivieren Sie das Kontrollkästchen **Weitergeben** und klicken Sie auf **OK**.

Entfernen von Berechtigungen

Sie können die Berechtigungen zu einem Objekt in der Objekthierarchie für einzelne Benutzer oder für Gruppen entfernen. Wenn Sie dies tun, verfügt der Benutzer nicht mehr über die Berechtigungen, die mit der Rolle zum Objekt verknüpft sind.

Verfahren

- 1 Navigieren Sie zum Objekt im Objektnavigator von vSphere Web Client.
- 2 Wählen Sie die Registerkarte **Verwalten** aus und klicken Sie auf **Berechtigungen**.
- 3 Klicken Sie auf das entsprechende Element, um die Kombination aus Rolle und Benutzer oder Gruppe auszuwählen.
- 4 Klicken Sie auf **Berechtigung entfernen**.

Ergebnisse

vCenter Server entfernt die Berechtigungseinstellung.

Ändern der Einstellungen für die Berechtigungsvalidierung

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 auf diese Weise nicht durchsucht werden.

Verfahren

- 1 Navigieren Sie im Objektnavigator des vSphere Web Client zum vCenter Server-System.
- 2 Wählen Sie die Registerkarte **Verwalten** und klicken Sie auf **Einstellungen**.
- 3 Klicken Sie auf **Allgemein** und anschließend auf **Bearbeiten**.
- 4 Wählen Sie **Benutzerverzeichnis** aus.

5 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 von Benutzern und Gruppen festzulegen, die vCenter Server anzeigt.
Größe der Abfragegrenze	Legt die maximale Anzahl von Benutzern und Gruppen fest, die vCenter Server von der ausgewählten Domäne im Dialogfeld Benutzer oder Gruppen auswählen anzeigt. 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.

6 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 vCenter 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 jedes Lösungsobjekt. Sie können Benutzern oder Gruppen globale Berechtigungen zuweisen und für jeden Benutzer oder jede Gruppe die Rolle festlegen. Die Rolle bestimmt die verfügbaren Rechte. Sie können eine vordefinierte Rolle zuweisen oder benutzerdefinierte Rollen erstellen. Siehe [Verwenden von Rollen zum Zuweisen von Rechten](#). Sie sollten unbedingt zwischen vCenter Server-Berechtigungen und globalen Berechtigungen unterscheiden.

vCenter Server-Berechtigungen

In den meisten Fällen wenden Sie eine Berechtigung auf ein vCenter Server-Bestandslistenobjekt an, wie beispielsweise ein 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. Stellen Sie sicher, dass Sie wirklich allen Objekten in allen Bestandslistenhierarchien Berechtigungen zuweisen möchten.

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.

Globale Berechtigungen sollten Sie mit Vorsicht verwenden. Stellen Sie sicher, dass Sie wirklich allen Objekten in allen Bestandslistenhierarchien Berechtigungen zuweisen möchten.

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 klicken Sie dann auf das Symbol „Berechtigung hinzufügen“.
- 3 Identifizieren Sie den Benutzer oder die Gruppe, für den die Rechte mithilfe der ausgewählten Rolle definiert werden.
 - a Wählen Sie im Dropdown-Menü **Domäne** die Domäne aus, in der sich der Benutzer oder die Gruppe befindet.
 - b Geben Sie einen Namen im Feld „Suchen“ ein oder wählen Sie einen Namen aus der Liste aus.
Das System sucht 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 Berechtigungen, die dieser Rolle zugewiesen sind, werden im Bereich unterhalb des Rollennamens aufgelistet.

- 5 Das Kontrollkästchen „An untergeordnete Objekte weitergeben“ sollten Sie in den meisten Fällen aktiviert lassen.

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 4-1. 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 das Root-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 4-2. 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 4-3. 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 Leseigenschaften und Rechte zum Ausführen von Aktionen. So besteht die Rolle des Administrators für virtuelle Maschinen beispielsweise aus Leseigenschaften und dem Recht zum Ausführen bestimmter Aktionen. Die Rolle erlaubt dem Benutzer, die Attribute virtueller Maschinen 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.

Wenn z. B. die beiden Ressourcenpools Pool A und Pool B in Ihrer Bestandsliste vorhanden sind, können Sie einem Benutzer für Pool A die Rolle „Benutzer virtueller Maschinen“ und für Pool B die Rolle „Nur Lesen“ zuweisen. Dieser Benutzer darf dann die virtuellen Maschinen in Pool A einschalten, jene in Pool B aber nur anzeigen.

vCenter Server umfasst standardmäßig Systemrollen 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 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

Benutzerdefinierte Rollen können Sie für vCenter Server und alle damit verwalteten Objekte erstellen, oder aber für einzelne Hosts.

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

Benutzerdefinierte Rollen können Sie für einzelne Hosts mit einem CLI-Befehl oder mit dem vSphere Client erstellen. Weitere Informationen finden Sie in der Dokumentation *vSphere-Verwaltung mit dem vSphere Client*. Auf benutzerdefinierte Hostrollen ist in vCenter Server kein Zugriff möglich.

Wenn Sie ESXi-Hosts über vCenter Server verwalten, beachten Sie, dass die Verwendung benutzerdefinierter Rollen auf dem Host und in vCenter Server zu Verwirrung und Missbrauch führen kann. In den meisten Fällen wird die Definition von vCenter Server-Rollen empfohlen.

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 und ihr keine Rechte zuweisen, wird die Rolle als eine schreibgeschützte Rolle mit drei systemdefinierten Rechten erstellt:

System.Anonymous, System.View und System.Read.



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 ein paar wenige 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, denen die Administrator-Rolle für ein Objekt zugewiesen wurde, 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 Zugriff“

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

Der Benutzer „administrator@vsphere.local“, der Root-Benutzer und vpxuser sind die einzigen Benutzer, denen standardmäßig nicht die Rolle „Kein Zugriff“ zugewiesen wird. Stattdessen wird ihnen die Rolle Administrator zugewiesen. Sie können die Berechtigungen des Root-

Benutzers entfernen oder seine Rolle in „Kein Zugriff“ ändern, sofern Sie zunächst auf Root-Ebene eine Ersatzberechtigung mit der Administratorrolle erstellen und diese Berechtigung einem anderen Benutzer zuordnen.

Rolle „Nur Lesen“

Benutzer, denen die Rolle „Nur Lesen“ für ein Objekt zugewiesen wurde, können den Status des Objekts und Details zum Objekt anzeigen. Mit dieser Rolle kann ein Benutzer die virtuelle Maschine, den Host und die Ressourcenpoolattribute anzeigen. Der Benutzer kann jedoch nicht die Remotekonsole eines Hosts anzeigen. Alle Vorgänge über die Menüs und Symbolleisten sind nicht zugelassen.

Erstellen einer benutzerdefinierten Rolle

Sie können benutzerdefinierte Rollen für vCenter Server erstellen, die den in Ihrer Umgebung bestehenden Anforderungen hinsichtlich der Zugriffssteuerung entsprechen.

Wenn Sie auf einem vCenter Server-System, das zur selben vCenter Single Sign-On-Domäne wie andere vCenter Server-Systeme gehört, eine Rolle erstellen oder bearbeiten, werden die vorgenommenen Änderungen vom VMware-Verzeichnisdienst (vmdir) an alle anderen vCenter Server-Systeme der Gruppe weitergegeben. 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 Klicken Sie auf die Schaltfläche **Rollenaktion erstellen**.
- 4 Geben Sie einen Namen für die neue Rolle ein.
- 5 Wählen Sie Berechtigungen für die Rolle aus und klicken Sie auf **OK**.

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.

Wenn Sie auf einem vCenter Server-System, das zur selben vCenter Single Sign-On-Domäne wie andere vCenter Server-Systeme gehört, eine Rolle erstellen oder bearbeiten, werden die vorgenommenen Änderungen vom VMware-Verzeichnisdienst (vmdir) an alle anderen vCenter Server-Systeme der Gruppe weitergegeben. 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.

Wenn Sie auf einem vCenter Server-System, das zur selben vCenter Single Sign-On-Domäne wie andere vCenter Server-Systeme gehört, eine Rolle erstellen oder bearbeiten, werden die vorgenommenen Änderungen vom VMware-Verzeichnisdienst (vmdir) an alle anderen vCenter Server-Systeme der Gruppe weitergegeben. 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:

- Weisen Sie eine Rolle nach Möglichkeit nicht einzelnen Benutzern, sondern einer Gruppe zu, um dieser Gruppe Rechte zu erteilen.

- Erteilen Sie Berechtigungen nur für die entsprechenden erforderlichen Objekte und weisen Sie Rechte nur den entsprechenden erforderlichen Benutzern oder Gruppen zu. Die Vergabe von so wenigen Berechtigungen wie möglich erleichtert das Verstehen und Verwalten Ihrer Berechtigungsstruktur.
- Wenn Sie einer Gruppe eine restriktive Rolle zuweisen, überprüfen Sie, dass die Gruppe weder den Administrator noch Benutzer mit Administratorrechten enthält. Anderenfalls könnten Sie die Rechte eines Administrators in den Teilen der Bestandslistenhierarchie ungewollt einschränken, für die Sie der Gruppe die restriktive Rolle zugewiesen haben.
- Verwenden Sie Ordner, um Objekte zu gruppieren. Wenn Sie z. B. einer Hostgruppe die Änderungsberechtigung und einer anderen Hostgruppe die Anzeigeberechtigung zuweisen möchten, 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.
- In den meisten Fällen sollten Sie beim Zuweisen von Berechtigungen zu einem Objekt die Weitergabe aktivieren. Dadurch wird sichergestellt, dass neue Objekte beim Einfügen in die Bestandslistenhierarchie die Berechtigungen übernehmen und für Benutzer verfügbar sind.
- Verwenden Sie die Rolle „Kein Zugriff“, um bestimmte Bereiche der Hierarchie zu maskieren, wenn bestimmte Benutzer oder Gruppen keinen Zugriff auf die Objekte in diesem Bereich der Objekthierarchie erhalten sollen.
- Änderungen an Lizenzen werden an alle vCenter Server-Systeme weitergegeben, die mit demselben Platform Services Controller oder mit Platform Services Controller-Instanzen in derselben vCenter Single Sign On-Domäne verknüpft sind, und zwar auch dann, wenn der Benutzer nicht über Berechtigungen für alle vCenter Server-Systeme verfügt.

Erforderliche Berechtigungen für allgemeine Aufgaben

Viele Aufgaben erfordern Berechtigungen für mehr als ein Objekt in der Bestandsliste. Sie können die Rechte, die zum Durchführen der Aufgaben erforderlich sind, sowie ggf. die entsprechenden Beispielrollen überprüfen.

In der folgenden Tabelle werden allgemeine Aufgaben aufgelistet, die mehrere Rechte erfordern. Sie können Berechtigungen zu Bestandslistenobjekten hinzufügen, indem Sie einem Benutzer eine der vordefinierten Rollen zuordnen. Sie können aber auch benutzerdefinierte Rollen mit den Rechten erstellen, die Ihrer Ansicht nach mehrmals verwendet werden.

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

- Jeder Vorgang, der Speicherplatz benötigt, wie z. B. das Erstellen einer virtuellen Festplatte oder eines Snapshots, erfordert das Recht **Datenspeicher.Speicher zuteilen** auf dem Zieldatenspeicher und das Recht, den Vorgang selbst durchzuführen.
- 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 **Ressourcen.Virtuelle Maschine zu Ressourcenpool zuweisen**.

Tabelle 4-4. Erforderliche Berechtigungen für allgemeine Aufgaben

Aufgabe	Erforderliche Berechtigungen	Gültige Rolle
Erstellen einer virtuellen Maschine	Im Zielordner oder Datencenter:	Administrator
	■ 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)	
	Auf dem Zielhost, -cluster oder -ressourcenpool: Ressourcen.Virtuelle Maschine zu Ressourcenpool zuweisen	Ressourcenpool-Administrator oder Administrator
	Auf dem Zieldatenspeicher oder -ordner, der einen Datenspeicher enthält: Datenspeicher.Speicher zuteilen	Datenspeicherkonsument oder Administrator
	Im Netzwerk, dem die virtuelle Maschine zugewiesen wird: Netzwerk.Netzwerk zuweisen	Netzwerkkonsument oder Administrator
Virtuelle Maschine aus einer Vorlage bereitstellen	Im Zielordner oder Datencenter:	Administrator
	■ Virtuelle Maschine.Bestandsliste.Aus vorhandener erstellen	
	■ Virtuelle Maschine.Konfiguration.Neue Festplatte hinzufügen	
	In einer Vorlage oder einem Vorlagenordner: Virtuelle Maschine.Bereitstellung.Vorlage bereitstellen	Administrator
	Auf dem Zielhost, -cluster oder -ressourcenpool: Ressourcen.Virtuelle Maschine zu Ressourcenpool zuweisen	Administrator
	Auf dem Zieldatenspeicher oder -datenspeicherordner: Datenspeicher.Speicher zuteilen	Datenspeicherkonsument oder Administrator

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

Aufgabe	Erforderliche Berechtigungen	Gültige Rolle
	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
Verschieben einer virtuellen Maschine in einen Ressourcenpool	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: <ul style="list-style-type: none"> ■ Ressourcen.Virtuelle Maschine zu Ressourcenpool zuweisen ■ Virtuelle Maschine.Bestandsliste.Verschieben 	Administrator
	Auf dem Zielressourcenpool: Ressourcen.Virtuelle Maschine zu Ressourcenpool zuweisen	Administrator
Installieren eines Gastbetriebssystems auf einer virtuellen Maschine	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: <ul style="list-style-type: none"> ■ 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 mit dem Installationsmedium ISO-Image: 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: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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 zu Ressourcenpool zuweisen	Ressourcenpool-Administrator oder Administrator

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

Aufgabe	Erforderliche Berechtigungen	Gültige Rolle
Cold-Migration (Verlagern) einer virtuellen Maschine	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: <ul style="list-style-type: none"> ■ Ressourcen.Ausgeschaltete virtuelle Maschine migrieren ■ Ressourcen.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 zu Ressourcenpool zuweisen	Ressourcenpool-Administrator oder Administrator
	Auf dem Zieldatenspeicher (wenn anders als die Quelle): Datenspeicher.Speicher zuteilen	Datenspeicherkonsument oder Administrator
Migrieren einer virtuellen Maschine mit Storage vMotion	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: Ressourcen.Eingeschaltete virtuelle Maschine migrieren	Ressourcenpool-Administrator oder Administrator
	Auf dem Zieldatenspeicher: Datenspeicher.Speicher zuteilen	Datenspeicherkonsument oder Administrator
Einen Host in einen Cluster verschieben	Auf dem Host: Host.Bestandsliste.Host zu Cluster hinzufügen	Administrator
	Auf dem Zielcluster: Host.Bestandsliste.Host zu Cluster hinzufügen	Administrator

Sichern der ESXi-Hosts

5

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-Zertifizierungsstelle (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:

- Verwenden von Skripts zum Verwalten von Hostkonfigurationseinstellungen
- Konfigurieren von ESXi-Hosts mit Hostprofilen
- Allgemeine ESXi-Sicherheitsempfehlungen
- Zertifikatsverwaltung für ESXi-Hosts
- Anpassen von Hosts mit dem Sicherheitsprofil
- Zuweisen der Berechtigungen für ESXi
- Verwenden von Active Directory zum Verwalten von ESXi-Benutzern
- Verwenden des vSphere Authentication Proxy
- Empfohlene Vorgehensweisen für die Sicherheit von ESXi
- Konfigurieren der Smartcard-Authentifizierung für ESXi
- ESXi-SSH-Schlüssel
- Verwenden der ESXi Shell
- Ändern von ESXi-Web-Proxy-Einstellungen
- vSphere Auto Deploy-Sicherheitsüberlegungen

■ Verwalten der ESXi-Protokolldateien

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)	<pre>esxcli <conn_options> system settings advanced get / UserVars/ESXiShellTimeout</pre> <pre>esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list grep /UserVars/ ESXiShellTimeout</pre>
PowerCLI	<pre>#List UserVars.ESXiShellInteractiveTimeout for each host Get-VMHost Select Name, @{N="UserVars.ESXiShellInteractiveTimeout";E={\$_ Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeout Select -ExpandProperty Value}}</pre> <pre># Set UserVars.ESXiShellTimeout to 900 on all hosts Get-VMHost Foreach { Get-AdvancedSetting -Entity \$_ -Name UserVars.ESXiShellInteractiveTimeout Set- AdvancedSetting -Value 900 }</pre>

- 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.

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, Permanentenspeicher, 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. Wenn Sie dies tun, vergewissern Sie sich, dass Sie in einer vertrauenswürdigen Umgebung arbeiten und dass Sie ausreichend andere Sicherheitsmaßnahmen ergriffen haben, um das Netzwerk insgesamt und die mit dem Host verbundenen Geräte zu schützen.

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 speziell für den Verwaltungszugriff auf den Host notwendig sind, geschlossen. Wenn Sie zusätzliche Dienste benötigen, müssen Sie die jeweiligen Ports öffnen.
- 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. Auf ESXi erstellte Standardzertifikate verwenden PKCS#1 SHA-256 mit RSA-Verschlüsselung als Signaturalgorithmus.
- Der Webservice Tomcat, der intern von ESXi verwendet wird, um den Zugriff von Webclients zu unterstützen, wurde so angepasst, dass nur diejenigen Funktionen ausgeführt werden, die für die Verwaltung und Überwachung von einem Webclient erforderlich sind. 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 könnten, und gibt, falls erforderlich, 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 der unsicheren Dienste zugunsten der sichereren Alternativen verzichten. 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.

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 auf verwaltete Hosts nicht direkt mit dem vSphere Client zu, und nehmen Sie keine Änderungen an verwalteten Hosts über die DCUI des Hosts vor.

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 den vSphere Client oder VMware CLIs oder APIs zum Verwalten eigenständiger ESXi-Hosts.

Verwenden Sie den vSphere Client, eine der VMware CLIs oder APIs zum Verwalten Ihrer ESXi-Hosts. Greifen Sie als Root-Benutzer nur zur Fehlerbehebung von der DCUI oder der ESXi Shell auf den Host zu. Wenn Sie die ESXi Shell verwenden möchten, beschränken Sie die Konten mit Zugriff und legen Sie Zeitüberschreitungen fest.

Verwenden Sie nur VMware-Quellen, um ESXi-Komponenten zu aktualisieren.

Der Host führt eine Vielzahl von Drittanbieterpaketen aus, um Verwaltungsschnittstellen oder von Ihnen durchzuführende Aufgaben zu unterstützen. Bei VMware dürfen diese Pakete nur über eine VMware-Quelle aktualisiert werden. 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 regelmäßig auf Sicherheitswarnungen.

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

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 im Abschnitt 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 vSphere Client. Beim Erstellen eines Kennworts müssen Sie standardmäßig Zeichen aus vier Zeichenklassen verwenden: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen (z. B. Unter- oder Schrägstriche).

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.

Kennwörter dürfen kein Wort aus einem Wörterbuch und keinen Teil eines Worts aus einem Wörterbuch enthalten.

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. Ausführliche Informationen finden Sie im Abschnitt 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 Web 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 3 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. Weitere Informationen zum Festlegen der erweiterten ESXi-Optionen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

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 im Abschnitt 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 zehn fehlgeschlagenen Anmeldeversuchen gesperrt. Das Konto wird standardmäßig nach zwei 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*.

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 z. B. sicher, dass 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 VMware vSphere vMotion®, VMware vSphere Fault Tolerance und Speicher verwendet. Diese Netzwerke werden als für ihre spezifischen Funktionen isoliert betrachtet und oft nicht außerhalb eines einzelnen physischen Satzes von Serverracks geroutet.
- Ein Managementnetzwerk isoliert Datenverkehr des Clients, der Befehlszeilenschnittstelle oder der API sowie Datenverkehr von Drittsoftware von normalem Datenverkehr. Auf dieses Netzwerk dürfen nur System-, Netzwerk- und Sicherheits-Administratoren Zugriff haben. Verwenden Sie Jump-Box oder Virtual Private Network (VPN), um den Zugriff auf das Managementnetzwerk zu sichern. Kontrollieren Sie den Zugriff innerhalb dieses Netzwerks strikt auf mögliche Malware-Quellen.
- 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.

Deaktivieren des Browsers für verwaltete Objekte (MOB)

Mit dem Browser für verwaltete Objekte kann das VMkernel-Objektmodell durchsucht werden. Allerdings können Angreifer diese Schnittstelle in böswilliger Absicht verwenden, um Konfigurationsänderungen oder andere Aktionen durchzuführen, denn mit dem Browser für verwaltete Objekte (Managed Object Browser, MOB) können Sie die Hostkonfiguration ändern.

Verwenden Sie den Managed Object Browser 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.

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.

Die Verwendung von `vim-cmd` über die ESXi Shell wird nicht mehr empfohlen.

Deaktivieren autorisierter Schlüssel (SSH)

Mit autorisierten Schlüsseln können Sie den Zugriff auf einen ESXi-Host über SSH ohne Benutzerauthentifizierung ermöglichen. Um die Hostsicherheit zu erhöhen, sollten Sie nicht zulassen, dass Benutzer mit autorisierten Schlüsseln auf Hosts zugreifen.

Ein Benutzer wird als vertrauenswürdig betrachtet, wenn sich sein öffentlicher Schlüssel in der Datei `/etc/ssh/keys-root/authorized_keys` auf einem Host befindet. Vertrauenswürdige Remotebenutzer dürfen auf den Host zugreifen, ohne ein Kennwort anzugeben.

Verfahren

- ◆ Für alltägliche Vorgänge deaktivieren Sie SSH auf ESXi-Hosts.
- ◆ Wenn SSH vorübergehend oder dauerhaft aktiviert ist, überwachen Sie den Inhalt der Datei `/etc/ssh/keys-root/authorized_keys`, um sicherzustellen, dass kein Benutzer ohne ordnungsgemäße Authentifizierung auf den Host zugreifen kann.
- ◆ Überwachen Sie die Datei `/etc/ssh/keys-root/authorized_keys`, um sicherzustellen, dass sie leer ist und dass ihr keine SSH-Schlüssel hinzugefügt wurden.
- ◆ Wenn Sie feststellen, dass die Datei `/etc/ssh/keys-root/authorized_keys` nicht leer ist, entfernen Sie die Schlüssel.

Ergebnisse

Wenn Sie den Remotezugriff mit autorisierten Schlüsseln deaktivieren, kann Ihre Fähigkeit eingeschränkt werden, Befehle auf einem Host ohne Angabe gültiger Anmeldedaten remote auszuführen. Dies kann beispielsweise bedeuten, dass ein automatisches Remoteskript nicht ausgeführt werden kann.

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 diese 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 6.0

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

Bis zu vSphere Version 5.5 werden die 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 5-1. Zertifikatmodi für ESXi-Hosts

Zertifikatmodus	Beschreibung
VMware Certificate Authority (Standard)	<p>Verwenden Sie diesen Modus, wenn VMCA die Zertifikate für alle ESXi-Hosts bereitstellt, entweder als Zertifizierungsstelle der obersten Ebene oder als Zwischenzertifizierungsstelle.</p> <p>Standardmäßig liefert VMCA alle Zertifikate für ESXi-Hosts.</p> <p>In diesem Modus können Sie Zertifikate in vSphere Web Client aktualisieren und verlängern.</p>
Benutzerdefinierte Zertifizierungsstelle	<p>Verwenden Sie diesen Modus, wenn Sie ausschließlich benutzerdefinierte, von einer Drittanbieter-Zertifizierungsstelle signierte Zertifikate verwenden möchten.</p> <p>In diesem Modus sind Sie für die Verwaltung der Zertifikate verantwortlich. Hier können Sie die Zertifikate nicht in vSphere Web Client aktualisieren und verlängern.</p> <p>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.</p>
Fingerabdruckmodus	<p>vSphere 5.5 verwendete den Fingerabdruckmodus, und dieser Modus ist in vSphere 6.0 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.</p> <p>Verwenden Sie diesen Modus nur, wenn Sie auf Probleme stoßen, die in den anderen beiden Modi nicht zu beheben sind. Einige Dienste aus vCenter 6.0 und höher funktionieren möglicherweise nicht korrekt im Fingerabdruckmodus.</p>

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 8 Monate) befindet. Ein roter Alarm wird ausgelöst, wenn sich das Zertifikat im Status **Ablauf steht bevor** (weniger als 2 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 neuerlichen Starts der ESXi-Hosts wiederverwendet. Ein Auto Deploy-Server ist Teil eines eingebetteten Bereitstellungs- oder Verwaltungsknotens.

Wenn beim erstmaligen Start eines Auto Deploy-Hosts die VMCA nicht verfügbar ist, versucht der Host zunächst, eine Verbindung aufzubauen, und schaltet sich dann so lange ab und wieder ein, bis die VMCA verfügbar ist und dem Host ein signiertes Zertifikat bereitstellen kann.

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 5-2. 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 selbstsignierte Zertifikate durch VMCA-signierte Zertifikate ersetzt. Der Prozess behält benutzerdefinierte Zertifikate bei, selbst wenn diese Zertifikate abgelaufen oder ungültig sind.

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

Host mit bereitgestellten Fingerabdruckzertifikaten

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

Hinweis Sie können keine VMCA-Zertifikate auf Legacy-Hosts bereitstellen. Es ist ein Upgrade auf ESXi 6.0 oder höher erforderlich.

Host mit bereitgestellten benutzerdefinierten Zertifikaten

Wenn auf dem Host benutzerdefinierte Zertifikate bereitgestellt wurden, in der Regel von einer Zertifizierungsstelle signierte Zertifikate eines Drittanbieters, dann werden diese Zertifikate beibehalten. Wechseln Sie den Zertifikatsmodus in den benutzerdefinierten Modus, um sicherzustellen, dass die Zertifikate 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.

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

Mit Auto Deploy verwalteten Hosts werden immer neue Zertifikate zugewiesen, wenn sie zum ersten Mal mit der ESXi 6.0-Software 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.

Standardeinstellungen für ESXi-Zertifikate

Wenn der vCenter Server eine Zertifikatsignieranforderung (CSR) von einem ESXi-Host anfordert, verwendet er Standardeinstellungen. Die meisten Standardwerte sind für viele Situationen gut geeignet, aber unternehmensspezifische Daten können geändert werden.

Ändern Sie eventuell das Unternehmen und Ortsangaben. Sie können viele Standardeinstellungen über den vSphere Web Client ändern. Siehe [Ändern der Standardeinstellungen für Zertifikate](#).

Tabelle 5-3. CSR-Einstellungen

Parameter	Standardwert	Erweiterte Option
Schlüssellänge	2048	Nicht zutreffend
Schlüsselalgorithmus	RSA	Nicht zutreffend

Tabelle 5-3. CSR-Einstellungen (Fortsetzung)

Parameter	Standardwert	Erweiterte Option
Zertifikat-Signaturalgorithmus	sha256WithRSAEncryption	Nicht zutreffend
Allgemeiner Name	Der Name des Hosts, wenn dieser dem vCenter Server nach dem Hostnamen hinzugefügt wurde. Die IP-Adresse des Hosts, wenn dieser dem vCenter Server nach der IP-Adresse hinzugefügt wurde.	Nicht zutreffend
Land	USA	vpxd.certmgmt.certs.cn.country
E-Mail-Adresse	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
Ort	Palo Alto	vpxd.certmgmt.certs.cn.localityName
Name der Organisationseinheit	VMware Engineering	vpxd.certmgmt.certs.cn.organizationalUnitName
Organisationsname	VMware	vpxd.certmgmt.certs.cn.organizationName
Bundesland/Kanton	Kalifornien	vpxd.certmgmt.certs.cn.state
Anzahl der Tage, die das Zertifikat gültig ist.	1825	vpxd.certmgmt.certs.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. Siehe Host-Upgrades und Zertifikate .	Standard ist vmca Sie können auch „Fingerabdruck“ oder „benutzerdefiniert“ festlegen. Siehe Ändern des Zertifikatmodus .	vpxd.certmgmt.mode

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 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.

3 Wählen Sie **System** und klicken Sie 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: <div> <p>Gut</p> <p>Normaler Betrieb.</p> <p>Läuft ab</p> <p>Zertifikat läuft bald ab.</p> <p>Läuft in Kürze ab</p> <p>Es fehlen nur noch 8 Monate oder weniger bis zum Ablauf (Standard).</p> <p>Ablauf steht bevor</p> <p>Es fehlen nur noch 2 Monate oder weniger bis zum Ablauf (Standard).</p> <p>Abgelaufen</p> <p>Das Zertifikat ist nicht gültig, weil es abgelaufen ist.</p> </div>

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 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Wählen Sie **System** aus und klicken Sie 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 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.

Ändern Sie unternehmensspezifische Standardeinstellungen für Zertifikate. Eine vollständige 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 die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Klicken Sie auf **Erweiterte Einstellungen** und auf **Bearbeiten**.
- 4 Geben Sie im Filterfeld **certmgmt** ein, um nur Zertifikatverwaltungsparameter anzuzeigen.
- 5 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.

Grundlegende Informationen zu Zertifikatmoduswechseln

Ab vSphere 6.0 sind ESXi-Hosts standardmäßig mit Zertifikaten der VMCA ausgestattet. Sie können stattdessen den benutzerdefinierten Zertifikatmodus oder zur Fehlerbehebung den 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.

Tabelle 5-4. Zertifikatmodi für ESXi-Hosts

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.

Ändern des Zertifikatmodus

In den meisten Fällen ist VMCA die beste Lösung zur Bereitstellung der ESXi-Hosts in Ihrer Umgebung. Wenn Ihre Unternehmensrichtlinie vorsieht, dass Sie benutzerdefinierte Zertifikate mit einer anderen Stammzertifizierungsstelle verwenden, können Sie in den erweiterten Optionen von vCenter Server festlegen, dass den Hosts bei der Zertifikataktualisierung nicht automatisch VMCA-Zertifikate bereitgestellt werden. In diesem Fall übernehmen Sie die Verantwortung 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 den vCenter Server aus, von dem die Hosts verwaltet werden, und klicken Sie auf **Einstellungen**.
- 2 Klicken Sie auf **Erweiterte Einstellungen** und auf **Bearbeiten**.
- 3 Geben Sie im Feld „Filter“ den Ausdruck **certmgmt** ein, um nur die Zertifikatsverwaltungsschlüssel anzuzeigen.
- 4 Ändern Sie „vpxd.certmgmt.mode“ zu **custom** (benutzerdefiniert), wenn Sie Ihre eigenen Zertifikate verwalten möchten, oder zu **thumbprint** (Fingerabdruck), wenn Sie vorübergehend in den Fingerabdruckmodus wechseln möchten. Klicken Sie anschließend auf **OK**.

5 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 Schlüssel, 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 organisatorischen Zertifizierungsstelle, wenn die Unternehmensrichtlinie dies vorsieht.

Die Standardzertifikate befinden sich am selben Speicherort wie die vSphere 5.5-Zertifikate. Es gibt mehrere 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.

■ Voraussetzungen für ESXi-Zertifikatssignieranforderungen

Wenn Sie ein von einer Zertifizierungsstelle (CA) signiertes Drittanbieterzertifikat verwenden möchten, entweder mit VMCA als untergeordneter Zertifizierungsstelle oder mit einer benutzerdefinierten Zertifizierungsstelle, müssen Sie eine Zertifikatssignieranforderung (CSR) zur 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 mit dem `vifs`-Befehl 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 von einer Zertifizierungsstelle (CA) signiertes Drittanbieterzertifikat verwenden möchten, entweder mit VMCA als untergeordneter Zertifizierungsstelle oder mit einer benutzerdefinierten Zertifizierungsstelle, müssen Sie eine Zertifikatssignieranforderung (CSR) zur Zertifizierungsstelle senden.

Verwenden Sie eine Zertifikatssignieranforderung mit den folgenden Eigenschaften:

- 2048 Bits
- PKCS1
- Keine Platzhalter
- 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. Informationen zum Aktivieren des Zugriffs auf die ESXi Shell finden Sie in der Dokumentation zu *vSphere-Sicherheit*.
- 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. Informationen zum Zuweisen von Rechten über Rollen finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

Verfahren

- 1 Melden Sie sich bei der ESXi Shell entweder direkt von der DCUI oder von einem SSH-Client als Benutzer mit Administratorrechten an.

- 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
```

- Kopieren Sie die Zertifikate, die Sie verwenden möchten, in `/etc/vmware/ssl`.
- Benennen Sie das neue Zertifikat und den Schlüssel um in `rui.crt` und `rui.key`.
- 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 `TRUSTED_ROOTS` in vCenter Server. Siehe [Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS \(Benutzerdefinierte Zertifikate\)](#).

Ersetzen eines Standardzertifikats und -schlüssels mit dem `vifs`-Befehl

Sie können die standardmäßigen VMCA-signierten ESXi-Zertifikate mit dem `vifs`-Befehl 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. Informationen zum Aktivieren des Zugriffs auf die ESXi Shell finden Sie in der Dokumentation zu *vSphere-Sicherheit*.
- 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. Informationen zum Zuweisen von Rechten über Rollen finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

Verfahren

- Sichern Sie die vorhandenen Zertifikate.
- Generieren Sie eine Zertifikatsanforderung gemäß den Anweisungen der Zertifizierungsstelle.
- 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. Siehe [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. Informationen zum Aktivieren des Zugriffs auf die ESXi Shell finden Sie in der Dokumentation zu *vSphere-Sicherheit*.
- 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. Informationen zum Zuweisen von Rechten über Rollen finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

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	<code>https://hostname/host/ssl_cert</code>
Schlüssel	<code>https://hostname/host/ssl_key</code>

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.

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 Führen Sie `vecs-cli` zum Hinzufügen der neuen Zertifikate zum Speicher `TRUSTED_ROOTS` aus. Beispiel:

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt
--cert /etc/vmware/ssl/custom1.crt
```

Option	Beschreibung
Linux	<pre>/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert /etc/vmware/ssl/ custom1.crt</pre>
Windows	<pre>C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt -- cert c:\ssl\custom1.crt</pre>

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 Zertifikatsmodus](#).

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 von Ihrer Zertifizierungsstelle ein Zertifikat an, das Ihren Anforderungen entspricht.
 - 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 Zertifikatsdatei `rbd-ca.crt` und die Schlüsseldatei `rbd-ca.key`.

Verfahren

- 1 Sichern Sie die standardmäßigen ESXi-Zertifikate.
Die Zertifikate befinden sich unter `/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, `rbd-ca.crt` und `rbd-ca.key` in `/etc/vmware-rbd/ssl/` durch Ihre benutzerdefinierte Zertifikatsdatei und Schlüsseldatei.

- 4 Aktualisieren Sie auf demselben System den Speicher TRUSTED_ROOTS im VECS, damit er die neuen Zertifikate verwendet.

```
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
```

Windows

C:\Programme\VMware\vCenter Server\vmafdd\vecs-cli.exe

Linux

/usr/lib/vmware-vmafd/bin/vecs-cli

- 5 Erstellen Sie die Datei `castore.pem`, die den Inhalt von TRUSTED_ROOTS 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 Zertifikatmodus des vCenter Server-Systems in **Benutzerdefiniert**.

Siehe [Ändern des Zertifikatmodus](#).

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

Ergebnisse

Bei der nächsten Zertifikatausstattung eines Hosts mit Auto Deploy generiert der Auto Deploy-Server ein Zertifikat anhand des Stammzertifikats, das Sie eben dem Speicher TRUSTED_ROOTS hinzugefügt haben.

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 die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Klicken Sie 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.



Hinzufügen zulässiger IP-Adressen zur ESXi-Firewall

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_Ougsspa2/uiConfId/49694343/)

Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 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 können Sie für jeden Dienst die Firewall öffnen oder schließen oder den Datenverkehr aus bestimmten IP-Adressen durchlassen.

Die folgende Tabelle enthält die Firewalls für die üblicherweise installierten Dienste. Wenn Sie andere VIBs auf Ihrem Host installieren, stehen Ihnen möglicherweise weitere Dienste und Firewall-Ports zur Verfügung.

Tabelle 5-5. Eingehende Firewall-Verbindungen

Dienst	Port	Kommentar
CIM-Server	5988 (TCP)	Server für CIM (Common Information Model)
Sicherer CIM-Server	5989 (TCP)	Sicherer Server für CIM
CIM-SLP	427 (TCP, UDP)	Der CIM-Client verwendet das Service Location Protocol, Version 2 (SLPv2), zum Ermitteln von CIM-Servern.
DHCPv6	546 (TCP, UDP)	DHCP-Client für IPv6

Tabelle 5-5. Eingehende Firewall-Verbindungen (Fortsetzung)

Dienst	Port	Kommentar
DVSSync	8301, 8302 (UDP)	DVSSync-Ports werden zur Synchronisierung des Status von verteilten virtuellen Ports zwischen Hosts mit aktivierter VMware FT-Aufzeichnung und -Wiedergabe verwendet. Diese Ports dürfen nur für Hosts geöffnet sein, auf denen primäre oder Backup-VMs ausgeführt werden. Für Hosts ohne VMware FT dürfen diese Ports nicht geöffnet sein.
NFC	902 (TCP)	Network File Copy (NFC) umfasst einen FTP-Dienst für vSphere-Komponenten, bei dem der Dateityp beachtet wird. ESXi verwendet NFC standardmäßig für Vorgänge wie das Kopieren und Verschieben von Daten zwischen Datenspeichern.
Virtual SAN-Clusterbildungsdienst	12345, 23451 (UDP)	Cluster-Überwachungs-, Mitgliedschafts- und Verzeichnisdienst für Virtual SAN. Verwendet UDP-basiertes IP-Multicast zur Bestimmung von Clustermitgliedern und Verteilung von Virtual SAN-Metadaten an alle Clustermitglieder. Wenn aktiviert, kann Virtual SAN nicht genutzt werden.
DHCP-Client	68 (UDP)	DHCP-Client für IPv4
DNS-Client	53 (UDP)	DNS-Client
Fault Tolerance	8200, 8100, 8300 (TCP, UDP)	Datenverkehr zwischen Hosts für vSphere Fault Tolerance (FT)
NSX Distributed Logical Router-Dienst	6999 (UDP)	NSX Virtual Distributed Router-Dienst Die Firewall für diesen Dienst wird geöffnet, wenn NSX-VIBs installiert werden und das VDR-Modul erstellt wird. Wenn keine VDR-Instanzen mit dem Host verbunden sind, muss der Port nicht geöffnet sein. In früheren Produktversionen wurde dieser Dienst als „NSX Distributed Logical Router“ bezeichnet.
Virtual SAN-Transport	2233 (TCP)	Zuverlässiger Datagramm-Transport für Virtual SAN. Verwendet TCP und dient der Virtual SAN-Speicher-E/A. Wenn aktiviert, kann Virtual SAN nicht genutzt werden.
SNMP-Server	161 (UDP)	Ermöglicht dem Host die Verbindung mit einem SNMP-Server.
SSH-Server	22 (TCP)	Erforderlich für SSH-Zugriff.
vMotion	8000 (TCP)	Erforderlich für die VM-Integration mit vMotion.
vSphere Web Client	902, 443 (TCP)	Client-Verbindungen

Tabelle 5-5. Eingehende Firewall-Verbindungen (Fortsetzung)

Dienst	Port	Kommentar
vsanvp	8080 (TCP)	VSAN-VASA-Anbieter-Provider. Wird vom Speicherverwaltungsdienst (Storage Management Service, SMS) im Umfang von vCenter für den Zugriff auf Daten zu Virtual SAN-Speicherprofilen, Funktionen und Compliance genutzt. Wenn deaktiviert, kann das Virtual SAN Storage Profile Based Management (SPBM) nicht genutzt werden.
vSphere Web Access	80 (TCP)	Begrüßungsseite mit Downloadlinks für verschiedene Schnittstellen
RFB-Protokoll	5900-5964 (TCP)	Wird von Verwaltungstools wie VNC verwendet.

Tabelle 5-6. Ausgehende Firewall-Verbindungen

Dienst	Port	Kommentar
CIM-SLP	427 (TCP, UDP)	Der CIM-Client verwendet das Service Location Protocol, Version 2 (SLPv2), zum Ermitteln von CIM-Servern.
DHCPv6	547 (TCP, UDP)	DHCP-Client für IPv6
DVSSync	8301, 8302 (UDP)	DVSSync-Ports werden zur Synchronisierung des Status von verteilten virtuellen Ports zwischen Hosts mit aktivierter VMware FT-Aufzeichnung und -Wiedergabe verwendet. Diese Ports dürfen nur für Hosts geöffnet sein, auf denen primäre oder Backup-VMs ausgeführt werden. Für Hosts ohne VMware FT dürfen diese Ports nicht geöffnet sein.
HBR	44046, 31031 (TCP)	Wird von vSphere Replication und VMware Site Recovery Manager für den laufenden Replizierungsdatenverkehr verwendet.
NFC	902 (TCP)	Network File Copy (NFC) umfasst einen FTP-Dienst für vSphere-Komponenten, bei dem der Dateityp beachtet wird. ESXi verwendet NFC standardmäßig für Vorgänge wie das Kopieren und Verschieben von Daten zwischen Datenspeichern.
WOL	9 (UDP)	Verwendet von „Wake on LAN“.
Virtual SAN-Clusterbildungsdienst	12345 23451 (UDP)	Cluster-Überwachungs-, Mitgliedschafts- und Verzeichnisdienst, verwendet von Virtual SAN
DHCP-Client	68 (UDP)	DHCP-Client
DNS-Client	53 (TCP, UDP)	DNS-Client
Fault Tolerance	80, 8200, 8100, 8300 (TCP, UDP)	Unterstützt VMware Fault Tolerance.

Tabelle 5-6. Ausgehende Firewall-Verbindungen (Fortsetzung)

Dienst	Port	Kommentar
Software-iSCSI-Client	3260 (TCP)	Unterstützt Software-iSCSI.
NSX Distributed Logical Router-Dienst	6999 (UDP)	Die Firewall für diesen Dienst wird geöffnet, wenn NSX-VIBs installiert werden und das VDR-Modul erstellt wird. Wenn keine VDR-Instanzen mit dem Host verbunden sind, muss der Port nicht geöffnet sein.
rabbitmqproxy	5671 (TCP)	Ein auf dem ESXi-Host ausgeführter Proxy, der Hostanwendungen innerhalb von virtuellen Maschinen die Kommunikation mit den AMQP-Brokern in der vCenter-Netzwerkdomäne ermöglicht. Die virtuelle Maschine muss sich nicht im Netzwerk befinden, d. h., es ist keine Netzwerkkarte erforderlich. Der Proxy verbindet sich mit den Brokern in der vCenter-Netzwerkdomäne. Die IP-Adressen der ausgehenden Verbindungen müssen daher mindestens die aktuell oder zukünftig verwendeten Broker enthalten. Bei einer Erweiterung können zusätzliche Broker hinzugefügt werden.
Virtual SAN-Transport	2233 (TCP)	Wird für den RDT-Datenverkehr (Unicast-Peer-to-Peer-Kommunikation) zwischen Virtual SAN-Knoten verwendet.
vMotion	8000 (TCP)	Erforderlich für die VM-Integration mit vMotion.
VMware vCenter Agent	902 (UDP)	vCenter Server-Agent
vsanvp	8080 (TCP)	Wird für Virtual SAN-Anbieter-Provider-Datenverkehr verwendet.

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.

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 Command-Line Interfaces* finden Sie eine Einführung, und *Konzepte und Beispiele zur vSphere-Befehlszeilenschnittstelle* enthält Beispiele für die Verwendung von ESXCLI für den Umgang mit Firewalls und Firewall-Regeln.

Tabelle 5-7. Firewall-Befehle

Befehl	Beschreibung
<code>esxcli network firewall get</code>	Gibt den aktivierten oder deaktivierten Status der Firewall zurück und listet die Standardaktionen auf.
<code>esxcli network firewall set --default-action</code>	Legen Sie „true“ fest, um die Standardaktion zu aktivieren. Legen Sie „false“ fest, um die Standardaktion zu deaktivieren.
<code>esxcli network firewall set --enabled</code>	Aktiviert bzw. deaktiviert die ESXi-Firewall.

Tabelle 5-7. Firewall-Befehle (Fortsetzung)

Befehl	Beschreibung
<code>esxcli network firewall load</code>	Lädt die Firewallmodul- und Regelsatz-Konfigurationsdateien.
<code>esxcli network firewall refresh</code>	Aktualisiert die Firewall-Konfiguration durch das Einlesen der Regelsatzdateien, wenn das Firewallmodul geladen ist.
<code>esxcli network firewall unload</code>	Löscht Filter und entlädt das Firewallmodul.
<code>esxcli network firewall ruleset list</code>	Listet Informationen zu Regelsätzen auf.
<code>esxcli network firewall ruleset set --allowed-all</code>	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.
<code>esxcli network firewall ruleset set --enabled --ruleset-id=<Zeichenfolge></code>	Legen Sie diese Option auf „true“ oder „false“ fest, um den angegebenen Regelsatz zu aktivieren bzw. zu deaktivieren.
<code>esxcli network firewall ruleset allowedip list</code>	Listet die zulässigen IP-Adressen des angegebenen Regelsatzes auf.
<code>esxcli network firewall ruleset allowedip add</code>	Ermöglicht den Zugriff auf den Regelsatz von der angegebenen IP-Adresse oder einem Bereich von IP-Adressen aus.
<code>esxcli network firewall ruleset allowedip remove</code>	Deaktiviert den Zugriff auf den Regelsatz von der angegebenen IP-Adresse oder einem Bereich von IP-Adressen aus.
<code>esxcli network firewall ruleset rule list</code>	Listet die Regeln jedes Regelsatzes in der Firewall auf.

Anpassen von ESXi-Diensten über das Sicherheitsprofil

Ein ESXi-Host umfasst mehrere Dienste, die standardmäßig ausgeführt werden. Andere Dienste, beispielsweise SSH, sind im Sicherheitsprofil des Hosts enthalten. Sie können diese nach Bedarf aktivieren und deaktivieren, sofern Ihre Unternehmensrichtlinien dies zulassen.

[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 5-8. 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
Local Security Authentication Server (Active Directory-Dienst)	Gestoppt	Teil des Active Directory-Diensts. Wenn Sie ESXi für Active Directory konfigurieren, wird dieser Dienst gestartet.
I/O Redirector (Active Directory-Dienst)	Gestoppt	Teil des Active Directory-Diensts. Wenn Sie ESXi für Active Directory konfigurieren, wird dieser Dienst gestartet.
Network Login Server (Active Directory-Dienst)	Gestoppt	Teil des Active Directory-Diensts. Wenn Sie ESXi für Active Directory konfigurieren, wird dieser Dienst gestartet.
NTP-Daemon	Gestoppt	Network Time Protocol-Daemon
CIM-Server	Wird ausgeführt	Ein Dienst, der von CIM-Anwendungen (Common Information Model) genutzt werden kann
SNMP-Server	Gestoppt	SNMP-Daemon. Informationen zur Konfiguration von SNMP v1, v2 und v3 erhalten Sie unter <i>vSphere-Überwachung und -Leistung</i> .
Syslog-Server	Gestoppt	Syslog-Daemon. Syslog kann in den erweiterten Systemeinstellungen in vSphere Web Client aktiviert werden. Siehe <i>Installations- und Einrichtungshandbuch für vSphere</i> .
vSphere High Availability Agent	Gestoppt	Unterstützt vSphere High Availability.
vProbe-Daemon	Gestoppt	vProbe-Daemon

Tabelle 5-8. ESXi-Dienste im Sicherheitsprofil (Fortsetzung)

Dienst	Standard	Beschreibung
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 manchen 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 die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 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 sind:** 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 kurz nach dem Starten des Hosts gestartet und kurz vor dessen Herunterfahren 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 [Angaben der Benutzerausnahmen für den Sperrmodus](#).



Sperrmodus in vSphere 6

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_zg4ylguO/uiConfId/49694343/)

Normaler Sperrmodus und strenger Sperrmodus

Ab vSphere 6.0 haben Sie die Wahl zwischen dem normalen und dem strengen Sperrmodus mit jeweils unterschiedlicher Sperrstärke.

Normaler Sperrmodus

Im normalen Sperrmodus wird der DCUI-Dienst nicht angehalten. Wenn die Verbindung mit dem vCenter Server-System unterbrochen wird und über den vSphere Web Client kein Zugriff mehr besteht, können sich die berechtigten Konten bei der Schnittstelle der direkten Konsole (DCUI) des ESXi-Hosts anmelden und den Sperrmodus verlassen. Nur die folgenden Konten haben Zugriff auf die Benutzerschnittstelle der direkten Konsole:

- Konten in der Liste der aus dem Sperrmodus ausgenommenen Benutzer mit Administratorrechten für den Host. Die Liste der ausgenommenen Benutzer ist für Dienstkonten gedacht, mit denen sehr spezielle Aufgaben ausgeführt werden. Wenn Sie dieser Liste ESXi-Administratoren hinzufügen, widerspricht dies dem Zweck des Sperrmodus.
- In der erweiterten Option DCUI.Access für den Host definierte Benutzer. Diese Option dient für den Notfallzugriff auf die Schnittstelle der direkten Konsole für den Fall, dass die Verbindung mit vCenter Server unterbrochen wird. Diese Benutzer benötigen keine Administratorrechte auf dem Host.

Strenger Sperrmodus

Im strengen Sperrmodus, neu in vSphere 6.0, wird der DCUI-Dienst angehalten. Wenn die Verbindung mit vCenter Server unterbrochen wird und der vSphere Web Client nicht mehr verfügbar ist, steht auch der ESXi-Host nicht mehr zur Verfügung – es sei denn, die ESXi Shell und die SSH-Dienste sind aktiviert und ausgenommene Benutzer wurden definiert. Wenn Sie die Verbindung mit dem vCenter Server-System nicht mehr herstellen können, müssen Sie den Host neu installieren.

Sperrmodus und ESXi Shell bzw. SSH-Dienste

Im strengen Sperrmodus wird der DCUI-Dienst angehalten. ESXi Shell und SSH-Dienste sind jedoch vom Sperrmodus nicht betroffen. Damit der Sperrmodus eine wirksame Schutzmaßnahme darstellen kann, müssen auch die ESXi Shell und die SSH-Dienste deaktiviert sein. Diese Dienste sind standardmäßig deaktiviert.

Bei einem Host im Sperrmodus können Benutzer in der Liste der ausgenommenen Benutzer über die ESXi Shell und SSH auf den Host zugreifen, wenn sie die Administratorrolle auf dem Host besitzen. Das ist sogar im strengen Sperrmodus möglich. Daher ist die sicherste Option, den ESXi Shell- und den SSH-Dienst deaktiviert zu lassen.

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

Aktivieren und Deaktivieren des Sperrmodus

Berechtigte Benutzer haben mehrere Möglichkeiten, den Sperrmodus zu aktivieren:

- Mit dem Assistenten **Host hinzufügen** beim Hinzufügen eines Hosts zu einem vCenter Server-System

- Mit dem vSphere Web Client. Weitere Informationen hierzu finden Sie unter [Aktivieren des Sperrmodus über vSphere Web Client](#). Sie können sowohl den normalen als auch den strengen Sperrmodus über den vSphere Web Client deaktivieren.
- Mit der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI). Weitere Informationen hierzu finden Sie unter [Aktivieren oder Deaktivieren des normalen Sperrmodus über die Benutzerschnittstelle der direkten Konsole](#).

Berechtigte Benutzer können den Sperrmodus im vSphere Web Client deaktivieren. Über die Benutzerschnittstelle der direkten Konsole kann der normale, nicht aber der strenge Sperrmodus deaktiviert werden.

Hinweis Wenn Sie den Sperrmodus über die Benutzerschnittstelle der direkten Konsole aktivieren bzw. deaktivieren, werden Berechtigungen für Benutzer und Gruppen auf dem Host verworfen. Um diese Berechtigungen beizubehalten, müssen Sie den Sperrmodus im vSphere Web Client aktivieren oder deaktivieren.

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 „Ausnahme für Benutzer“ mit Administratorrechten und Benutzer, die in der erweiterten Systemeinstellung DCUI.Access angegeben sind, auf die DCUI zugreifen.
- Falls die ESXi Shell oder SSH aktiviert sind und der Host in den strengen oder normalen Sperrmodus wechselt, können diese Dienste von Konten in der Liste „Ausnahme für 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 5-9. Verhalten im Sperrmodus

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

Wenn Benutzer bei der ESXi Shell angemeldet sind oder über SSH auf den Host zugreifen, bevor der Sperrmodus aktiviert wird, bleiben Benutzer in der Liste „Ausnahme für Benutzer“ mit Administratorrechten auf dem Host 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.

Sie können den strengen Sperrmodus auswählen, um den direkten Zugriff auf einen Host vollständig zu unterbinden. 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. Siehe [Verhalten im Sperrmodus](#).

Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 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 sind, könnte der Zugriff möglich sein.
Streng	Der Zugriff auf den Host ist nur über vCenter Server möglich. Falls SSH oder die ESXi Shell aktiviert sind, 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 die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.

- 3 Klicken Sie unter „System“ auf **Sicherheitsprofil**.
- 4 Klicken Sie im Bereich „Sperrmodus“ auf **Bearbeiten**.
- 5 Klicken Sie auf **Sperrmodus** und wählen Sie **Keine** 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 Benutzerberechtigungen beim Aktivieren des Sperrmodus erhalten, und die Benutzerberechtigungen 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 bei einem schwerwiegenden Fehler von vCenter Server Zugriff auf den ESXi-Host hat.

Welche Aktionen mit unterschiedlichen Konten bei aktiviertem Sperrmodus standardmäßig ausgeführt werden können und wie Sie das Standardverhalten ändern können, hängt von der Version der vSphere-Umgebung ab.

- In Versionen von vSphere vor vSphere 5.1 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. Diese Option ist für schwerwiegende Fehler von vCenter Server gedacht, und das Kennwort für den Benutzer mit diesem Zugriff ist in der Regel an einem sicheren Ort aufbewahrt. 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

Mit der erweiterten Option DCUI.Access können Sie in erster Linie den Sperrmodus beenden, falls Sie bei einem schwerwiegenden Fehler über vCenter Server nicht 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. Dadurch kann die Sicherheit Ihres Hosts beeinträchtigt werden. 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. Siehe [Angeben der Benutzerausnahmen für den Sperrmodus](#).

Verfahren

- 1 Navigieren Sie zum Host im Objektnavigator von vSphere Web Client.

- 2 Wählen Sie die Registerkarte **Verwalten** und klicken Sie auf **Einstellungen**.
- 3 Klicken Sie auf **Erweiterte Systemeinstellungen** und wählen Sie **DCUI.Access** aus.
- 4 Klicken Sie auf **Bearbeiten**, um die Benutzernamen durch Kommas getrennt einzugeben.

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.

- 5 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, Dienstknoten 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 Dienstknoten 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 die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 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.

Überprüfen der Akzeptanzebenen von Hosts und VIBs

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.

Sie können ESXCLI-Befehle verwenden, um eine Akzeptanzebene für einen Host festzulegen. Die Akzeptanzebene des Hosts darf nicht restriktiver als die Akzeptanzebene des VIBs sein, das Sie zu diesem Host hinzufügen möchten. 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.

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. Heute werden nur IOVP-Treiber 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“ oder „VMwareAccepted“ gesetzt ist, indem Sie folgenden Befehl ausführen:

```
esxcli software acceptance get
```

- 2 Wenn es sich bei der Akzeptanzebene des Hosts nicht um „VMwareCertified“ oder „VMwareAccepted“ handelt, stellen Sie fest, ob, und wenn ja, welche der VIBs sich nicht auf der Ebene „VMwareCertified“ oder „VMwareAccepted“ befinden, indem Sie folgende Befehle ausführen:

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

- 3 Entfernen Sie alle VIBs, die sich auf der Ebene „PartnerSupported“ oder „CommunitySupported“ befinden, indem Sie folgenden Befehl ausführen:

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

- 4 Ändern Sie die Akzeptanzebene des Hosts, indem Sie folgenden Befehl ausführen:

```
esxcli software acceptance set --level acceptance_level
```

Zuweisen der Berechtigungen für ESXi

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 Administratorrolle einer beschränkten Anzahl von Benutzern zuweisen, die eventuell direkte Verwaltungsaufgaben auf dem ESXi-Host ausführen. 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 vSphere Client können Sie lokale Benutzer hinzufügen und benutzerdefinierte Rollen definieren.

Für alle ESXi-Versionen 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 Standardeinstellung. Die Standardeinstellung kann bei Bedarf überschrieben werden.

Sie können lokale Benutzer und Gruppen verwalten und lokale benutzerdefinierte Rollen zu einem ESXi-Host hinzufügen, indem Sie einen vSphere Client verwenden, der direkt mit dem ESXi-Host verbunden ist.

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 also einem der beiden eine Rolle zuweisen, gilt die Rolle für den anderen nicht.

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 unberechtigtes Eindringen in einen ESXi-Host begünstigen und die Zuordnung einzelner Aktionen zu einem bestimmten Administrator erschweren.

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. In vSphere 5.1 und höher ist es nur dem Root-Benutzer und keinem anderen benannten Benutzer mit der Administratorrolle gestattet, einen Host zu vCenter Server hinzuzufügen.

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, falls möglich, die Active Directory-Anmeldedaten verwalten können.

Wichtig Wenn Sie die Zugriffsrechte für den Root-Benutzer entfernen, müssen Sie 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 Konfigurationsänderungen vornehmen, die für die Unterstützung virtueller Maschinen notwendig sind.

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 auf dem jeweiligen 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.

Installieren oder Durchführen eines Upgrades von vSphere Authentication Proxy

Installieren Sie vSphere Authentication Proxy, um ESXi-Hosts den Beitritt zu einer Domäne zu ermöglichen, ohne Active Directory-Anmeldeinformationen zu verwenden. vSphere Authentication Proxy verbessert die Sicherheit für von PXE gestartete Hosts sowie von Hosts, die unter Verwendung von Auto Deploy bereitgestellt werden, weil Active Directory-Anmeldeinformationen nicht in der Hostkonfiguration gespeichert werden müssen.

Wenn auf Ihrem System eine frühere Version von vSphere Authentication Proxy installiert ist, sorgt dieser Vorgang dafür, dass ein Upgrade von vSphere Authentication Proxy auf die aktuelle Version durchgeführt wird.

Sie können vSphere Authentication Proxy auf derselben Maschine wie den verknüpften vCenter Server oder auf einer anderen Maschine installieren, die über eine Netzwerkverbindung mit vCenter Server verfügt. vSphere Authentication Proxy wird ab vCenter Server-Version 5.0 unterstützt.

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 Netzwerkumgebung befinden, in der nur IPv4, IPv4 und IPv6 oder nur IPv6 eingesetzt wird. Allerdings muss die Maschine, die eine Verbindung zu vCenter Server über den vSphere Web Client herstellt, über eine IPv4-Adresse verfügen, damit der vSphere Authentication Proxy-Dienst funktionieren kann.

Voraussetzungen

- Installieren Sie Microsoft .NET Framework 3.5 auf dem System, auf dem Sie vSphere Authentication Proxy installieren möchten.
- Stellen Sie sicher, dass Sie über Administratorberechtigungen verfügen.

- Stellen Sie sicher, dass die Hostmaschine über einen unterstützten Prozessor und ein unterstütztes Betriebssystem verfügt.
- Achten Sie darauf, dass die Hostmaschine über eine gültige IPv4-Adresse verfügt. Sie können vSphere Authentication Proxy auf einer Maschine in einer Netzwerkumgebung installieren, in der nur IPv4 oder sowohl IPv4 als auch IPv6 eingesetzt werden. Sie können vSphere Authentication Proxy jedoch nicht in einer Netzwerkumgebung installieren, in der nur IPv6 eingesetzt wird.
- Wenn Sie vSphere Authentication Proxy auf einer Windows Server 2008 R2-Hostmaschine installieren, laden Sie den im Windows-KB-Artikel 981506 auf der Website support.microsoft.com beschriebenen Windows-Hotfix herunter und installieren Sie ihn. Wenn dieser Hotfix nicht installiert ist, kann der vSphere Authentication Proxy-Adapter nicht initialisiert werden. Zu diesem Problem werden Fehlermeldungen in der Datei `camadapter.log` protokolliert, die den Meldungen `CAM-Website konnte nicht mit CTL gebunden werden` und `CAMAdapter konnte nicht initialisiert werden` ähneln.
- Laden Sie das vCenter Server-Installationsprogramm herunter.

Sammeln Sie die folgenden Informationen, um die Installation bzw. das Upgrade abzuschließen:

- Der Installationsspeicherort von vSphere Authentication Proxy, wenn Sie den Standardspeicherort nicht verwenden.
- Die Adresse und Anmeldeinformationen von vCenter Server, mit dem vSphere Authentication Proxy eine Verbindung herstellt: IP-Adresse oder Name, HTTP-Port, Benutzername und Kennwort.
- Der Hostname oder die IP-Adresse, die zum Identifizieren von vSphere Authentication Proxy im Netzwerk verwendet wird.

Verfahren

- 1 Fügen Sie die Hostmaschine dort hinzu, wo Sie den Authentication Proxy-Dienst für die Domäne installieren.
- 2 Verwenden Sie das Domänenadministratorkonto, um sich bei der Hostmaschine anzumelden.
- 3 Doppelklicken Sie im Software-Installationsprogrammverzeichnis auf die Datei `autorun.exe`, um das Installationsprogramm zu starten.
- 4 Wählen Sie **VMware vSphere Authentication Proxy** aus und klicken Sie auf **Installieren**.
- 5 Folgen Sie den Eingabeaufforderungen des Assistenten, um die Installation bzw. das Upgrade abzuschließen.

Während der Installation registriert sich der Authentifizierungsdienst mit der vCenter Server-Instanz, auf der Auto Deploy registriert ist.

Ergebnisse

Wenn Sie den vSphere Authentication Proxy-Dienst installieren, erstellt das Installationsprogramm ein Domänenkonto mit den entsprechenden Berechtigungen zum Ausführen des Authentication Proxy-Diensts. Der Name des Kontos beginnt mit dem Präfix `CAM-` und ihm wird ein 32-stelliges, nach dem Zufallsprinzip generiertes Kennwort zugeordnet. Das Kennwort ist so konfiguriert, dass es nie abläuft. Ändern Sie die Kontoeinstellungen nicht.

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 Computernamen 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.Domänenname

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 die Registerkarte **Verwalten** und anschließend auf **Netzwerk**.
 - c Klicken Sie auf „DNS“, und vergewissern Sie sich, dass die Informationen zu Hostnamen und DNS-Server des Hosts korrekt sind.

Nächste Schritte

Verwenden Sie vSphere Web Client, um einer Verzeichnisdienst-Domäne beizutreten. 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](#).

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 Domännennamen 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 die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Wählen Sie unter „System“ die Option **Authentifizierungsdienste**.
- 4 Klicken Sie auf **Domäne beitreten**.
- 5 Geben Sie eine Domäne ein.

Verwenden Sie das Formular **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.

Anzeigen der Verzeichnisdiensteinstellungen

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

Verfahren

- 1 Navigieren Sie zum Host im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Wählen Sie unter „System“ die Option **Authentifizierungsdienste**.

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

Verwenden des vSphere Authentication Proxy

Wenn Sie den vSphere Authentication Proxy verwenden, müssen Sie die Active Directory-Anmeldedaten nicht auf dem Host speichern. Benutzer geben beim Hinzufügen eines Hosts zu einer Domäne den Domänennamen des Active Directory-Servers und die IP-Adresse des Authentication Proxy-Servers an.

vSphere Authentication Proxy ist besonders nützlich in Kombination mit Auto Deploy. Dabei richten Sie einen Referenzhost ein, der auf Authentication Proxy verweist, und legen eine Regel fest, die das Profil des Referenzhosts auf alle ESXi-Hosts anwendet, die mit Auto Deploy bereitgestellt wurden. Selbst wenn Sie vSphere Authentication Proxy in einer Umgebung mit VMCA- oder Drittanbieterzertifikaten einsetzen, funktioniert dieser Vorgang reibungslos, vorausgesetzt Sie halten sich an die Anweisungen zur Verwendung von benutzerdefinierten Zertifikaten mit Auto Deploy. Weitere Informationen hierzu finden Sie unter [Verwenden benutzerdefinierter Zertifikate mit Auto Deploy](#).

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

Installieren oder Durchführen eines Upgrades von vSphere Authentication Proxy

Installieren Sie vSphere Authentication Proxy, um ESXi-Hosts den Beitritt zu einer Domäne zu ermöglichen, ohne Active Directory-Anmeldeinformationen zu verwenden. vSphere Authentication Proxy verbessert die Sicherheit für von PXE gestartete Hosts sowie von

Hosts, die unter Verwendung von Auto Deploy bereitgestellt werden, weil Active Directory-Anmeldeinformationen nicht in der Hostkonfiguration gespeichert werden müssen.

Wenn auf Ihrem System eine frühere Version von vSphere Authentication Proxy installiert ist, sorgt dieser Vorgang dafür, dass ein Upgrade von vSphere Authentication Proxy auf die aktuelle Version durchgeführt wird.

Sie können vSphere Authentication Proxy auf derselben Maschine wie den verknüpften vCenter Server oder auf einer anderen Maschine installieren, die über eine Netzwerkverbindung mit vCenter Server verfügt. vSphere Authentication Proxy wird ab vCenter Server-Version 5.0 unterstützt.

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 Netzwerkumgebung befinden, in der nur IPv4, IPv4 und IPv6 oder nur IPv6 eingesetzt wird. Allerdings muss die Maschine, die eine Verbindung zu vCenter Server über den vSphere Web Client herstellt, über eine IPv4-Adresse verfügen, damit der vSphere Authentication Proxy-Dienst funktionieren kann.

Voraussetzungen

- Installieren Sie Microsoft .NET Framework 3.5 auf dem System, auf dem Sie vSphere Authentication Proxy installieren möchten.
- Stellen Sie sicher, dass Sie über Administratorberechtigungen verfügen.
- Stellen Sie sicher, dass die Hostmaschine über einen unterstützten Prozessor und ein unterstütztes Betriebssystem verfügt.
- Achten Sie darauf, dass die Hostmaschine über eine gültige IPv4-Adresse verfügt. Sie können vSphere Authentication Proxy auf einer Maschine in einer Netzwerkumgebung installieren, in der nur IPv4 oder sowohl IPv4 als auch IPv6 eingesetzt werden. Sie können vSphere Authentication Proxy jedoch nicht in einer Netzwerkumgebung installieren, in der nur IPv6 eingesetzt wird.
- Wenn Sie vSphere Authentication Proxy auf einer Windows Server 2008 R2-Hostmaschine installieren, laden Sie den im Windows-KB-Artikel 981506 auf der Website support.microsoft.com beschriebenen Windows-Hotfix herunter und installieren Sie ihn. Wenn dieser Hotfix nicht installiert ist, kann der vSphere Authentication Proxy-Adapter nicht initialisiert werden. Zu diesem Problem werden Fehlermeldungen in der Datei `camadapter.log` protokolliert, die den Meldungen `CAM-Website konnte nicht mit CTL gebunden werden` und `CAMAdapter konnte nicht initialisiert werden` ähneln.
- Laden Sie das vCenter Server-Installationsprogramm herunter.

Sammeln Sie die folgenden Informationen, um die Installation bzw. das Upgrade abzuschließen:

- Der Installationsspeicherort von vSphere Authentication Proxy, wenn Sie den Standardspeicherort nicht verwenden.

- Die Adresse und Anmeldeinformationen von vCenter Server, mit dem vSphere Authentication Proxy eine Verbindung herstellt: IP-Adresse oder Name, HTTP-Port, Benutzername und Kennwort.
- Der Hostname oder die IP-Adresse, die zum Identifizieren von vSphere Authentication Proxy im Netzwerk verwendet wird.

Verfahren

- 1 Fügen Sie die Hostmaschine dort hinzu, wo Sie den Authentication Proxy-Dienst für die Domäne installieren.
- 2 Verwenden Sie das Domänenadministratorkonto, um sich bei der Hostmaschine anzumelden.
- 3 Doppelklicken Sie im Software-Installationsprogrammverzeichnis auf die Datei `autorun.exe`, um das Installationsprogramm zu starten.
- 4 Wählen Sie **VMware vSphere Authentication Proxy** aus und klicken Sie auf **Installieren**.
- 5 Folgen Sie den Eingabeaufforderungen des Assistenten, um die Installation bzw. das Upgrade abzuschließen.

Während der Installation registriert sich der Authentifizierungsdienst mit der vCenter Server-Instanz, auf der Auto Deploy registriert ist.

Ergebnisse

Wenn Sie den vSphere Authentication Proxy-Dienst installieren, erstellt das Installationsprogramm ein Domänenkonto mit den entsprechenden Berechtigungen zum Ausführen des Authentication Proxy-Diensts. Der Name des Kontos beginnt mit dem Präfix `CAM-` und ihm wird ein 32-stelliges, nach dem Zufallsprinzip generiertes Kennwort zugeordnet. Das Kennwort ist so konfiguriert, dass es nie abläuft. Ändern Sie die Kontoeinstellungen nicht.

Konfigurieren eines Hosts zum Verwenden des vSphere Authentication Proxy für die Authentifizierung

Nachdem Sie den vSphere Authentication Proxy-Dienst (CAM-Dienst) installiert haben, müssen Sie den Host so konfigurieren, dass er zum Authentifizieren von Benutzern den Authentication Proxy-Server verwendet.

Voraussetzungen

Installieren Sie den vSphere Authentication Proxy-Dienst (CAM-Dienst) auf einem Host. Siehe [Installieren oder Durchführen eines Upgrades von vSphere Authentication Proxy](#).

Verfahren

- 1 Verwenden Sie den IIS-Manager auf dem Host zum Einrichten des DHCP-Adressbereichs.

Durch das Festlegen des Adressbereichs können Hosts, die DHCP im Verwaltungsnetzwerk verwenden, den Authentication Proxy-Dienst verwenden.

Option	Aktion
Für IIS 6	<ol style="list-style-type: none"> a Navigieren Sie zur Computerkontoverwaltung - Website. b Klicken Sie mit der rechten Maustaste auf das virtuelle Verzeichnis CAM ISAPI. c Wählen Sie Eigenschaften > Verzeichnissicherheit > IP-Adress- und Domännennameneinschränkungen bearbeiten > Gruppe von Computern hinzufügen.
Für IIS 7	<ol style="list-style-type: none"> a Navigieren Sie zur Computerkontoverwaltung - Website. b Klicken Sie auf das virtuelle Verzeichnis CAM ISAPI im linken Bereich und öffnen Sie IPv4-Adress- und Domäneneinschränkungen. c Wählen Sie Zulassungseintrag hinzufügen > IPv4-Adressbereich.

- 2 Wenn ein Host nicht durch Auto Deploy bereitgestellt wird, ändern Sie das Standard-SSL-Zertifikat in ein selbstsigniertes Zertifikat oder in ein von einer kommerziellen Zertifizierungsstelle (CA) signiertes Zertifikat.

Option	Beschreibung
VMCA-Zertifikat	<p>Bei Verwendung von standardmäßigen VMCA-signierten Zertifikaten müssen Sie sicherstellen, dass der Authentication Proxy-Host das VMCA-Zertifikat als vertrauenswürdig einstuft.</p> <ol style="list-style-type: none"> a Fügen Sie das VMCA-Zertifikat manuell dem Zertifikatspeicher für vertrauenswürdige Stammzertifizierungsstellen hinzu. b Fügen Sie das von VMCA signierte Zertifikat (<code>root.cer</code>) zum lokalen Speicher für vertrauenswürdige Zertifikate auf dem System hinzu, auf dem der Authentication Proxy-Dienst installiert ist. Die Datei befindet sich in <code>C:\ProgramData\VMware\CIS\data\vmca</code>. c Starten Sie den vSphere Authentication Proxy-Dienst neu.
Von einer Zertifizierungsstelle (CA) signiertes Drittanbieterzertifikat	<p>Fügen Sie das von einer Zertifizierungsstelle (CA) signierte Zertifikat (DER-codiert) zum lokalen Speicher für vertrauenswürdige Zertifikate auf dem System hinzu, auf dem der Authentication Proxy-Dienst installiert ist, und starten Sie den vSphere Authentication Proxy-Dienst neu.</p> <ul style="list-style-type: none"> ■ Windows 2003: Kopieren Sie die Zertifikatsdatei in <code>C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\vsphere Authentication Proxy\trust</code>. ■ Windows 2008: Kopieren Sie die Zertifikatsdatei in <code>C:\Program Data\VMware\vsphere Authentication Proxy\trust</code>.

Einrichten von vSphere Authentication Proxy

Ihre ESXi-Hosts können einen vSphere Authentication Proxy-Server verwenden, wenn sie über die Authentication Proxy-Zertifikatsdaten verfügen.

Sie brauchen den Server nur ein Mal zu authentifizieren.

Hinweis ESXi und der Authentication Proxy-Server müssen zur Authentifizierung berechtigt sein. Stellen Sie sicher, dass diese Authentifizierungsfunktionalität jederzeit aktiviert ist. Wenn Sie die Authentifizierung deaktivieren müssen, können Sie im Dialogfeld „Erweiterte Einstellungen“ das Attribut `UserVars.ActiveDirectoryVerifyCAMCertificate` auf 0 setzen.

Exportieren des vSphere Authentication Proxy-Zertifikats

Um den vSphere Authentication Proxy-Server mit ESXi authentifizieren zu können, müssen Sie ESXi mit dem Proxy-Serverzertifikat ausstatten.

Voraussetzungen

Installieren Sie den vSphere Authentication Proxy (CAM-Dienst) auf einem Host. Siehe [Installieren oder Durchführen eines Upgrades von vSphere Authentication Proxy](#).

Verfahren

- 1 Verwenden Sie den IIS-Manager auf dem Authentifizierungs-Proxy-Serversystem, um das Zertifikat zu exportieren.

Option	Aktion
Für IIS 6	<ol style="list-style-type: none"> a Klicken Sie mit der rechten Maustaste auf Computerkontoverwaltung - Website. b Wählen Sie Eigenschaften > Verzeichnissicherheit > Zertifikat anzeigen.
Für IIS 7	<ol style="list-style-type: none"> a Klicken Sie im linken Bereich auf Computerkontoverwaltung - Website. b Wählen Sie Bindungen, um das Dialogfeld „Sitebindungen“ zu öffnen. c Wählen Sie die Bindung https aus. d Wählen Sie Bearbeiten > SSL-Zertifikat anzeigen.

- 2 Wählen Sie **Details > In Datei kopieren**.
- 3 Wählen Sie die Optionen **Nein, privaten Schlüssel nicht exportieren** und **Base-64-codiert X.509 (.CER)** aus.

Nächste Schritte

Importieren Sie das Zertifikat in ESXi.

Importieren eines Proxy-Serverzertifikats in ESXi

Um den vSphere Authentication Proxy-Server mit ESXi authentifizieren zu können, laden Sie das Proxy-Serverzertifikat auf ESXi hoch.

Sie verwenden die Benutzeroberfläche des vSphere Web Client, um das vSphere Authentication Proxy-Serverzertifikat auf den ESXi-Host hochzuladen.

Voraussetzungen

Installieren Sie den vSphere Authentication Proxy-Dienst (CAM-Dienst) auf einem Host. Siehe [Installieren oder Durchführen eines Upgrades von vSphere Authentication Proxy](#).

Exportieren Sie das Zertifikat des vSphere Authentication Proxy-Servers, wie unter [Exportieren des vSphere Authentication Proxy-Zertifikats](#) beschrieben.

Verfahren

- 1 Wechseln Sie zu dem Host, klicken Sie auf die Registerkarte **Verwalten**, auf **Einstellungen** und anschließend auf **Authentifizierungsdienste**.
- 2 Klicken Sie auf **Zertifikat importieren**.
- 3 Geben Sie den vollständigen Pfad zur Authentication Proxy-Server-Zertifikatsdatei auf dem Host und die IP-Adresse des Authentication Proxy-Servers ein.

Verwenden Sie das Formular [*Datenspeichername*] *Dateipfad*, um den Pfad des Proxy-Servers einzugeben.

- 4 Klicken Sie auf **OK**.

Verwenden des vSphere Authentication Proxy zum Hinzufügen eines Hosts zu einer Domäne

Wenn Sie einen Host zu einer Verzeichnisdienst-Domäne hinzufügen, können Sie für die Authentifizierung den vSphere Authentication Proxy anstelle von benutzerdefinierten Active Directory-Anmeldeinformationen verwenden.

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

- Stellen Sie mit dem vSphere Web Client eine Verbindung zu einem vCenter Server-System her.
- Wenn ESXi mit einer DHCP-Adresse konfiguriert ist, legen Sie den DHCP-Bereich fest.
- Wenn ESXi mit einer statischen IP-Adresse konfiguriert ist, stellen Sie sicher, dass sein zugehöriges Profil so konfiguriert ist, dass zum Beitreten einer Domäne der vSphere Authentication Proxy-Dienst verwendet wird, damit der Authentifizierungs-Proxy-Server der IP-Adresse von ESXi vertrauen kann.
- Wenn ESXi ein VMCA-signiertes Zertifikat verwendet, stellen Sie sicher, dass der Host zu vCenter Server hinzugefügt wurde. Dies ermöglicht dem Authentifizierungs-Proxy-Server ESXi zu vertrauen.

- Wenn ESXi ein CA-signiertes Zertifikat verwendet und nicht durch Auto Deploy bereitgestellt wird, stellen Sie sicher, dass das CA-Zertifikat zum lokalen Zertifikatspeicher des Authentifizierungs-Proxy-Servers hinzugefügt wurde, wie unter [Konfigurieren eines Hosts zum Verwenden des vSphere Authentication Proxy für die Authentifizierung](#) beschrieben.
- Führen Sie eine Authentifizierung des vSphere Authentication Proxy-Servers mit dem Host durch.

Verfahren

- 1 Wählen Sie im vSphere Web Client den Host aus und klicken Sie auf die Registerkarte **Verwalten**.
- 2 Klicken Sie auf **Einstellungen** und wählen Sie **Authentifizierungsdienste** aus.
- 3 Klicken Sie auf **Domäne beitreten**.
- 4 Geben Sie eine Domäne ein.
Verwenden Sie das Formular `name.tld` oder `name.tld/container/path`.
- 5 Wählen Sie **Proxy-Server verwenden** aus.
- 6 Geben Sie die IP-Adresse des Authentication Proxy-Servers ein.
- 7 Klicken Sie auf **OK**.

Ersetzen des Authentifizierungs-Proxy-Zertifikats für den ESXi-Host

Sie können ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle vom vSphere Web Client aus importieren.

Voraussetzungen

- Laden Sie die Authentifizierungs-Proxy-Zertifikatsdatei auf den ESXi-Host hoch.

Verfahren

- 1 Wählen Sie im vSphere Web Client den ESXi-Host aus.
- 2 Wählen Sie auf der Registerkarte **Einstellungen** im Bereich **System** die Option **Authentifizierungsdienste** aus.
- 3 Klicken Sie auf **Zertifikat importieren**.
- 4 Geben Sie den Pfad des SSL-Zertifikats und den vSphere Authentication Proxy-Server ein.

Empfohlene Vorgehensweisen für die Sicherheit von ESXi

Die Einhaltung der empfohlenen Vorgehensweisen für die Sicherheit in Bezug auf ESXi ist eine wichtige Maßnahme zur Wahrung der Integrität Ihrer vSphere-Bereitstellung. Weitere Informationen finden Sie im *Hardening-Handbuch*.

Überprüfen der Installationsmedien

Überprüfen Sie nach dem Download eines ISO-Images, Offline-Pakets oder Patches stets den Hashwert der Datei, um die Integrität und Authentizität der heruntergeladenen Dateien sicherzustellen. Wenn Sie physische Medien von VMware erhalten und das Sicherheitssiegel beschädigt ist, schicken Sie die Software an VMware zurück, um Ersatz zu erhalten.

Nach dem Herunterladen der Medien überprüfen Sie mithilfe des MD5-Summenwerts die Integrität des Downloads. Vergleichen Sie die ausgegebene MD5-Summe mit dem auf der VMware-Website angegebenen Wert. Jedes Betriebssystem verwendet eine andere Methode und ein anderes Tool zum Überprüfen der MD5-Summenwerte. Für Linux verwenden Sie den Befehl „md5sum“. Für Microsoft Windows können Sie ein Add-On-Produkt herunterladen.

Manuelles Überprüfen von CRLs

Standardmäßig unterstützt ein ESXi-Host die CRL-Überprüfung nicht. Sie müssen manuell nach widerrufenen Zertifikaten suchen und sie entfernen. Diese Zertifikate sind in der Regel benutzerdefinierte generierte Zertifikate von einer Unternehmens- oder einer Drittanbieter-Zertifizierungsstelle. Viele Unternehmen verwenden Skripts, um auf ESXi-Hosts nach widerrufenen SSL-Zertifikaten zu suchen und sie zu ersetzen.

Überwachen der Active Directory-Gruppe „ESX Admins“

Die Active Directory-Gruppe, die von vSphere verwendet wird, wird von der erweiterten Einstellung `plugins.hostsvc.esxAdminsGroup` definiert. Standardmäßig ist diese Option auf „ESX Admins“ festgelegt. Alle Mitglieder der „ESX Admins“-Gruppe haben vollständigen Verwaltungszugriff auf alle ESXi-Hosts in der Domäne.. überwachen Sie Active Directory bezüglich der Erstellung dieser Gruppe und beschränken Sie die Mitgliedschaft auf hoch vertrauenswürdige Benutzer und Gruppen.

Überwachen von Konfigurationsdateien

Obwohl die meisten ESXi-Konfigurationseinstellungen über eine API gesteuert werden, betrifft eine begrenzte Anzahl der Konfigurationsdateien den Host direkt. Diese Dateien werden über die vSphere-Dateitransfer-API offengelegt, die HTTPS verwendet. Wenn Sie Änderungen an diesen Dateien vornehmen, müssen Sie auch die entsprechende Verwaltungsaktion wie z. B. eine Konfigurationsänderung vornehmen.

Hinweis Versuchen Sie nicht, Dateien zu überwachen, die NICHT über diese Dateitransfer-API offengelegt werden.

Verwenden von vmkfstools zum Löschen vertraulicher Daten

Wenn Sie eine VMDK-Datei mit vertraulichen Daten löschen, fahren Sie die virtuelle Maschine herunter bzw. halten Sie sie an und senden Sie den vCLI-Befehl `vmkfstools --writezeros` für diese Datei. Sie können dann die Datei aus dem Datenspeicher löschen.

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

durch einen fehlerhaften oder bösartigen Code ausgelöst werden, wie z. B. ein Gerätetreiber, der im Gastbetriebssystem im privilegierten Modus ausgeführt wird. Branchenübliche Hardware und Firmware verfügen derzeit nicht über ausreichend Unterstützung zur Fehlereingrenzung, damit ESXi die Schwachstelle vollständig beheben kann.

Es wird empfohlen, PCI- oder PCIe-Passthrough zu einer virtuellen Maschine nur dann zu verwenden, 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 Passthrough-Hardware-Geräten oder aber aufgrund von Problemen mit Treibern im Gastbetriebssystem auftreten.
- Das Gastbetriebssystem generiert möglicherweise einen DMA-Vorgang (Direct Memory Access), der einen IOMMU-Seitenfehler auf dem ESXi-Host verursacht, z. B. wenn der DMA-Vorgang eine Adresse außerhalb des Speichers der virtuellen Maschine zum Ziel hat. Auf einigen Maschinen konfiguriert Host-Firmware IOMMU-Fehler, um durch ein nicht maskierbares Interrupt (NMI) einen schweren Fehler zu melden, was zum Absturz des ESXi-Hosts führt. Dieses Problem kann aufgrund von Problemen mit den Treibern im Gastbetriebssystem auftreten.
- Wenn das Betriebssystem auf dem ESXi-Host nicht das Neuordnen von Interrupts verwendet, injiziert das Gastbetriebssystem möglicherweise einen störenden Interrupt in den ESXi-Host auf einem beliebigen Vektor. ESXi verwendet derzeit das Neuordnen von Interrupts auf den Intel-Plattformen, wo dies verfügbar ist. Das Neuordnen von Interrupts stellt einen Teil des Intel VT-d-Funktionssatzes dar. ESXi verwendet das Neuordnen von Interrupts nicht auf AMD-Plattformen. Ein störender Interrupt führt wahrscheinlich zu einem Absturz des ESXi-Hosts. Theoretisch sind jedoch u. U. andere Möglichkeiten für das Ausnutzen von Interrupts vorhanden.

Konfigurieren der Smartcard-Authentifizierung für ESXi

Sie können sich mit Chipkarten-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 Standardeingabeaufforderung für einen Benutzernamen und ein Kennwort verwenden.

Eine Chipkarte (Smartcard) ist eine kleine Plastikkarte mit einem integrierten Schaltkreis (Chip). Viele staatliche Behörden und große Unternehmen verwenden eine auf Chipkarten basierende Zwei-Faktor-Authentifizierung, um die Sicherheit ihrer Systeme zu erhöhen und bestehende Sicherheitsbestimmungen zu erfüllen.

Wenn Chipkarten-Authentifizierung auf einem ESXi-Host aktiviert ist, brauchen Sie für die DCUI eine gültige Chipkarte und eine PIN-Kombination anstelle des standardmäßigen Benutzernamens und Kennworts.

- 1 Wenn Sie die Chipkarte in den Chipkartenleser 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 Chipkarte gespeicherten PIN und überprüft das Zertifikat auf der Chipkarte mit Active Directory.
- 4 Nach erfolgreicher Prüfung des Chipkartenzertifikats 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 Chipkarte gesperrt. Eine gesperrte Chipkarte kann nur von ausgewähltem Personal entsperrt werden.

Smartcard-Authentifizierung aktivieren

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 Web Client zum Hinzufügen von Stammzertifikaten. Siehe [Zertifikatsverwaltung für ESXi-Hosts](#).

Verfahren

- 1 Navigieren Sie zum Host im vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 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).
- 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 die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 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 von Anmeldedaten im Falle von Konnektivitätsproblemen

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. Wenn keine Verbindung zum AD-Sever besteht, können Sie sich mit den Anmeldedaten eines lokalen ESXi-Benutzers bei der ESXi-DCUI anmelden. So können Sie Diagnoseschritte ausführen oder andere Notfallmaßnahmen ergreifen. 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 [Angaben 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.

ESXi-SSH-Schlüssel

Sie können einen SSH-Schlüssel verwenden, um den Zugang zu einem ESXi-Host zu beschränken, zu steuern und zu sichern. Mithilfe eines SSH-Schlüssels können Sie vertrauenswürdigen Benutzern oder Skripts die Anmeldung zu einem Host erlauben, 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. Es ist auch möglich, HTTPS PUT zu 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 auf den Host ist mit bestimmten Risiken verbunden und in einer abgesicherten Umgebung nicht zu empfehlen. Weitere Informationen hierzu finden Sie unter [Deaktivieren autorisierter Schlüssel \(SSH\)](#).

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. Das wird in ESXi 5.1 behoben.

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.

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 Skripts zum Ausführen von Routinetätigkeiten schreiben.

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

- Autorisierte Schlüsseldatei für 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.

Verfahren

- ◆ Verwenden Sie in der Befehlszeile oder auf einem Verwaltungsserver den `vifs`-Befehl, um den SSH-Schlüssel auf den 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	<code>/host/ssh_root_authorized_keys</code> Sie benötigen zum Hochladen dieser Datei vollständige Administratorrechte.
RSA-Schlüssel	<code>/host/ssh_host_rsa_key</code>
Öffentliche RSA-Schlüssel	<code>/host/ssh_host_rsa_key</code>

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	<code>https://Hostname_oder_IP-Adresse/host/ssh_root_authorized_keys</code> Sie benötigen zum Hochladen dieser Datei vollständige Administratorrechte auf dem Host.
DSA-Schlüssel	<code>https://Hostname_oder_IP-Adresse/host/ssh_host_dsa_key</code>
Öffentliche DSA-Schlüssel	<code>https://Hostname_oder_IP-Adresse/host/ssh_host_dsa_key_pub</code>
RSA-Schlüssel	<code>https://Hostname_oder_IP-Adresse/host/ssh_host_rsa_key</code>
Öffentliche RSA-Schlüssel	<code>https://Hostname_oder_IP-Adresse/host/ssh_host_rsa_key_pub</code>

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.

Siehe *vSphere-Sicherheit*.

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 die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 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 die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
- 4 Wählen Sie „UserVars.ESXiShellTimeOut“ und klicken Sie auf das Symbol **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 die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 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.

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. Siehe [Erstellen einer Zeitüberschreitung für die ESXi Shell-Verfügbarkeit in der Benutzerschnittstelle der direkten Konsole](#) und [Erstellen einer Zeitüberschreitung für die 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 die 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 Sie sich das nächste Mal bei der ESXi Shell anmelden. Sie gelten nicht für aktuelle Sitzungen.

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.

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

Um Ihrer Umgebung einen optimalen Schutz zu bieten, sollen Sie sich über die Sicherheitsrisiken im Klaren sein, die es gibt, wenn Sie Auto Deploy mit Hostprofilen verwenden.

Netzwerksicherheit

Sichern Sie Ihr Netzwerk wie bei jeder anderen PXE-basierten Bereitstellungsmethode. 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 Hostanpassungseinstellung 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-Authentifizierungsdienst zum Einrichten von Active Directory, um zu verhindern, dass die Active Directory-Kennwörter freigelegt 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.

Verwalten der ESXi-Protokolldateien

Protokolldateien sind eine wichtige Komponente bei der Fehlersuche nach Angriffen und für die Suche nach Informationen über Verletzungen der Hostsicherheit. 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 für den Host verfügbaren Serveraktivität.
- Die Remoteprotokollierung auf einem zentralen Host ermöglicht Ihnen die Sammlung von Protokolldateien auf einem zentralen Host, auf dem Sie alle Hosts mit einem einzigen Tool überwachen können. Sie können auch eine kumulierte Analyse und Suche in den Protokolldaten durchführen und damit Informationen über bestimmte Ereignisse wie koordinierte Angriffe auf mehrere Hosts erfassen.
- Konfigurieren Sie das sichere Remote-Syslog auf ESXi-Hosts mit einer Remote-Befehlszeile wie vCLI oder PowerCLI oder mit einem API-Client.
- Fragen Sie die Syslog-Konfiguration ab, um sicherzustellen, dass ein gültiger Syslog-Server konfiguriert wurde, einschließlich des richtigen Ports.

Konfiguration von Syslog auf ESXi-Hosts

Auf allen ESXi-Hosts wird ein syslog-Dienst (`vm syslogd`) ausgeführt, der Meldungen vom VMkernel und anderen Systemkomponenten in Protokolldateien ablegt.

Sie können den vSphere Web Client oder den vCLI-Befehl `esxcli system syslog` zum Konfigurieren des syslog-Dienstes verwenden.

Weitere Informationen zur Verwendung von vCLI-Befehlen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

Verfahren

- 1 Wählen Sie den Host im Bestandslistenbereich des vSphere Web Client aus.
- 2 Klicken Sie auf die Registerkarte **Verwalten**.
- 3 Klicken Sie im Bereich „System“ auf **Erweiterte Einstellungen**.
- 4 Suchen Sie den Bereich **Syslog** in der Liste „Erweiterte Systemeinstellungen“.
- 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	Legt die maximale Anzahl der beizubehaltenden Archive fest. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.defaultSize	Legt die Standardgröße des Protokolls in KB fest, bevor das System eine Rotation der Protokolle durchführt. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.

Option	Beschreibung
Syslog.global.LogDir	Verzeichnis, in dem Protokolle gespeichert werden. Das Verzeichnis kann sich auf gemounteten NFS- oder VMFS-Volumes befinden. Nur das Verzeichnis <code>/scratch</code> auf dem lokalen Dateisystem bleibt nach einem Neustart konsistent. Das Verzeichnis sollte das Format <code>[Datenspeichername] Pfad_zur_Datei</code> aufweisen, wobei sich der Pfad auf das Stammverzeichnis des Volumes bezieht, in dem sich das Backing für den Datenspeicher befindet. Beispielsweise ist der Pfad <code>[storage1] /systemlogs</code> dem Pfad <code>/vmfs/volumes/storage1/systemlogs</code> zuzuordnen.
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. <code>ssl://Hostname1:1514</code> . UDP (Standard), 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 Protokollgröße an, die Sie verwenden möchten.
- 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	<code>/var/log/vmkernel.log</code>	Zeichnet Aktivitäten in Verbindung mit virtuellen Maschinen und ESXi auf.
VMkernel-Warnungen	<code>/var/log/vmkwarning.log</code>	Zeichnet Aktivitäten in Verbindung mit virtuellen Maschinen auf.
VMkernel-Übersicht	<code>/var/log/vmksummary.log</code>	Wird verwendet, um die Betriebszeit und die Verfügbarkeitsstatistiken für ESXi (kommagetrennt) zu bestimmen.

Komponente	Speicherort	Zweck
ESXi-Hostagenten-Protokoll	<code>/var/log/hostd.log</code>	Enthält Informationen zum Agenten, mit dem der ESXi-Host und seine virtuellen Maschinen verwaltet und konfiguriert werden.
vCenter-Agent-Protokoll	<code>/var/log/vpxa.log</code>	Enthält Informationen zum Agenten, der mit vCenter Server kommuniziert (wenn der Host von vCenter Server verwaltet wird).
Shell-Protokoll	<code>/var/log/shell.log</code>	Enthält einen Datensatz mit allen Befehlen, die in die ESXi Shell eingegeben wurden, und die Shell-Ereignisse (z. B. bei Aktivierung der Shell).
Authentifizierung	<code>/var/log/auth.log</code>	Enthält alle Ereignisse, die sich auf die Authentifizierung für das lokale System beziehen.
Systemmeldungen	<code>/var/log/syslog.log</code>	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: <code>/vmfs/volumes/Datenspeicher/virtuelle Maschine/vmware.log</code>	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

Wenn Sie Fault Tolerance (FT) aktivieren, erfasst VMware vLockstep Eingaben und Ereignisse einer primären virtuellen Maschine und sendet sie an die sekundäre virtuelle Maschine, die auf einem anderen Host ausgeführt wird.

Dieser Protokollierungsdatenverkehr zwischen der primären und der sekundären virtuellen Maschine erfolgt unverschlüsselt und enthält Gastnetzwerk- und Storage I/O-Daten sowie die Speicherinhalte des Gastbetriebssystems. Dieser Datenverkehr kann vertrauliche Daten enthalten, 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 Fault Tolerance-Protokollierungsdatenverkehr.

Sichern von vCenter Server-Systemen

6

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](#)
- [Überprüfen der Fingerabdrücke bei Legacy-ESXi-Hosts](#)
- [Überprüfen der Aktivierung der SSL-Zertifikatsvalidierung über eine Netzwerkdatei-Kopie](#)
- [vCenter Server TCP- und UDP-Ports](#)
- [Steuern des Zugriffs auf das CIM-basierte Hardwareüberwachungs-Tool](#)

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 derzeit vollständige Administratorrechte für vCenter Server hat, entfernen Sie diese Zugriffsrechte und gewähren Sie die Rechte einem oder mehreren benannten vCenter Server-Administratorkonten. Gewähren Sie nur den Administratoren vollständige Administratorrechte, die diese Rechte benötigen. Gewähren Sie diese Rechte keiner Gruppe, deren Mitgliedschaft nicht streng kontrolliert wird.

Hinweis Ab vSphere 6.0 hat der lokale Administrator standardmäßig keine vollständigen Administratorrechte mehr für vCenter Server. Es wird nicht empfohlen, lokale Betriebssystembenutzer zu verwenden.

- 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.

Minimieren des Zugriffs

Sorgen Sie dafür, dass sich keine Benutzer direkt an der vCenter Server-Hostmaschine anmelden können. Benutzer, die bei vCenter Server angemeldet sind, können absichtlich oder unabsichtlich Schaden anrichten, indem sie Einstellungen und Prozesse ändern. Sie haben auch potenziell Zugriff auf vCenter-Anmeldedaten wie das SSL-Zertifikat. Erlauben Sie nur Benutzern mit legitimen Aufgaben, sich am System anzumelden, und vergewissern Sie sich, dass diese Anmeldeereignisse überprüft werden.

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.

Gewähren von minimalen Rechten für vCenter Server-Datenbankbenutzer

Der Datenbankbenutzer benötigt nur bestimmte Rechte für den Datenbankzugriff. Außerdem sind einige Rechte nur für die Installation und das Upgrade erforderlich. Diese Rechte können entfernt werden, nachdem das Produkt installiert oder aktualisiert wurde.

Beschränken des Zugriffs auf den Datenspeicherbrowser

Mithilfe des Datenspeicherbrowsers können Benutzer mit entsprechenden Rechten Dateien auf Datenspeichern über den Webbrowser oder den vSphere Web Client anzeigen, hochladen oder herunterladen, die im Zusammenhang mit der vSphere-Bereitstellung stehen. Weisen Sie das Recht **Datenspeicher.Datenspeicher durchsuchen** nur Benutzern oder Gruppen zu, die tatsächlich diese Rechte benötigen.

Beschränken der Ausführung von Befehlen durch Benutzer innerhalb einer virtuellen Maschine

Standardmäßig kann ein Benutzer mit vCenter Server-Administratorrolle mit Dateien und Programmen 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. Siehe [Beschränken der Ausführung von Befehlen durch Benutzer innerhalb einer virtuellen Maschine](#).

Überprüfen der Kennwortrichtlinie für vpxuser

Standardmäßig ändert vCenter Server das vpxuser-Kennwort automatisch alle 30 Tage. Vergewissern Sie sich, dass diese Einstellung Ihre Richtlinien erfüllt, oder konfigurieren Sie die Richtlinie so, dass sie die Kennwortablauf Richtlinien Ihres Unternehmens erfüllt. Siehe [Festlegen der vCenter Server-Kennwortrichtlinie](#).

Hinweis Vergewissern Sie sich, dass die Kennwortablauf Richtlinie 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 Benutzergruppe, dem/der die Administratorrolle für den Root-Ordner zugeordnet ist, während eines Neustarts nicht als gültiger Benutzer bzw. gültige Gruppe verifiziert werden kann, wird die Rolle aus diesem Benutzer oder der Gruppe entfernt. Stattdessen weist vCenter Server dem vCenter Single Sign On-Konto administrator@vsphere.local die Administratorrolle zu. Dieses Konto kann dann als Administrator fungieren.

Richten Sie erneut ein benanntes Administratorkonto ein und weisen Sie diesem Konto die Administratorrolle zu, um die Verwendung des anonymen Kontos 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 die Registerkarte **Verwalten** und die untergeordnete Registerkarte **Einstellungen**.
- 3 Klicken Sie auf **Erweiterte Einstellungen** und geben Sie **VimPasswordExpirationInDays** im Filterfeld ein.
- 4 Legen Sie `VirtualCenter.VimPasswordExpirationInDays` entsprechend Ihren Anforderungen fest.

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*.

Entfernen abgelaufener oder widerrufenen Zertifikate und Protokolle fehlgeschlagener Installationen

Wenn Sie abgelaufene oder widerrufenen 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 widerrufen Zertifikate entfernt werden:

- Wenn abgelaufene oder widerrufen Zertifikate nicht vom vCenter Server-System entfernt werden, wird die Umgebung anfällig für Man-in-the-Middle-Angriffe (MITM).
- In bestimmten Fällen wird eine Protokolldatei, die das Datenbankkennwort als normalen Text enthält, auf dem System erstellt, wenn die Installation von vCenter Server fehlschlägt. Ein Angreifer, der in das vCenter Server eindringt, könnte sich Zugriff auf dieses Kennwort verschaffen und zugleich auf die vCenter Server-Datenbank zugreifen.

Begrenzen der vCenter Server-Netzwerkonnektivität

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 Netzwerkonnektivität 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 Netzwerkonnektivität 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.

Einschränken der Verwendung von Linux-Clients

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.

Selbst wenn Sie die VMCA-signierten Zertifikate im vCenter Server-System und auf den ESXi-Hosts durch von einer Drittanbieter-Zertifizierungsstelle signierte Zertifikate ersetzt haben, ist die Kommunikation mit Linux-Clients dennoch 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.

Untersuchen der installierten 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.

Eine vCenter-Installation enthält das vSphere Web Client-Extensibilitätsframework, das die Erweiterung des vSphere Web Client um Menüauswahlpunkte oder Symbole der Symbolleiste ermöglicht, über die auf vCenter-Add-On-Komponenten oder externe, webbasierte Funktionen zugegriffen werden kann. Diese Flexibilität bringt das Risiko mit sich, dass unbeabsichtigte Funktionen eingeführt werden. Wenn beispielsweise ein Administrator ein Plug-In in einer Instanz des vSphere Web Client installiert, kann das Plug-In dann auf der Berechtigungsstufe dieses Administrators beliebige Befehle ausführen.

Zur Vermeidung potenzieller Schädigungen des vSphere Web Client können Sie alle installierten Plug-Ins regelmäßig untersuchen und sicherstellen, dass alle Plug-Ins aus einer vertrauenswürdigen Quelle stammen.

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 Umgebung sicherer machen.

Konfigurieren von NTP

Stellen Sie sicher, dass alle Systeme dieselbe relative Zeitquelle (einschließlich der relevanten Lokalisierungsdivergenz) verwenden und dass die relative Zeitquelle auf einen vereinbarten Zeitstandard (wie Koordinierte Weltzeit, UTC) bezogen ist. Synchronisierte Systeme sind für die Gültigkeit des Zertifikats wesentlich. NTP vereinfacht auch die Erkennung von Eindringungsversuchen in den Protokolldateien. Bei falschen Zeiteinstellungen kann es schwierig werden, Protokolldateien zur Suche nach Angriffen zu untersuchen und abzugleichen. Dies kann zu ungenauen Ergebnissen beim Audit führen. Siehe [Synchronisieren der Uhrzeit in vCenter Server Appliance mit einem NTP-Server](#).

Beschränken des vCenter Server Appliance-Netzwerkzugriffs

Beschränken Sie den Zugriff auf die wesentlichen Komponenten, die für die Kommunikation mit der vCenter Server Appliance erforderlich sind. Durch Blockieren des Zugriffs von nicht erforderlichen Systemen aus verringern Sie die Wahrscheinlichkeit allgemeiner Angriffe auf das Betriebssystem. Durch Einschränken des Zugriffs auf die wesentlichen Komponenten werden Risiken minimiert.

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 Gehen Sie zum vCenter Server-System im vSphere Web Client-Objektnavigator.
- 2 Wählen Sie die Registerkarte **Verwalten** aus und klicken Sie auf **Einstellungen** und anschließend auf **Allgemein**.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Klicken Sie auf **SSL-Einstellungen**.

- 5 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.

- 6 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.

- 7 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 Datacenters 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 Wählen Sie die Registerkarte **Einstellungen** aus und klicken Sie auf **Erweiterte Einstellungen**.
- 3 Klicken Sie auf **Bearbeiten**.

4 Geben Sie unten im Dialogfeld den folgenden Schlüssel und Wert ein:

Feld	Wert
Schlüssel	config.nfc.useSSL
Wert	Wahr

5 Klicken Sie auf **OK**.

vCenter Server TCP- und UDP-Ports

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.

Die Tabelle enthält eine Auflistung von TCP- und UDP-Ports mit dem jeweiligen Zweck und Typ. Bei der Installation standardmäßig geöffnete Ports werden angegeben (Standard). Eine aktuelle Liste von Ports aller vSphere-Komponenten für verschiedene Versionen von vSphere finden Sie im [VMware Knowledgebase-Artikel 1012382](#).

Tabelle 6-1. vCenter Server TCP- und UDP-Ports

Port	Zweck
80 (Standard)	HTTP-Zugriff vCenter Server benötigt Port 80 für direkte HTTP-Verbindungen. Port 80 leitet Anforderungen an HTTPS-Port 443 weiter. Diese Umleitung ist nützlich, falls Sie versehentlich <code>http://server</code> anstelle von <code>https://server</code> verwenden. WS-Management (Port 443 muss offen sein)
88, 2013	RPC des Schnittstellen-Steuerelements für Kerberos, verwendet von vCenter Single Sign On.
123	NTP-Client
135 (Standard)	Für die vCenter Server Appliance ist dieser Port für die Active Directory-Authentifizierung vorgesehen. Bei einer vCenter Server-Installation unter Windows wird dieser Port für den verknüpften Modus verwendet, und Port 88 wird für die Active Directory-Authentifizierung verwendet.
161 (Standard)	SNMP-Server. Dies ist sowohl auf einem ESXi-Host als auch auf einer vCenter Server Appliance der Standardport.
389	LDAP von vCenter Single Sign On (6.0 und höher)
636	LDAPS von vCenter Single Sign On (6.0 und höher)
443 (Standard)	vCenter Server-Systeme verwenden den Port 443, um die Datenübertragung von SDK-Clients zu überwachen. Dieser Port wird auch für die folgenden Dienste verwendet: <ul style="list-style-type: none"> ■ WS-Management (Port 80 muss offen sein) ■ Verbindungen von Netzwerkverwaltungs-Clients von Drittanbietern mit vCenter Server ■ Zugriff von Netzwerkverwaltungs-Client von Drittanbietern auf Hosts

Tabelle 6-1. vCenter Server TCP- und UDP-Ports (Fortsetzung)

Port	Zweck
2012	RPC-Port für VMware Directory Service (vmdir).
2014	RPC-Port für VMware Certificate Authority (VMCA).
2020	RPC-Port für VMware Authentication Framework-Dienst (vmafd).
31031, 44046 (Standard)	vSphere Replication
7444	HTTPS von vCenter Single Sign On.
8093	Das Client-Integrations-Plug-In verwendet einen lokalen Loopback-Hostnamen und Port 8093 sowie zufällige Ports im Bereich von 50100 bis 60099. Das Client-Integrations-Plug-In verwendet Port 8093 nur für die lokale Kommunikation. Der Port bleibt möglicherweise durch die Firewall blockiert.
8109	VMware Syslog Collector.
9443	vSphere Web Client HTTP-Zugriff auf ESXi-Hosts.
10080	Inventory Service.
11711	LDAP von vCenter Single Sign On (Umgebungen, für die ein Upgrade von vSphere 5.5 durchgeführt wird)
11712	LDAPS von vCenter Single Sign On (Umgebungen, für die ein Upgrade von vSphere 5.5 durchgeführt wird)
12721	VMware Identity Management Service.
15005	ESX Agent Manager (EAM). Ein ESX-Agent kann eine virtuelle Maschine oder ein optionales VIB sein. Der Agent erweitert die Funktionen eines ESXi-Hosts um zusätzliche Dienste, die eine vSphere-Lösung wie etwa NSX-v oder vRealize Automation benötigt.
15007	vService Manager (VSM). Dieser Dienst registriert vCenter Server-Erweiterungen. Öffnen Sie diesen Port nur, wenn dies für Erweiterungen erforderlich ist, die Sie verwenden möchten.
50100-60099	Das Client-Integrations-Plug-In verwendet einen lokalen Loopback-Hostnamen und Port 8093 sowie zufällige Ports im Bereich von 50100 bis 60099. Das Client-Integrations-Plug-In verwendet diesen Portbereich nur für die lokale Kommunikation. Der Port bleibt möglicherweise durch die Firewall blockiert.

Zusätzlich zu diesen Ports können Sie bei Bedarf weitere Ports konfigurieren.

Steuern des Zugriffs auf das CIM-basierte Hardwareüberwachungs-Tool

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 Anwendungen nur den nötigen Mindestzugriff einräumen. Wenn eine Anwendung mit einem Root- oder Volladministratorkonto bereitgestellt wurde und die Anwendung manipuliert wird, ist möglicherweise die gesamte virtuelle Umgebung gefährdet.

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

CIM-Anbieter werden als Mechanismus zum Bereitstellen des Verwaltungszugriffs auf Gerätetreiber und die zugrunde liegende Hardware verwendet. Hardwareanbieter einschließlich Serverhersteller und Anbieter spezieller Hardwaregeräte können Anbieter für die Überwachung und Verwaltung ihrer speziellen Geräte entwickeln. VMware schreibt auch Anbieter, mit denen die Überwachung von Serverhardware, ESXi-Speicherinfrastruktur und virtualisierungsspezifischen Ressourcen implementiert wird. Diese Anbieter werden im ESXi-System ausgeführt. Aus diesem Grund sind sie sehr leichtgewichtig und auf spezifische Verwaltungsaufgaben ausgerichtet. Der CIM-Broker erfasst Informationen von allen CIM-Anbietern und stellt sie der Außenwelt über Standard-APIs bereit, wobei WS-MAN der geläufigste ist.

Stellen Sie Remoteanwendungen keine Root-Anmeldedaten für den Zugriff auf die CIM-Schnittstelle bereit. Erstellen Sie stattdessen ein für diese Anwendungen bestimmtes Dienstkonto und gewähren Sie jedem auf dem ESXi-System festgelegten lokalen Konto sowie jeder in vCenter Server definierten Rolle Nur-Lesezugriff auf CIM-Informationen.

Verfahren

- 1 Erstellen Sie ein für CIM-Anwendungen bestimmtes Dienstkonto.
- 2 Gewähren Sie jedem auf dem ESXi-System festgelegten lokalen Konto sowie jeder in vCenter Server definierten Rolle Nur-Lesezugriff auf CIM-Informationen.
- 3 (Optional) Wenn die Anwendung Schreibzugriff auf die CIM-Schnittstelle erfordert, erstellen Sie eine auf das Dienstkonto anzuwendende Rolle mit nur zwei Rechten:
 - **Host.Config.SystemManagement**
 - **Host.CIM.CIMInteraction**

Diese Rolle kann je nach Funktionsweise der Überwachungsanwendung lokal auf dem Host oder auf vCenter Server zentral definiert sein.

Ergebnisse

Wenn sich ein Benutzer am Host mit dem Dienstkonto anmeldet, das Sie für CIM-Anwendungen erstellt haben, verfügt er nur über die Rechte **SystemManagement** und **CIMInteraction** oder hat nur Lesezugriff.

Sichern von virtuellen Maschinen

7

Das Gastbetriebssystem, das in der virtuellen Maschine läuft, ist denselben Sicherheitsrisiken ausgesetzt wie ein physisches System. Sichern Sie virtuelle Maschinen so, wie Sie physische Maschinen sichern würden.

Dieses Kapitel enthält die folgenden Themen:

- Beschränken informativer Meldungen von virtuellen Maschinen auf VMX-Dateien
- Verhindern des Verkleinerns von virtuellen Festplatten
- Virtuelle Maschine – Empfohlene Vorgehensweisen für die Sicherheit

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 kann auftreten, wenn Sie die Größe der VMX-Datei einer virtuellen Maschine nicht kontrollieren und die Informationsmenge die Kapazität des Datenspeichers überschreitet.

Die Konfigurationsdatei, welche die informativen Name/Wert-Paare enthält, ist standardmäßig auf 1 MB beschränkt. Diese Kapazität reicht für die meisten Fälle aus, aber Sie können den Wert erforderlichenfalls ändern. Beispiel: Sie können die Grenze erhöhen, wenn große Mengen benutzerdefinierter Informationen in der Konfigurationsdatei gespeichert werden.

Hinweis Wägen Sie sorgfältig ab, wie viele Informationen Sie benötigen. Wenn die Informationsmenge die Kapazität des Datenspeichers überschreitet, kann dies zu einer Dienstverweigerung führen.

Das Standardlimit von 1 MB wird auch dann angewendet, wenn der Parameter `tools.setInfo.sizeLimit` in den erweiterten Optionen nicht aufgeführt wird.

Verfahren

- 1 Suchen Sie die virtuelle Maschine in der Bestandsliste des vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus.
 - b Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
- 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 Suchen Sie die virtuelle Maschine in der Bestandsliste des vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus.
 - b Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
- 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 können auf die Energieverwaltung der virtuellen Maschine und auf Konnektivitätssteuerelemente des Wechselmediums zugreifen, wodurch eventuell ein böswilliger Angriff auf eine virtuelle Maschine ermöglicht wird.

■ 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 nicht benötigt werden, verringern Sie die Anzahl angreifbarer Komponenten.

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, dass 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 grundlegenden Sicherheitsniveau erstellt werden.

Sie können Vorlagen verwenden, die ein abgesichertes, gepatchtes und korrekt konfiguriertes Betriebssystem enthalten, um andere, anwendungsspezifische Vorlagen zu erstellen, oder mithilfe der Anwendungsvorlage virtuelle Maschinen bereitstellen.

Verfahren

- ◆ Stellen Sie Vorlagen für die Erstellung von virtuellen Maschinen bereit, die abgesicherte, gepatchte und korrekt konfigurierte Betriebssystembereitstellungen enthalten.

Wenn möglich, stellen Sie auch Anwendungen in Vorlagen bereit. Achten Sie darauf, dass die Anwendungen nicht von Informationen abhängen, die spezifisch für eine virtuelle Maschine sind, die bereitgestellt werden soll.

Nächste Schritte

Weitere Informationen zu Vorlagen finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Beschränken der Verwendung der VM-Konsole auf ein Minimum

Die VM-Konsole bietet für eine virtuelle Maschine dieselbe Funktionalität wie ein Monitor auf einem physischen Server. Benutzer mit Zugriff auf die VM-Konsole können auf die Energieverwaltung der virtuellen Maschine und auf Konnektivitätssteuerelemente des Wechselmediums zugreifen, wodurch eventuell ein böswilliger Angriff auf eine virtuelle Maschine ermöglicht wird.

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 zur Konsole auf so wenig Verbindungen wie nötig.

Beschränken Sie beispielsweise in einer Hochsicherheitsumgebung die Verbindungen auf eine. In manchen Umgebungen können Sie dieses Limit erhöhen, je nachdem, wie viele gleichzeitige Verbindungen für übliche 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 *Handbuch zur vSphere-Ressourcenverwaltung*.

Deaktivieren unnötiger Funktionen innerhalb von virtuellen Maschinen

Jeder Dienst, der in einer virtuellen Maschine ausgeführt wird, ist ein potenzielles Angriffsziel. Indem Sie Systemkomponenten deaktivieren, die zur Ausführung der Anwendung bzw. des Dienstes nicht benötigt werden, verringern Sie die Anzahl angreifbarer Komponenten.

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 nicht verwendete Anzeigefunktionen oder HGFS (Host Guest-Dateisystem).
- ◆ 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 ohne 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 ungenutzter Hardwaregeräte kann somit Angriffe verhindern.

Ein Angreifer mit Zugang zu einer virtuellen Maschine kann ein nicht verbundenes Hardwaregerät verbinden und auf vertrauliche Informationen auf dem Medium zugreifen, das sich im Laufwerk befindet. Er kann auch einen Netzwerkadapter trennen und die virtuelle Maschine vom Netzwerk isolieren, was zu einem Denial-of-Service führt.

- Vergewissern Sie sich, dass nicht autorisierte Geräte nicht verbunden sind, und entfernen Sie nicht benötigte oder nicht benutzte Hardwaregeräte.
- Deaktivieren Sie nicht benötigte virtuelle Geräte in einer virtuellen Maschine.
- Vergewissern Sie sich, dass kein Gerät an einer virtuellen Maschine angeschlossen ist, das nicht benötigt wird. Serielle und parallele Ports werden selten für virtuelle Maschinen in einem Datacenter benutzt und CD/DVD-Laufwerke werden in der Regel nur kurzfristig während der Softwareinstallation angeschlossen.

Verfahren

- 1 Melden Sie sich bei einem vCenter Server-System mithilfe des vSphere Web Client an.
- 2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
- 3 Prüfen Sie die einzelnen Hardwaregeräte und überlegen Sie, ob sie wirklich angeschlossen sein müssen.

Prüfen Sie insbesondere auch die folgenden Geräte:

- Diskettenlaufwerke

- Serielle Schnittstellen
- 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 Suchen Sie die virtuelle Maschine in der Bestandsliste des vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus.
 - b Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
- 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 Legen Sie bei Bedarf die folgenden Parameter fest, indem Sie sie hinzufügen oder bearbeiten.

Option	Beschreibung
<code>svga.vgaonly</code>	Wenn Sie diesen Parameter auf TRUE setzen, werden erweiterte Grafikfunktionen deaktiviert. Nur der Textkonsolenmodus ist noch verfügbar. Bei dieser Einstellung bleibt der Parameter <code>mks.enable3d</code> wirkungslos. Hinweis Wenden Sie diese Einstellung nur auf virtuelle Maschinen an, die keine virtualisierte Grafikkarte benötigen.
<code>mks.enable3d</code>	Auf virtuellen Maschinen, die keine 3D-Funktion benötigen, können Sie diesen Parameter auf FALSE setzen.

Deaktivieren nicht freigelegter Funktionen

Virtuelle VMware-Maschinen sind dafür ausgelegt, sowohl auf vSphere-Systemen als auch auf gehosteten Virtualisierungsplattformen wie Workstation und Fusion zu funktionieren. Bestimmte VM-Parameter müssen nicht aktiviert werden, wenn eine virtuelle Maschine auf einem vSphere-System ausgeführt wird. Deaktivieren Sie diese Parameter, um potenzielle Schwachstellen zu vermeiden.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

- 1 Suchen Sie die virtuelle Maschine in der Bestandsliste des vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus.
 - b Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
- 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 von HGFS-Dateiübertragungen

Bestimmte Vorgänge wie automatisierte Tools-Upgrades nutzen eine Komponente im Hypervisor, die als Host Guest File System (HGFS) bezeichnet wird. In Umgebungen mit hohen Sicherheitsanforderungen können Sie diese Komponente deaktivieren und damit das Risiko minimieren, dass ein Angreifer mithilfe von HGFS Dateien innerhalb des Gastbetriebssystems übertragen kann.

Verfahren

- 1 Suchen Sie die virtuelle Maschine in der Bestandsliste des vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus.
 - b Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
- 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.

Ergebnisse

Wenn Sie diese Änderung vornehmen, reagiert der VMX-Prozess nicht mehr auf Befehle des Tools-Prozesses. APIs, die mithilfe von HGFS-Dateien zum und vom Gastbetriebssystem übertragen (z. B. manche VIX-Befehle oder das Dienstprogramm für automatische Upgrades von VMware Tools), funktionieren dann nicht mehr.

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 mit dem 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 mithilfe des 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
<code>isolation.tools.copy.disable</code>	Wahr
<code>isolation.tools.paste.disable</code>	Wahr
<code>isolation.tools.setGUIOptions.enable</code>	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. Sobald das Konsolenfenster den Eingabefokus hat, können unbefugte Benutzer und Prozesse in der virtuellen Maschine auf die Zwischenablage der Konsole der virtuellen Maschine zugreifen. Wenn ein Benutzer vor der Verwendung der Konsole vertrauliche Informationen in die Zwischenablage kopiert, macht der Benutzer der virtuellen Maschine, ggf. unwissentlich, vertrauliche Daten 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 vCenter Server-Administratorrolle mit Dateien und Programmen 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.

Seien Sie beim Zulassen des Zugriffs auf das virtuelle Datacenter aus Sicherheitsgründen so restriktiv wie beim physischen Datacenter. Um Benutzern nicht den vollen Administratorzugriff gewähren zu müssen, erstellen Sie eine benutzerdefinierte Rolle, die den Gastzugriff deaktiviert, und wenden Sie diese Rolle auf Benutzer an, die Administratorrechte benötigen, aber nicht zur Interaktion mit Dateien und Programmen innerhalb eines Gastbetriebssystems autorisiert sind.

Beispielsweise könnte eine Konfiguration eine virtuelle Maschine in der Infrastruktur mit vertraulichen Daten enthalten. Für Aufgaben wie die Migration mit vMotion und Storage vMotion muss die IT-Rolle Zugriff auf die virtuelle Maschine haben. Deaktivieren Sie in diesem Fall einige Remotevorgänge innerhalb eines Gastbetriebssystems, um sicherzustellen, dass mit der IT-Rolle kein Zugriff auf die vertraulichen Daten möglich ist.

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 von der Standardadministratorrolle.

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 haben die Möglichkeit, Geräte zu verbinden oder zu 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 dauerhaft entfernen möchten, können Sie verhindern, dass ein Benutzer oder Prozess einer virtuellen Maschine das Gerät aus dem Gastbetriebssystem heraus einbindet oder trennt.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

- 1 Suchen Sie die virtuelle Maschine in der Bestandsliste des vSphere Web Client.
 - a Wählen Sie ein Datencenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus.
 - b Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
- 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**.

Ändern des variablen Speicherlimits des Gastbetriebssystems

Sie können das variable Speicherlimit des Gastbetriebssystems erhöhen, wenn große Mengen von benutzerdefinierten Informationen in der Konfigurationsdatei gespeichert werden.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

- 1 Suchen Sie die virtuelle Maschine in der Bestandsliste des vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus.
 - b Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
- 2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
- 3 Wählen Sie **VM-Optionen > Erweitert** aus und klicken Sie auf **Konfiguration bearbeiten**.
- 4 Fügen Sie den Parameter `tools.setInfo.sizeLimit` hinzu oder bearbeiten Sie ihn und legen Sie den Wert mit einer Anzahl von Byte fest.
- 5 Klicken Sie auf **OK**.

Verhindern, dass Gastbetriebssystemprozesse Konfigurationsnachrichten an den Host senden

Sie können Gäste daran hindern, Name/Wert-Paare in die Konfigurationsdatei zu schreiben. Dies bietet sich an, wenn Gastbetriebssysteme am Ändern von Konfigurationseinstellungen gehindert werden müssen.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

- 1 Suchen Sie die virtuelle Maschine in der Bestandsliste des vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus.
 - b Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
- 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:
 - In der Spalte „Name“: **isolation.tools.setinfo.disable**
 - In der Spalte „Wert“: **Wahr**
- 6 Klicken Sie auf **OK**, um das Dialogfeld „Konfigurationsparameter“ zu schließen, und klicken Sie erneut auf **OK**.

Vermeiden der Verwendung von unabhängigen, nicht-dauerhaften Festplatten

Wenn Sie unabhängige, nicht dauerhafte Festplatten verwenden, können erfolgreiche Angreifer Beweise, dass die Maschine manipuliert wurde, durch Herunterfahren oder Neustarten des Systems beseitigen. Ohne eine dauerhafte Aufzeichnung der Aktivitäten auf einer virtuellen Maschine registrieren Administratoren einen Angriff möglicherweise überhaupt nicht. Deshalb sollten Sie die Verwendung unabhängiger, nicht dauerhafter Festplatten vermeiden.

Verfahren

- ◆ Stellen Sie sicher, dass die Aktivitäten der virtuellen Maschine auf einem separaten Server per Remoteprotokollierung aufgezeichnet werden, beispielsweise auf einem Syslog-Server oder einem gleichwertigen Windows-basierten Ereignis-Collector.
- Falls die Remoteprotokollierung von Ereignissen und Aktivitäten nicht für den Gast konfiguriert ist, sollte für „scsiX:Y.mode“ eine der folgenden Einstellungen verwendet werden:
- Nicht vorhanden
 - Nicht eingestellt auf unabhängig, nicht dauerhaft

Ergebnisse

Wenn der nicht dauerhafte Modus nicht aktiviert ist, können Sie für eine virtuelle Maschine kein Rollback auf einen bekannten Status ausführen, wenn Sie das System neu starten.

Sichern 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
- Absichern des Netzwerks mit Firewalls
- Sichern des physischen Switches
- Sichern von Standard-Switch-Ports mit Sicherheitsrichtlinien
- Sichern von vSphere Standard-Switches
- Sichern von vSphere Distributed Switches und verteilten Portgruppen
- Absichern virtueller Maschinen durch VLANs
- Erstellen einer Netzwerk-DMZ auf einem einzelnen ESXi-Host
- Erstellen mehrerer Netzwerke auf einem einzelnen ESXi-Host
- Internet Protocol Security (IPsec)
- Sicherstellen einer korrekten SNMP-Konfiguration
- Bedarfsgerechtes Verwenden von virtuellen Switches mit der vSphere Network Appliance-API
- vSphere Networking, empfohlene Vorgehensweisen für die Sicherheit

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 einigen oder allen virtuellen Maschinen im Netzwerk hinzu.

Aus Effizienzgründen können Sie private Ethernet-Netzwerke virtueller Maschinen oder Virtuelle Netzwerke einrichten. Bei virtuellen Netzwerken installieren Sie eine hostbasierte Firewall auf einer virtuellen Maschine am Eingang des virtuellen Netzwerks. Diese Firewall dient als Schutzpufferzone zwischen dem physischen Netzwerkadapter und den übrigen virtuellen Maschinen im virtuellen Netzwerk.

Da hostbasierte Firewalls die Leistung beeinträchtigen können, sollten Sie Sicherheitsbedürfnisse und Leistungsanforderungen gegeneinander abwägen, bevor Sie hostbasierte Firewalls in anderen virtuellen Maschinen im 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 virtuellen Maschinenzonen. Die Segmentierung verhindert mehrere Gefahren. Zu diesen Gefahren gehört auch die Manipulation des Adressauflösungsprotokolls (ARP), wobei der Angreifer die ARP-Tabelle so manipuliert, dass die MAC- und IP-Adressen neu zugeordnet werden, wodurch ein Zugriff auf den Netzwerkdatenverkehr vom und zum Host möglich ist. 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.

Eine sorgfältige Planung der Segmentierung senkt das Risiko von Paketübertragungen zwischen virtuellen Maschinenzonen und somit von Spionageangriffen, die voraussetzen, dass dem Opfer Netzwerkdatenverkehr zugestellt wird. 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. Jede Methode hat ihre Vorteile.

- 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 dar, und gleichzeitig ist sie am wenigsten anfällig für Konfigurationsfehler nach dem Anlegen des ersten Segments.
- Richten Sie virtuelle LANs (VLANs) zur Absicherung des Netzwerks ein. Da VLANs fast alle Sicherheitsvorteile bieten, die auch die Implementierung physisch getrennter Netzwerke aufweist, ohne dass dafür der Mehraufwand an Hardware eines physischen Netzwerks notwendig ist, stellen sie eine rentable Lösung zur Verfügung, die die Kosten für die Bereitstellung und Wartung zusätzlicher Geräte, Kabel usw. einsparen kann. Weitere Informationen hierzu finden Sie unter [Absichern virtueller Maschinen durch VLANs](#).

Verhindern des nicht autorisierten Zugriffs

Wenn das Netzwerk virtueller Maschinen an ein physisches Netzwerk angeschlossen ist, kann es ebenso Sicherheitslücken aufweisen wie ein Netzwerk, das aus physischen Maschinen besteht. Selbst wenn das virtuelle Maschinennetzwerk nicht an ein physisches Netzwerk angeschlossen ist, kann ein Angriff auf virtuelle Maschinen innerhalb des Netzwerks von anderen virtuellen Maschinen des Netzwerks aus erfolgen. Die Anforderungen an die Absicherung virtueller Maschinen und physischer Maschinen sind oft identisch.

Virtuelle Maschinen sind voneinander isoliert. Eine virtuelle Maschine kann weder Lese- noch Schreibvorgänge im Speicher der anderen virtuellen Maschine ausführen noch auf deren Daten zugreifen, ihre Anwendungen verwenden usw. Im Netzwerk kann jedoch jede virtuelle Maschine oder eine Gruppe virtueller Maschinen Ziel eines unerlaubten Zugriffs von anderen virtuellen Maschinen sein und daher weiteren Schutzes durch externe Maßnahmen bedürfen.

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. Diese Firewall bietet einen Grundschutz für das Netzwerk.

Zwischen den Clients und vCenter Server kann sich eine Firewall befinden. Abhängig von Ihrer Bereitstellung können sich vCenter Server und die Clients auch hinter einer Firewall befinden. Wichtig ist es sicherzustellen, dass eine Firewall an den Punkten vorhanden ist, die Sie als Eingangspunkte in das System betrachten.

Einer umfassende Liste der TCP- und UDP-Ports, darunter die Ports für vSphere vMotion™ und vSphere Fault Tolerance finden Sie unter [vCenter Server TCP- und UDP-Ports](#).

Netzwerke, die über vCenter Server konfiguriert werden, können Daten über den vSphere Web Client oder Netzwerkverwaltungs-Clients von Drittanbietern erhalten, die über das SDK eine Schnittstelle zum Host einrichten. Während des normalen Betriebs wartet vCenter Server an bestimmten Ports auf Daten von verwalteten Hosts und Clients. vCenter Server geht auch davon aus, dass die verwalteten Hosts an bestimmten Ports auf Daten von vCenter Server warten. Wenn sich zwischen diesen Elementen eine Firewall befindet, muss sichergestellt werden, dass Firewall-Ports für den Datenverkehr geöffnet wurden.

Firewalls können auch an vielen anderen Zugriffspunkten im Netzwerk installiert werden. Dies hängt von der Sicherheitsebene, die für die verschiedenen Geräte benötigt wird, sowie davon ab, wie das Netzwerk genutzt werden soll. Bestimmen Sie die Installationspunkte für Ihre Firewalls anhand der Sicherheitsrisiken, die eine Analyse der Netzwerkkonfiguration ergeben hat. Die folgende Liste führt verschiedene Installationspunkte für Firewalls auf, die in ESXi-Implementierungen häufig auftreten.

- 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 virtuelle Maschinen auf einen anderen Server verschieben, klonen oder vMotion verwenden möchten, müssen Sie auch Ports in allen Firewalls zwischen Quell- und Zielhost öffnen, damit Quelle und Ziel miteinander kommunizieren können.

- Zwischen ESXi-Hosts und Netzwerkspeicher, z. B. NFS- oder iSCSI-Speicher. Diese Ports sind nicht VMware-spezifisch und werden anhand der Spezifikationen für das jeweilige Netzwerk konfiguriert.

Herstellen einer Verbindung mit einem vCenter Server über eine Firewall

vCenter Server verwendet TCP-Port 443, um die Datenübertragung von den 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.

Öffnen Sie TCP-Port 443 in der Firewall, um vCenter Server den Empfang von Daten über den vSphere Web Client zu ermöglichen. Die Firewall-Konfiguration hängt von den an Ihrer Site verwendeten Komponenten ab. Weitere Informationen erhalten Sie von Ihrem lokalen Firewall-Systemadministrator.

Wenn Sie Port 443 nicht als Port für die Kommunikation zwischen vSphere Web Client und vCenter Server verwenden möchten, können Sie den Port über die vCenter Server-Einstellungen im vSphere Web Client ändern. Informationen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Falls Sie weiterhin den vSphere Client verwenden, finden Sie in der Dokumentation zur *vSphere-Administration mit vSphere Client* weitere Informationen.

Firewalls für Konfigurationen ohne vCenter Server

Sie können Clients direkt mit Ihrem ESXi-Netzwerk verbinden anstatt vCenter Server zu verwenden.

Netzwerke, die nicht über vCenter Server konfiguriert werden, können Daten über den vSphere Client, eine der vSphere-Befehlszeilenschnittstellen, das vSphere Web Services SDK oder Drittanbieter-Clients erhalten. Wenn ein vCenter Server vorhanden ist, sind die Anforderungen der Firewall größtenteils die gleichen, aber es gibt einige markante Unterschiede.

- Wie bei Konfigurationen mit vCenter Server sollten Sie sicherstellen, dass Ihre ESXi-Ebene oder, je nach Konfiguration, Ihre Clients und die ESXi-Ebene geschützt sind. 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 über den Server abgewickelt wird, ist kein getrennter Lizenzserver erforderlich. Dadurch entfällt die Firewall zwischen dem Lizenzserver und dem ESXi-Netzwerk.

Sie können Firewallports mithilfe von ESXCLI, vSphere Client oder Firewallregeln konfigurieren. Siehe [ESXi-Firewall-Konfiguration](#).

Verbinden von ESXi-Hosts über Firewalls

Wenn Sie eine Firewall zwischen zwei ESXi-Hosts eingerichtet haben und Transaktionen zwischen den Hosts ermöglichen möchten oder mit vCenter Server Quell/Ziel-Aktivitäten wie Datenverkehr im Rahmen von vSphere High Availability (vSphere HA), Migrationen, Klonen oder vMotion durchführen möchten, müssen Sie eine Verbindung konfigurieren, über die 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](#). Weitere Informationen zur Konfiguration der Ports erhalten Sie beim Firewall-Administrator.

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, ist abhängig vom Typ der VM-Konsole und ob Sie die Verbindung über vCenter Server mit dem vSphere Web Client herstellen oder direkt mit dem ESXi-Host vom vSphere Client aus.

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.

Direkte Verbindung zwischen ESXi-Hosts und dem vSphere Client

Sie können die VM-Konsole des vSphere Client verwenden, wenn Sie eine direkte Verbindung zu einem ESXi-Host herstellen.

Hinweis Verwenden Sie den vSphere Client nicht, um eine Direktverbindung mit Hosts herzustellen, die von einem vCenter Server-System verwaltet werden. Wenn Sie im vSphere Client an Hosts dieser Art Änderungen vornehmen, wird Ihre Umgebung instabil.

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

Der vSphere 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 mit Sicherheitsrichtlinien

Wie bei physischen Netzwerkadaptern kann ein Netzwerkadapter einer virtuellen Maschine Datenblöcke versenden, die von einer anderen virtuellen Maschine zu stammen scheinen oder eine andere virtuelle Maschine imitieren, damit er Datenblöcke aus dem Netzwerk empfangen kann, die für die jeweilige virtuelle Maschine bestimmt sind. Außerdem kann ein Netzwerkadapter einer virtuellen Maschine, genauso wie ein physischer Netzwerkadapter, so konfiguriert werden, dass er Datenblöcke empfängt, die für andere virtuelle Maschinen bestimmt sind. Beide Szenarien stellen ein Sicherheitsrisiko dar.

Wenn Sie einen Standard-Switch für Ihr Netzwerk erstellen, fügen Sie Portgruppen zum vSphere Web Client hinzu, um für die an den Switch angeschlossenen virtuellen Maschinen und VMkernel-Adapter Richtlinien festzulegen.

ESXi konfiguriert als Teil des Hinzufügens einer VMkernel-Portgruppe oder Portgruppe für virtuelle Maschinen zu einem Standard-Switch 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. Diese Sicherheitsfunktion wurde so implementiert, dass das Gastbetriebssystem, welches für die Imitation verantwortlich ist, nicht erkennt, dass diese verhindert wurde.

Die Sicherheitsrichtlinie bestimmt, wie streng der Schutz gegen Imitierungs- oder Abfangangriffe auf virtuelle Maschinen sein soll. Damit Sie die Einstellungen des Sicherheitsprofils richtig anwenden können, müssen Sie verstehen, wie Netzwerkadapter virtueller Maschinen Datenübertragungen steuern und wie Angriffe auf dieser Ebene vorgenommen werden. Lesen Sie den Abschnitt über Sicherheitsrichtlinien in der Veröffentlichung *vSphere-Netzwerk*.

.

Sichern von vSphere Standard-Switches

Datenverkehr auf dem Standard-Switch kann vor Ebene 2-Angriffen gesichert werden, indem einige MAC-Adressmodi mithilfe der Sicherheitseinstellungen der Switches beschränkt werden.

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 böswillige Angriffe auf die Geräte in einem Netzwerk durchführen, indem es einen Netzwerkadapter imitiert, der vom Empfängernetzwerk autorisiert wurde.

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:

- Promiscuous-Modus (siehe [Betrieb im Promiscuous-Modus](#))
- MAC-Adressänderungen (siehe [MAC-Adressänderungen](#))
- 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.

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.

Sichern von vSphere Distributed Switches und verteilten Portgruppen

Die Administratoren haben mehrere Optionen zum Sichern von vSphere Distributed Switches in ihrer vSphere-Umgebung.

Verfahren

- 1 Überprüfen Sie für verteilte Portgruppen mit statischer Bindung, ob die Funktion zum automatischen Erweitern deaktiviert ist.

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 vollständig nachverfolgbar sind, kann es zur 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 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 Feld 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 anzuzeigen, dass er nur für interne Netzwerke zwischen dem privaten virtuellen Switch einer virtuellen Maschine ist, an den keine physischen Netzwerkadapter gebunden sind.

- 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:

- Promiscuous-Modus (siehe [Betrieb im Promiscuous-Modus](#))
- MAC-Adressänderungen (siehe [MAC-Adressänderungen](#))
- 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*.

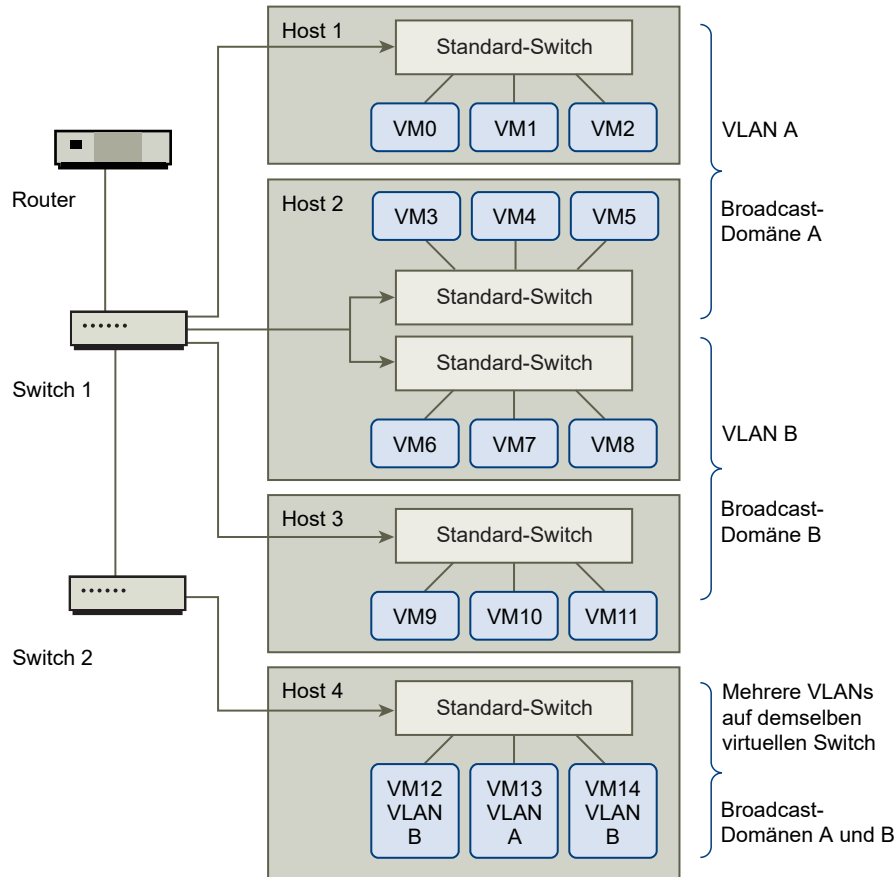
Absichern virtueller Maschinen durch VLANs

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.

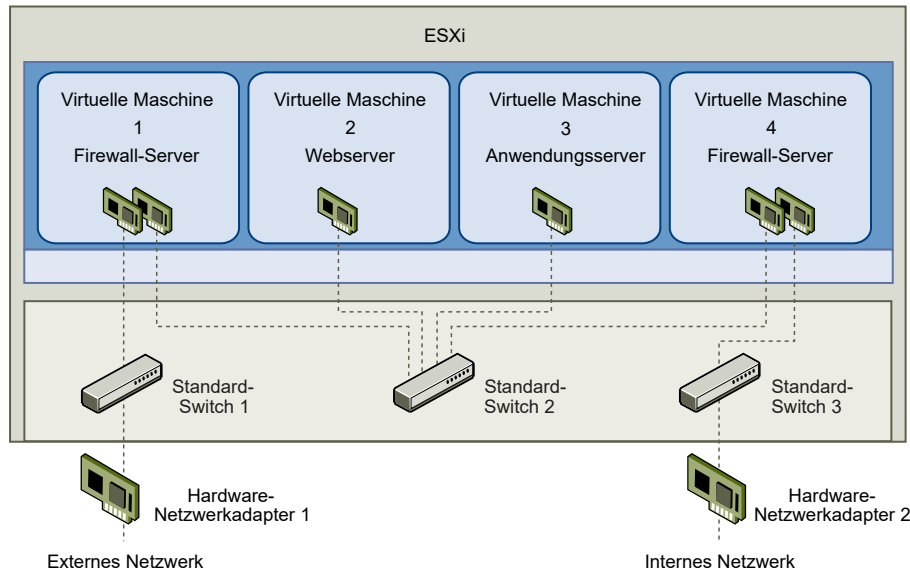
Auf einem Standard-Switch können Sie den VLAN-Netzwerkmodus auf Switch- oder Portgruppenebene konfigurieren, und auf einem Distributed Switch auf der Ebene der verteilten Portgruppe oder des Ports.

- 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 einer Netzwerk-DMZ auf einem einzelnen ESXi-Host

Ein Beispiel für die Anwendung der ESXi-Isolierung und der virtuellen Netzwerkfunktionen zur Umgebungsabsicherung ist die Einrichtung einer so genannten „entmilitarisierten Zone“ (DMZ) auf einem einzelnen Host.

Abbildung 8-2. Konfigurierte DMZ auf einem einzelnen ESXi-Host



In diesem Beispiel sind vier virtuelle Maschinen so konfiguriert, dass sie eine virtuelle DMZ auf dem Standard-Switch 2 bilden:

- Die virtuelle Maschine 1 und die virtuelle Maschine 4 führen Firewalls aus und sind über Standard-Switches an physische Netzwerkadapter angeschlossen. Diese beiden virtuellen Maschinen verwenden mehrere Switches.
- Auf der virtuellen Maschine 2 wird ein Webserver ausgeführt, auf der virtuellen Maschine 3 ein Anwendungsserver. Diese beiden virtuellen Maschinen sind mit einem virtuellen Switch verbunden.

Der Webserver und der Anwendungsserver befinden sich in der DMZ zwischen den zwei Firewalls. Die Verbindung zwischen diesen Elementen ist der Standard-Switch2, der die Firewalls mit den Servern verbindet. Dieser Switch ist nicht direkt mit Elementen außerhalb der DMZ verbunden und wird durch die beiden Firewalls vom externen Datenverkehr abgeschirmt.

Während des Betriebs der DMZ betritt externer Datenverkehr aus dem Internet die virtuelle Maschine 1 über den Hardware-Netzwerkadapter 1 (weitergeleitet vom Standard-Switch 1) und wird von der auf dieser virtuellen Maschine installierten Firewall überprüft. Wenn die Firewall den Datenverkehr autorisiert, wird er an den Standard-Switch in der DMZ, den Standard-Switch 2, weitergeleitet. Da der Webserver und der Anwendungsserver ebenfalls an diesen Switch angeschlossen sind, können sie die externen Anforderungen bearbeiten.

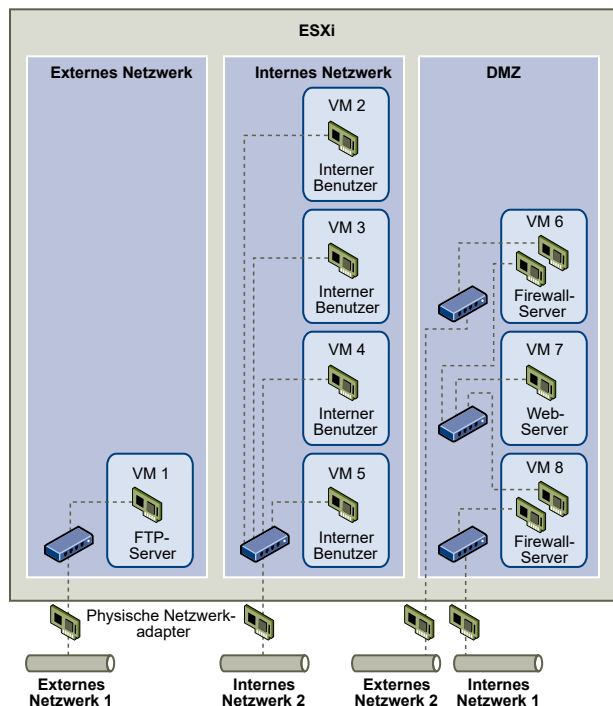
Der Standard-Switch 2 ist auch an die virtuelle Maschine 4 angeschlossen. Auf dieser virtuellen Maschine schirmt eine Firewall die DMZ vom internen Firmennetzwerk ab. Diese Firewall filtert Pakete vom Web- und Anwendungsserver. Wenn ein Paket überprüft wurde, wird es über den Standard-Switch 3 an den Hardware-Netzwerkadapter 2 weitergeleitet. Der Hardware-Netzwerkadapter 2 ist an das interne Firmennetzwerk angeschlossen.

Bei der Implementierung einer DMZ auf einem einzelnen Host können Sie relativ einfache Firewalls verwenden. Obwohl eine virtuelle Maschine in dieser Konfiguration keine direkte Kontrolle über eine andere virtuelle Maschine ausüben oder auf ihren Arbeitsspeicher zugreifen kann, sind die virtuellen Maschinen dennoch über ein virtuelles Netzwerk verbunden. Dieses Netzwerk kann für die Verbreitung von Viren oder für andere Angriffe missbraucht werden. Die virtuellen Maschinen in der DMZ sind ebenso sicher wie getrennte physische Computer, die an dasselbe Netzwerk angeschlossen sind.

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 8-3. 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
<code>--sa-source= <i>Quelladresse</i></code>	Erforderlich. Geben Sie die Quelladresse an.
<code>--sa-destination= <i>Zieladresse</i></code>	Erforderlich. Geben Sie die Zieladresse an.
<code>--sa-mode= <i>Modus</i></code>	Erforderlich. Geben Sie als Modus entweder <code>transport</code> oder <code>tunnel</code> an.

Option	Beschreibung
--sa-spi= <i>Sicherheitsparameter-Index</i>	Erforderlich. Geben Sie den Sicherheitsparameter-Index an. Der Sicherheitsparameter-Index identifiziert die Sicherheitsverbindung dem Host gegenüber. Er muss eine Hexadezimalzahl mit dem Präfix 0x sein. Jede von Ihnen erstellte Sicherheitsverbindung muss eine eindeutige Kombination aus Protokoll und Sicherheitsparameter-Index besitzen.
--encryption-algorithm= <i>Verschlüsselungsalgorithmus</i>	Erforderlich. Verwenden Sie einen der folgenden Parameter, um den Verschlüsselungsalgorithmus anzugeben. <ul style="list-style-type: none"> ■ 3des-cbc ■ aes128-cbc ■ null (bietet keine Verschlüsselung)
--encryption-key= <i>Verschlüsselungsschlüssel</i>	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= <i>Authentifizierungsalgorithmus</i>	Erforderlich. Geben Sie den Authentifizierungsalgorithmus an: hmac-sha1 oder hmac-sha2-256.
--integrity-key= <i>Authentifizierungsschlüssel</i>	Erforderlich. Geben Sie den Authentifizierungsschlüssel an. Sie können Schlüssel als ASCII-Text oder als Hexadezimalzahl mit dem Präfix 0x eingeben.
--sa-name= <i>Name</i>	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 0x6970763672656164796c6f677366465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sal
```

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= <i>Quelladresse</i>	Erforderlich. Geben Sie Quell-IP-Adresse und die Präfixlänge an.
--sp-destination= <i>Zieladresse</i>	Erforderlich. Geben Sie Zieladresse und die Präfixlänge an.
--source-port= <i>Port</i>	Erforderlich. Geben Sie den Quellport an. Der Quellport muss eine Zahl zwischen 0 und 65535 sein.
--destination-port= <i>Port</i>	Erforderlich. Geben Sie den Zielport an. Der Quellport muss eine Zahl zwischen 0 und 65535 sein.
--upper-layer-protocol= <i>Protokoll</i>	Verwenden Sie einen der folgenden Parameter, um das Protokoll für höhere Schichten anzugeben. <ul style="list-style-type: none"> ■ TCP ■ UDP ■ ICMP6 ■ alle
--flow-direction= <i>Richtung</i>	Wählen Sie als Richtung, in der Sie den Datenverkehr überwachen möchten, entweder <i>in</i> oder <i>out</i> aus.

Option	Beschreibung
--action= <i>Aktion</i>	Geben Sie mithilfe eines der folgenden Parameters die Aktion an, die ausgeführt werden soll, wenn auf Datenverkehr mit den angegebenen Parametern gestoßen wird. <ul style="list-style-type: none"> ■ 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= <i>Modus</i>	Geben Sie als Modus entweder <code>tunnel</code> oder <code>transport</code> an.
--sa-name= <i>Name der Sicherheitsverbindung</i>	Erforderlich. Geben Sie den Namen der Sicherheitsverbindung an, die die Sicherheitsrichtlinie verwenden soll.
--sp-name= <i>Name</i>	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=sal
--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 böartigen Host gesendet werden. Der böartige Host kann dann mithilfe dieser Informationen einen Angriff planen.

Verfahren

- 1 Führen Sie `esxcli system snmp get` aus, um zu bestimmen, ob SNMP aktuell verwendet wird.
- 2 Wenn Ihr System SNMP benötigt, stellen Sie durch Ausführen des Befehls `esxcli system snmp set --enable true` sicher, dass SNMP ausgeführt wird.
- 3 Falls Ihr System SNMP verwendet, finden Sie in der Dokumentation zur *Überwachung und Leistung* Setup-Informationen für SNMP 3.

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

Bedarfsgerechtes Verwenden von virtuellen Switches mit der vSphere Network Appliance-API

Wenn Sie keine Produkte verwenden, die die vSphere Network Appliance API (DvFilter) nutzen, konfigurieren Sie den Host nicht zum Senden von Netzwerkinformationen an eine virtuelle Maschine. 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 richtig 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 Um sicherzustellen, dass der Kernelparameter `Net.DVFilterBindIpAddress` den richtigen Wert hat, suchen Sie den Parameter mit dem vSphere Web Client.
 - a Wählen Sie den Host aus und klicken Sie auf die Registerkarte **Verwalten**.
 - b Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
 - c 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 Feld „Filter“ ein, um alle zugehörigen Parameter anzuzeigen.

- 2 Wenn Sie die DvFilter-Einstellungen nicht verwenden, stellen Sie sicher, dass der Wert leer ist.

- 3 Wenn Sie die DvFilter-Einstellungen verwenden, stellen Sie sicher, dass der Wert des Parameters dem Wert entspricht, den das Produkt, das DvFilter verwendet, nutzt.

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.

- Stellen Sie sicher, dass Ports physischer Switches mit Portfast konfiguriert sind, wenn STP (Spanning Tree Protocol) aktiviert ist. Da virtuelle Switches von VMware STP nicht unterstützen, muss Portfast für Ports physischer Switches, die mit einem ESXi-Host verbunden sind, konfiguriert sein, wenn STP aktiviert ist, 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 sind nicht verschlüsselt und können Informationen über das virtuelle Netzwerk enthalten, was die Wahrscheinlichkeit eines erfolgreichen Man-in-the-Middle-Angriffs erhöht. 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. Beispiel: Administratoren virtueller Maschinen sollten nur über Zugriff auf Portgruppen verfügen, in denen sich ihre virtuellen Maschinen befinden. Netzwerkadministratoren sollten Berechtigungen für alle virtuellen Netzwerkkomponenten, aber keinen Zugriff auf virtuelle Maschinen haben. 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 angegeben sind, werden jedoch mit „1“ gekennzeichnet. Deshalb wird Datenverkehr vom ESXi-Host, der das native VLAN zum Ziel hat, nicht ordnungsgemäß weitergeleitet, da er mit „1“ gekennzeichnet ist, anstatt nicht gekennzeichnet zu sein. 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, soll Datenverkehr von virtuellen Maschinen auf diesem Port nicht für das native VLAN auf dem Switch sichtbar sein, 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 Außerkräftsetzungen für die Konfiguration auf Portebene auf einem verteilten virtuellen Switch. Außerkräftsetzungen für die Konfiguration auf Portebene sind standardmäßig deaktiviert. Wenn sie aktiviert sind, ermöglichen Außerkräftsetzungen für eine virtuelle Maschine andere Sicherheitseinstellungen als die Einstellungen auf der Portgruppenebene. Für bestimmte virtuelle Maschinen sind andere Konfigurationen erforderlich. Dies muss jedoch unbedingt überwacht werden. Wenn Außerkräftsetzungen nicht überwacht werden, kann jeder, der sich Zugriff auf eine virtuelle Maschine mit einer nicht so 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.

Einführen angemessener Netzwerkisolierungspraktiken

Durch die Einführung angemessener 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 virtuellen Maschine, 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 gemeinsamen vSwitch. Der vSwitch kann für den Produktsdatenverkehr (virtuelle Maschine) freigegeben werden, solange das VLAN der vSphere-Verwaltungsportgruppe nicht von Produktions-VMs verwendet wird. Stellen Sie sicher, dass das Netzwerksegment nicht geroutet ist. Ausnahmen sind möglicherweise Netzwerke, bei denen andere verwaltungsrelevante Elemente anzutreffen sind, beispielsweise in Verbindung mit vSphere Replication. Stellen Sie insbesondere sicher, dass der Datenverkehr der Produktions-VM nicht auf dieses Netzwerk geroutet werden kann.

Aktivieren Sie den Zugriff auf die Verwaltungsfunktionen streng kontrolliert mit einem der folgenden Ansätze.

- Konfigurieren Sie für besonders vertrauliche Umgebungen ein kontrolliertes Gateway oder eine andere kontrollierte Methode für den Zugriff auf das Verwaltungsnetzwerk. Legen Sie z. B. fest, dass Administratoren sich über ein VPN mit dem Verwaltungsnetzwerk verbinden, und erlauben Sie nur vertrauenswürdigen Administratoren den Zugriff.
- 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. Virtuelle Maschinen können virtuelle Switches und VLANs mit den IP-basierten Speicherkonfigurationen gemeinsam benutzen. Bei diesem Konfigurationstyp kann der IP-basierte Speicherdatenverkehr unautorisierten Benutzern der virtuellen Maschine ausgesetzt sein.

IP-basierter Speicher ist häufig nicht verschlüsselt, und jeder Benutzer mit Zugriff auf das Netzwerk kann ihn 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 virtuellen Maschine 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.

Die vMotion-Portgruppe sollte sich in einem dedizierten VLAN auf einem gemeinsamen vSwitch befinden. Der vSwitch kann für den Produktsdatenverkehr (virtuelle Maschine) freigegeben werden, solange das VLAN der vMotion-Verwaltungsportgruppe nicht von Produktions-VMs verwendet wird.

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 5 Sichern der ESXi-Hosts](#) und [Kapitel 7 Sichern von virtuellen Maschinen](#).

Dieses Kapitel enthält die folgenden Themen:

- [Synchronisieren der Systemuhren im vSphere-Netzwerk](#)
- [Speichersicherheit, empfohlene Vorgehensweisen](#)
- [Überprüfen, ob das Senden von Host-Leistungsdaten 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 der Maschinen im 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 jede Windows-Hostmaschine, auf der eine vCenter-Komponente ausgeführt wird, mit dem NTP-Server synchronisiert wird. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel <http://kb.vmware.com/kb/1318>.

- [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 vSphere 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 vSphere Client und stellen Sie eine Verbindung mit dem ESXi-Host her.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Uhrzeitkonfiguration**.
- 3 Klicken Sie auf **Eigenschaften** und anschließend auf **Optionen**.
- 4 Wählen Sie **NTP-Einstellungen**.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie im Dialogfeld „NTP-Server hinzufügen“ die IP-Adresse oder den vollqualifizierten Domännennamen des NTP-Servers ein, mit dem synchronisiert werden soll.
- 7 Klicken Sie auf **OK**.

Die Hostuhrzeit 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 kommasetrennte 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 kommasetrennte 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 diese Sicherheitsrisiken durch verschiedene Maßnahmen minimieren.

iSCSI ist ein Instrument für den Zugriff auf SCSI-Geräte und zum Austausch von Datensätzen, indem das TCP/IP über einen Netzwerkport und nicht über einen direkten Anschluss an ein SCSI-Gerät eingesetzt wird. In iSCSI-Übertragungen werden Raw-SCSI-Datenblöcke in iSCSI-Datensätze eingekapselt und an das Gerät oder den Benutzer, das/der die Anforderung gestellt hat, übertragen.

iSCSI-SANs ermöglichen die effiziente Verwendung bestehender Ethernet-Infrastrukturen zum Zugriff auf Speicherressourcen durch Hosts, die diese Ressourcen dynamisch teilen können. Deshalb bieten iSCSI-SANs eine wirtschaftliche Speicherlösung für Umgebungen, die auf einem gemeinsamen Speicherpool für verschiedene Benutzer basieren. 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 Sie für Hosts und für iSCSI verwenden, die direkt über den Host konfiguriert werden.

Schützen von iSCSI-Geräten

iSCSI-Geräte können gegen ungewollten Zugriff abgesichert werden, indem der Host, der „Initiator“, vom iSCSI-Gerät, dem „Ziel“, authentifiziert werden muss, wenn der Host versucht, auf Daten in der Ziel-LUN zuzugreifen.

Ziel der Authentifizierung ist es zu überprüfen, dass der Initiator das Recht hat, auf ein Ziel zuzugreifen. Dieses Recht wird bei der Konfiguration der Authentifizierung gewährt.

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. Das Geheimnis der beiderseitigen Authentifizierung muss für jeden Host anders lauten; nach Möglichkeit sollte das Geheimnis für jeden Client, der sich beim Server authentifiziert, ebenfalls anders lauten. Damit wird sichergestellt, dass wenn ein Einzelhost manipuliert wird, ein Angreifer nicht einen beliebigen anderen Host erstellen und sich beim Speichergerät authentifizieren kann. Mit einem einzelnen gemeinsamen geheimen Schlüssel kann ein Angreifer mit der Manipulierung eines Hosts sich 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-Anmeldedaten für NFS 4.1

Mit NFS-Version 4.1 unterstützt ESXi den Kerberos-Authentifizierungsmechanismus.

Kerberos ist ein Authentifizierungsdienst, mit dem ein auf ESXi installierter NFS 4.1-Client vor dem Mounten einer NFS-Freigabe bei einem NFS-Server seine Identität nachweisen kann. Kerberos verwendet Kryptographie bei der Arbeit über eine ungesicherte Netzwerkverbindung. Die vSphere-Implementierung von Kerberos für NFS 4.1 unterstützt nur die Identitätsprüfung für den Client und den Server, stellt aber keine Datenintegrität oder Vertraulichkeitsdienste bereit.

Wenn Sie die Kerberos-Authentifizierung verwenden, ist Folgendes zu beachten:

- ESXi verwendet die Kerberos-Version 5 mit Active Directory-Domäne und KD-Center.
- 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 denselben NFS 4.1-Datenspeicher nutzen, müssen Sie dieselben Active Directory-Anmeldedaten für alle Hosts verwenden, die auf den gemeinsam genutzten Datenspeicher zugreifen. Sie können dies durch Festlegen des Benutzers in Hostprofilen und Anwenden des Profils auf alle ESXi-Hosts automatisieren.
- NFS 4.1 unterstützt nicht gleichzeitige AUTH_SYS- und Kerberos-Mounts.
- NFS 4.1 mit Kerberos bietet keine Unterstützung für IPv6. Nur IPv4 wird unterstützt.

Überprüfen, ob das Senden von Host-Leistungsdaten 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.

Die Fähigkeit, Host-Leistungsdaten an eine virtuelle Gastmaschine zu senden, ist standardmäßig deaktiviert. Durch diese Standardeinstellung wird verhindert, dass eine virtuelle Maschine detaillierte Informationen über den physischen Host erhält, und Hostdaten sind im Falle eines Sicherheitsverstoßes im Zusammenhang mit der virtuellen Maschine nicht verfügbar.

Hinweis Die grundlegende Vorgehensweise wird im Folgenden beschrieben. Verwenden Sie vSphere oder eine der vSphere-Befehlszeilenschnittstellen (vCLI, PowerCLI usw.), um diese Aufgabe stattdessen 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 Sie sich das nächste Mal bei der ESXi Shell anmelden. Sie gelten nicht für aktuelle Sitzungen.

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-Neukonfigurationsprogramm

10

Mit dem TLS-Neukonfigurationsprogramm können Sie TLS-Protokollversionen aktivieren oder deaktivieren. Sie können TLS 1.0 in der vSphere-Umgebung deaktivieren, oder Sie können sowohl TLS 1.0 als auch TLS 1.1 deaktivieren. Ab vSphere 6.5 sind die TLS-Protokollversionen 1.0, 1.1 und 1.2 standardmäßig aktiviert.

Für die Neukonfiguration müssen auf vCenter Server, Platform Services Controller, vSphere Update Manager und ESXi-Hosts in der Umgebung die Softwareversionen ausgeführt werden, die die Deaktivierung erlauben. Im VMware Knowledgebase-Artikel [2145796](#) finden Sie eine Aufstellung der VMware-Produkte, die die Deaktivierung von TLS 1.0 unterstützen.

Bevor Sie TLS 1.0 deaktivieren, müssen Sie auch sicherstellen, dass andere VMware-Produkte und Drittanbieterprodukte ein aktiviertes TLS-Protokoll unterstützen. In Abhängigkeit von Ihrer Konfiguration kann es sich dabei um TLS 1.2 oder sowohl TLS 1.1 als auch TLS 1.2 handeln.

Dieses Kapitel enthält die folgenden Themen:

- [Ports, die die Deaktivierung von TLS-Versionen unterstützen](#)
- [Deaktivieren von TLS-Versionen in vSphere](#)
- [Installieren des TLS-Konfigurationsprogramms](#)
- [Durchführen einer optionalen manuellen Sicherung](#)
- [Deaktivieren von TLS-Versionen auf vCenter Server-Systemen](#)
- [Deaktivieren von TLS-Versionen auf ESXi-Hosts](#)
- [Deaktivieren von TLS-Versionen auf Platform Services Controller-Systemen](#)
- [Zurücksetzen von TLS-Konfigurationsänderungen](#)
- [Deaktivieren von TLS-Versionen in vSphere Update Manager](#)

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.

In der folgenden Tabelle sind die Ports aufgelistet. Wenn ein Port nicht enthalten ist, hat das Dienstprogramm keine Auswirkungen auf diesen Port.

Tabelle 10-1. Vom TLS-Konfigurationsprogramm betroffene vCenter Server und Platform Services Controller

Dienst	Name unter Windows	Name unter Linux	Port
VMware HTTP Reverse Proxy	rhttpproxy	vmware-rhttpproxy	443
VMware Directory Service	VMWareDirectoryService	vmldird	636
VMware Syslog Collector (*)	vmwaresyslogcollector (*)	rsyslogd	1514
vSphere Auto Deploy Waiter	vmware-autodeploy-waiter	vmware-rbd-watchdog	6501 6502
VMware Secure Token Service	VMwareSTS	vmware-stsd	7444
vSphere Update Manager-Dienst (**)	vmware-ufad-vci (**)	vmware-updatemgr	8084 9087
vSphere Web Client	vspherewebclientsvc	vsphere-client	9443
VMware Directory Service	VMWareDirectoryService	vmldird	11712

(*) TLS wird durch die Liste der Schlüssel für diese Dienste gesteuert. Eine detaillierte Verwaltung ist nicht möglich. Nur TLS 1.2 oder alle TLS 1.x-Versionen werden unterstützt.

(*) 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](#).

Tabelle 10-2. Vom TLS-Konfigurationsprogramm betroffene ESXi-Ports

Dienst	Dienstname	Port
VMware HTTP Reverse Proxy und Hostdaemon	Hostd	443
VMware vSAN-VASA-Anbieter-Provider	vSANVP	8080
VMware-Fehlerdomänen-Manager	FDM	8182
VMware vSphere API für E/A-Filter	ioFilterVPsServer	9080
VMware-Autorisierungsdaemon	vmware-authd	902

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 nicht 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	<ol style="list-style-type: none"> Melden Sie sich als Benutzer mit Administratorrechten an. Kopieren Sie die Datei <code>VMware-vSphereTlsReconfigurator-version-build_number.x86_64.msi</code>, die Sie soeben heruntergeladen haben. Installieren Sie die MSI-Datei.
Linux	<ol style="list-style-type: none"> Stellen Sie mithilfe von SSH eine Verbindung mit der Appliance her und melden Sie sich als Benutzer mit Berechtigungen zum Ausführen von Skripten an. Kopieren Sie die Datei <code>VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm</code> mithilfe eines SCP-Clients in die Appliance. Wenn die Bash-Shell derzeit nicht aktiviert ist, führen Sie die folgenden Befehle aus. <pre>shell.set --enabled true shell</pre> Wechseln Sie in das Verzeichnis, in dem sich die hochgeladene RPM-Datei befindet, und führen Sie den folgenden Befehl aus. <pre>rpm -Uvh VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm</pre>

Ergebnisse

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

Betriebssystem	Speicherort
Windows	<ul style="list-style-type: none"> ■ <code>C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\VcTlsReconfigurator</code> ■ <code>C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\EsxTlsReconfigurator</code>
Linux	<ul style="list-style-type: none"> ■ <code>/usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</code> ■ <code>/usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator</code>

Durchführen einer optionalen manuellen Sicherung

Das TLS-Konfigurationsprogramm führt jedes Mal eine Sicherung durch, wenn das Skript vCenter Server, Platform Services Controller oder vSphere Update Manager ändert. Wenn Sie eine Sicherung für ein bestimmtes Verzeichnis benötigen, können Sie eine manuelle Sicherung durchführen.

Das Standardverzeichnis ist für Windows und die Appliance unterschiedlich.

Betriebssystem	Sicherungsverzeichnis
Windows	c:\users\current_user\appdata\local\temp\yearmonthdayTtime
Linux	/tmp/yearmonthdayTtime

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	<i>directory_path</i> \VcTlsReconfigurator> reconfigureVc backup -d <i>backup_directory_path</i>
Linux	<i>directory_path</i> /VcTlsReconfigurator> ./ reconfigureVc backup -d <i>backup_directory_path</i>

- 3 Stellen Sie sicher, dass die Sicherungskopie erfolgreich erstellt wurde.

Eine erfolgreiche Sicherung ähnelt derjenigen im folgenden Beispiel.

```
vCenter Transport Layer Security reconfigurator, version=6.0.0, build=8482376
For more information, refer to the following article: https://kb.vmware.com/kb/2148819
Log file: "C:\ProgramData\VMware\vCenterServer\logs\vmware\vSphere-
TlsReconfigurator\VcTlsReconfigurator.log".
===== Backing up vCenter Server TLS configuration =====
Using backup directory: c:\users\admini~1\appdata\local\temp\1\20170202T054311
Backing up: vmsyslogcollector
Backing up: vspherewebclientsvc
Backing up: vmware-autodeploy-waiter
Backing up: rhttpproxy
Backing up: VMwareSTS
Backing up: VMWareDirectoryService
```

- 4 (Optional) Wenn Sie später eine Wiederherstellung durchführen müssen, 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	<code>cd C:\Programme\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vsphereTlsReconfigurator/VcTlsReconfigurator</code>

- 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	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2</code>
Linux	<code>directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>

- 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	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2</code>

- 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.

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.

Verfahren

- 1 Melden Sie sich beim vCenter Server-Host als Benutzer an, der Skripts ausführen kann, und navigieren Sie zu dem Verzeichnis, in dem sich das Skript befindet.

Betriebssystem	Befehl
Windows	<code>C:\Program Files\VMware\CIS\vSphereTLSReconfigurator\EsxTlsReconfigurator</code>
Linux	<code>/usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator</code>

- 2 Um TLS auf allen Hosts in einem Cluster zu deaktivieren, führen Sie 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	<code>reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- 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	<code>reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2</code>

- 3 Um TLS zu deaktivieren, 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	<code>reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- 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	<code>reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.2</code>

- 4 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	<code>cd C:\Programme\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</code>

- 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	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>

- 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	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2</code>

- 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. Das Zurücksetzen von Änderungen wird für ESXi-Hosts nicht unterstützt.

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	<ol style="list-style-type: none"> 1 Melden Sie sich als Benutzer mit Administratorrechten an. 2 Wechseln Sie zum Verzeichnis VcTlsReconfigurator. <pre>cd C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\VcTlsReconfigurator</pre>
Linux	<ol style="list-style-type: none"> 1 Stellen Sie mithilfe von SSH eine Verbindung mit der Appliance her und melden Sie sich als Benutzer mit Berechtigungen zum Ausführen von Skripten an. 2 Wenn die Bash-Shell derzeit nicht aktiviert ist, führen Sie die folgenden Befehle aus. <pre>shell.set --enabled true shell</pre> 3 Wechseln Sie zum Verzeichnis VcTlsReconfigurator. <pre>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</pre>

3 Prüfen Sie die vorherige Sicherung.

Betriebssystem	Prozedur
Windows	<pre>C:\ProgramData\VMware\vCenterServer\logs\vSphere- TlsReconfigurator\VcTlsReconfigurator.log</pre> <p>Die Ausgabe ähnelt derjenigen im folgenden Beispiel.</p> <pre>c:\users\username\appdata\local\temp\20161108T161539 c:\users\username\appdata\local\temp\20161108T171539</pre>
Linux	<pre>grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/ VcTlsReconfigurator.log</pre> <p>Die Ausgabe ähnelt derjenigen im folgenden Beispiel.</p> <pre>2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920 2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259</pre>

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

Betriebssystem	Prozedur
Windows	<pre>reconfigureVc restore -d <i>Directory_path_from_previous_step</i></pre> <p>Beispiel:</p> <pre>reconfigureVc restore -d c:\users\username\AppData\Local\temp\20161108T171539</pre>
Linux	<pre>reconfigureVc restore -d <i>Directory_path_from_previous_step</i></pre> <p>Beispiel:</p> <pre>reconfigureVc restore -d /tmp/20161117T172920</pre>

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

- 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. In den Tabellen in diesem Anhang steht VC für vCenter Server und HC für Hostclient, einen eigenständigen ESXi- oder Workstation-Host.

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:

- [Alarmrechte](#)
- [Rechte für Auto Deploy und Image-Profile](#)
- [Zertifikatsrechte](#)
- [Rechte für Inhaltsbibliotheken](#)
- [Rechte für Datencenter](#)
- [Berechtigungen für Datenspeicher](#)
- [Rechte für Datenspeichercluster](#)
- [Rechte für Distributed Switches](#)
- [ESX Agent Manager-Rechte](#)
- [Rechte für Erweiterungen](#)
- [Rechte für Ordner](#)
- [Globale Rechte](#)
- [Host-CIM-Rechte](#)

- Rechte für die Hostkonfiguration
- Hostbestandsliste
- Rechte für lokale Hostoperationen
- vSphere Replication-Rechte von Hosts
- Hostprofil-Berechtigungen
- Rechte für Inventory Service-Anbieter
- Rechte für die Inventory Service-Kennzeichnung
- Netzwerkberechtigungen
- Leistungsrechte
- Rechte für Berechtigungen
- Profilgesteuerte Speicherrechte
- Rechte für Ressourcen
- Rechte für geplante Aufgaben
- Sitzungsrechte
- Speicheransichtsberechtigungen
- Rechte für Aufgaben
- Transfer Service-Rechte
- VRM-Richtlinienberechtigungen
- 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

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 Ordnebene 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 *Installations- und Einrichtungshandbuch für vSphere*.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnersebene 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

Tabelle 11-2. Auto Deploy-Rechte (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
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. Weitere Informationen zur Zertifikatsverwaltung von vCenter Server finden Sie unter [Erforderliche Rechte für Zertifikatsverwaltungsvorgänge](#).

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnebene 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

Rechtsname	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 Ordnebene 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

Rechtsname	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 abonniertter 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
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, weil ein Import aus einer Speicher-URL Import von Inhalt impliziert. Aktivieren Sie dieses Recht nur, wenn es notwendig ist und keine Sicherheitsbedenken für den Benutzer, der den Import ausführt, existieren.	Bibliothek

Tabelle 11-4. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Inhaltsbibliothek.Abonnementinformationen prüfen	Mit diesem Recht können Lösungsbenutzer und APIs die Abonnementinformationen einer Remote-Bibliothek einschließlich URL, SSL-Zertifikat und Kennwort untersuchen. Die resultierende Struktur beschreibt, ob die Abonnementkonfiguration erfolgreich ist oder ob Probleme wie beispielsweise SSL-Fehler vorliegen.	Bibliothek
Inhaltsbibliothek.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.Typeninspektion	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
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 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 Ordner Ebene 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 Datencenter

Rechtename	Beschreibung	Erforderlich bei
Datencenter.Datencenter erstellen	Ermöglicht das Erstellen eines neuen Datencenters.	Datencenterordner oder Stammobjekt
Datencenter.Datencenter verschieben	Ermöglicht das Verschieben eines Datencenters. Das Recht muss für Quelle und Ziel vorhanden sein.	Datencenter, Quelle und Ziel
Datencenter.Konfiguration des Netzwerkprotokollprofils	Ermöglicht die Konfiguration des Netzwerkprofils für ein Datencenter.	Datencenter
Datencenter.IP-Pool-Zuteilung abfragen	Ermöglicht die Konfiguration eines Pools von IP-Adressen.	Datencenter
Datencenter.Datencenter neu konfigurieren	Ermöglicht die Neukonfiguration eines Datencenters.	Datencenter
Datencenter.IP-Zuteilung freigeben	Ermöglicht die Freigabe der zugewiesenen IP-Zuteilung für ein Datencenter.	Datencenter
Datencenter.Datencenter entfernen	Ermöglicht das Entfernen eines Datencenters. 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 Ordnebene 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. Berechtigungen für Datenspeicher

Rechtsname	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 ausgeführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Datenspeicher
Datenspeicher.Datei entfernen	Ermöglicht das Löschen von Dateien im Datenspeicher. Dieses Recht ist veraltet. Weisen Sie das Recht Dateivorgänge auf niedriger Ebene zu.	Datenspeicher
Datenspeicher.Datenspeicher umbenennen	Ermöglicht das Umbenennen eines Datenspeichers.	Datenspeicher
Datenspeicher.Dateien der virtuellen Maschine aktualisieren	Ermöglicht das Aktualisieren der Dateipfade der VM-Dateien auf einem Datenspeicher, nachdem der Datenspeicher neu signiert wurde.	Datenspeicher
Datenspeicher.Metadaten der virtuellen Maschine aktualisieren	Ermöglicht das Aktualisieren von Metadaten der virtuellen Maschine für einen Datenspeicher.	Datenspeicher

Rechte für Datenspeichercluster

Datenspeicher-Clusterrechte steuern die Konfiguration des Datenspeicher-Clusters für Speicher-DRS.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordner Ebene 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. Rechte für Datenspeichercluster

Rechtsname	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 Ordner Ebene 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 vSphere Distributed Switch

Rechtsname	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 ausgeführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Distributed Switches
Distributed Switch.Hostvorgang	Ermöglicht das Ändern der Hostmitglieder eines Distributed Switch.	Distributed Switches
Distributed Switch.Ändern	Ermöglicht das Ändern der Konfiguration eines Distributed Switch.	Distributed Switches
Distributed Switch.Verschieben	Ermöglicht das Verschieben eines vSphere Distributed Switch in einen anderen Ordner.	Distributed Switches
Distributed Switch.Network I/O Control-Vorgang	Ermöglicht das Ändern der Ressourceneinstellungen für einen vSphere Distributed Switch.	Distributed Switches
Distributed Switch.Richtlinienvorgang	Ermöglicht das Ändern der Richtlinie eines vSphere Distributed Switch.	Distributed Switches
Distributed Switch.Portkonfigurationsvorgang	Ermöglicht das Ändern der Konfiguration eines Ports in einem vSphere Distributed Switch.	Distributed Switches

Tabelle 11-8. Rechte für vSphere Distributed Switch (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
Distributed Switch.Porteneinstellungsvorgang	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 virtuellen 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 Ordnersebene 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. ESX Agent Manager

Rechtsname	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 Ordnersebene 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. 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 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 Ordnersebene 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 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 ausgeführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Ordner
Ordner.Ordner verschieben	Ermöglicht das Verschieben eines Ordners. Das Recht muss für Quelle und Ziel vorhanden sein.	Ordner
Ordner.Ordner umbenennen	Ermöglicht das Ändern des Namens eines Ordners.	Ordner

Globale Rechte

Globale Rechte steuern globale Aufgaben im Zusammenhang mit Aufgaben, Skripts und Erweiterungen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnersebene 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. 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.Gesundheit	Ermöglicht das Anzeigen des Status der vCenter Server-Komponenten.	Root-vCenter Server
Global.Lizenzen	Ermöglicht das Anzeigen installierter Lizenzen und das Hinzufügen bzw. Entfernen von Lizenzen.	Root-Host oder vCenter Server
Global.Ereignis protokollieren	Ermöglicht das Protokollieren eines benutzerdefinierten Ereignisses für ein bestimmtes verwaltetes Element.	Beliebiges Objekt
Global.Benutzerdefinierte Attribute verwalten	Ermöglicht das Hinzufügen, Entfernen oder Umbenennen von benutzerdefinierten Felddefinitionen.	Root-vCenter Server
Global.Proxy	Ermöglicht Zugriff auf eine interne Schnittstelle für das Hinzufügen oder Entfernen von Endpunkten zu oder vom Proxy.	Root-vCenter Server
Global.Skriptaktion	Ermöglicht das Planen einer Skriptaktion in Zusammenhang mit einem Alarm.	Beliebiges Objekt
Global.Dienst-Manager	Ermöglicht die Verwendung des <code>resxtop</code> -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

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 Ordner Ebene 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. Host-CIM-Rechte

Rechtsname	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 Ordner Ebene 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. Rechte für die Hostkonfiguration

Rechtsname	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

Tabelle 11-14. Rechte für die Hostkonfiguration (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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.Arbeitspeicherkonfiguration	Ermöglicht Änderungen an der Hostkonfiguration.	Hosts
Host.Konfiguration.Netzwerkkonfiguration	Ermöglicht das Konfigurieren von Netzwerk, Firewall und vMotion-Netzwerk.	Hosts
Host.Konfiguration.Betrieb	Ermöglicht das Konfigurieren der Energieverwaltungseinstellungen des Hosts.	Hosts
Host.Konfiguration.Patch abfragen	Ermöglicht das Abfragen installierbarer Patches und das Installieren von Patches auf dem Host.	Hosts
Host.Konfiguration.Sicherheitsprofil und Firewall	Ermöglicht das Konfigurieren von Internetdiensten wie SSH, Telnet, SNMP und Hostfirewall.	Hosts
Host.Konfiguration.Konfiguration für Speicherpartition	Ermöglicht das Verwalten der VMFS-Datenspeicher und Diagnosepartitionen. Benutzer mit diesem Recht können nach neuen Speichergeräten suchen und iSCSI verwalten.	Hosts
Host.Konfiguration.System-Management	Ermöglicht Erweiterungen eine Änderung des Dateisystems auf dem Host.	Hosts
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 Ordner Ebene 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 Hostbestandsliste

Rechtename	Beschreibung	Erforderlich bei
Host.Bestandsliste.Host zu Cluster hinzufügen	Ermöglicht das Hinzufügen eines Hosts zu einem vorhandenen Cluster.	Cluster
Host.Bestandsliste.Eigenständigen Host hinzufügen	Ermöglicht das Hinzufügen eines eigenständigen Hosts.	Hostordner
Host.Bestandsliste.Cluster erstellen	Ermöglicht das Erstellen eines neuen Clusters.	Hostordner
Host.Bestandsliste.Cluster ändern	Ermöglicht das Ändern der Eigenschaften eines Clusters.	Cluster
Host.Bestandsliste.Cluster oder eigenständigen Host verschieben	Ermöglicht das Verschieben eines Clusters oder eigenständigen Hosts zwischen Ordnern. Das Recht muss für Quelle und Ziel vorhanden sein.	Cluster
Host.Bestandsliste.Host verschieben	Ermöglicht das Verschieben einer Gruppe vorhandener Hosts in einen oder aus einem Cluster. Das Recht muss für Quelle und Ziel vorhanden sein.	Cluster
Host.Bestandsliste.Cluster entfernen	Ermöglicht das Löschen eines Clusters oder eines eigenständigen Hosts. Dieser Vorgang kann nur ausgeführt 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 ausgeführt 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 vSphere-Client und einem Host durchgeführt werden.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordner Ebene 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 lokale Hostoperationen

Rechtsname	Beschreibung	Erforderlich bei
Host.Lokale Operationen.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 Operationen.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 Operationen.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.NVRAM-Inhalt extrahieren	Ermöglicht die Extraktion des NVRAM-Inhalts eines Hosts.	
Host.Lokale Operationen.Benutzergruppen verwalten	Ermöglicht die Verwaltung lokaler Konten auf einem Host.	Root-Host
Host.Lokale Operationen.Virtuelle Maschine neu konfigurieren	Ermöglicht die erneute Konfiguration einer virtuellen Maschine.	Root-Host
Host.Lokale Operationen.Snapshots neu entwerfen	Ermöglicht Änderungen am Layout der Snapshots 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 Ordnebene 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. vSphere Replication-Rechte von Hosts

Rechtsname	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 Ordnersebene 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. Hostprofil-Berechtigungen

Rechtsname	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

Rechte für Inventory Service-Anbieter

Rechte für Inventory Service-Anbieter werden nur intern verwendet. Nicht verwenden.

Rechte für die Inventory Service-Kennzeichnung

Die Rechte für die Inventory Service-Kennzeichnung bestimmen, ob Tags und Tag-Kategorien erstellt und gelöscht sowie ob Tags in vSphere-Bestandslistenobjekten zugewiesen und entfernt werden können.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnersebene 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. vCenter Inventory Service-Rechte

Rechtsname	Beschreibung	Erforderlich bei
Inventory Service.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-Bestandsliste.	Beliebiges Objekt
Inventory Service.vSphere-Tagging.vSphere-Tag erstellen	Ermöglicht das Erstellen eines Tags.	Beliebiges Objekt
Inventory Service.vSphere-Tagging.vSphere-Tag-Kategorie erstellen	Ermöglicht das Erstellen einer Tag-Kategorie.	Beliebiges Objekt

Tabelle 11-19. vCenter Inventory Service-Rechte (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
Inventory Service.vSphere-Tagging.vSphere-Tag-Geltungsbereich erstellen	Ermöglicht das Erstellen eines Tag-Bereichs.	Beliebiges Objekt
Inventory Service.vSphere-Tagging.vSphere-Tag löschen	Ermöglicht das Löschen einer Tag-Kategorie.	Beliebiges Objekt
Inventory Service.vSphere-Tagging.vSphere-Tag-Kategorie löschen	Ermöglicht das Löschen einer Tag-Kategorie.	Beliebiges Objekt
Inventory Service.vSphere-Tagging.vSphere-Tag-Umfang löschen	Ermöglicht das Löschen eines Tag-Bereichs.	Beliebiges Objekt
Inventory Service.vSphere-Tagging.vSphere-Tag Bearbeiten	Ermöglicht das Bearbeiten eines Tags.	Beliebiges Objekt
Inventory Service.vSphere-Tagging.vSphere-Tag-Kategorie bearbeiten	Ermöglicht das Bearbeiten einer Tag-Kategorie.	Beliebiges Objekt
Inventory Service.vSphere-Tagging.vSphere-Tag-Geltungsbereich bearbeiten	Ermöglicht das Bearbeiten eines Tag-Bereichs.	Beliebiges Objekt
Inventory Service.vSphere-Tagging.Feld „Verwendet von“ für Kategorie ändern	Ermöglicht das Ändern des UsedBy-Felds für eine Tag-Kategorie.	Beliebiges Objekt
Inventory Service.vSphere-Tagging.Feld „Verwendet von“ für Tag ändern	Ermöglicht das Ändern des UsedBy-Felds für ein Tag.	Beliebiges Objekt

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 Ordner Ebene 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

Rechtsname	Beschreibung	Erforderlich bei
Netzwerk.Netzwerk zuweisen	Ermöglicht das Zuweisen eines Netzwerks zu einer virtuellen Maschine.	Netzwerke, virtuelle Maschinen
Netzwerk.Konfigurieren	Ermöglicht das Konfigurieren eines Netzwerks.	Netzwerke, virtuelle Maschinen

Tabelle 11-20. Netzwerkberechtigungen (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
Netzwerk.Netzwerk verschieben	Ermöglicht das Verschieben eines Netzwerks zwischen Ordnern. Das Recht muss für Quelle und Ziel vorhanden sein.	Netzwerke
Netzwerk.Entfernen	Ermöglicht das Entfernen eines Netzwerks. Dieses Recht ist veraltet. Dieser Vorgang kann nur ausgeführt 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 Ordner Ebene 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

Rechtsname	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 Ordner Ebene 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 ausgeführt 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.Berechtigung 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 Ordner Ebene 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 Ordnebene 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 zu Ressourcenpool zuweisen	Ermöglicht die Zuweisung einer vApp zu einem Ressourcenpool.	Ressourcenpools
Ressourcen.Virtuelle Maschine zu Ressourcenpool zuweisen	Ermöglicht die Zuweisung einer virtuellen Maschine zu einem Ressourcenpool.	Ressourcenpools
Ressourcen.Ressourcenpool erstellen	Ermöglicht die Erstellung von Ressourcenpools.	Ressourcenpools, Cluster
Ressourcen.Ausgeschaltete virtuelle Maschine migrieren	Ermöglicht die Migration einer ausgeschalteten virtuellen Maschine auf einen anderen Ressourcenpool oder Host.	virtuelle Maschinen
Ressourcen.Eingeschaltete virtuelle Maschine migrieren	Ermöglicht die Migration mithilfe von vMotion einer eingeschalteten virtuellen Maschine auf einen anderen Ressourcenpool oder Host.	
Ressourcen.Ressourcenpool ändern	Ermöglicht Änderungen an den Zuweisungen eines Ressourcenpools.	Ressourcenpools
Ressourcen.Ressourcenpool verschieben	Ermöglicht das Verschieben eines Ressourcenpools. Das Recht muss für Quelle und Ziel vorhanden sein.	Ressourcenpools
Ressourcen.vMotion abfragen	Ermöglicht die Abfrage der allgemeinen vMotion-Kompatibilität einer virtuellen Maschine mit einer Hostgruppe.	Root-vCenter Server
Ressourcen.Ressourcenpool entfernen	Ermöglicht das Löschen eines Ressourcenpools. Dieser Vorgang kann nur ausgeführt 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 Ordnebene 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

Rechtsname	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 Ordnebene 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

Rechtsname	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

Speicheransichtsberechtigungen

Speicheransichtsberechtigungen bestimmen die Rechte für Speicherüberwachungsdienst-APIs.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 11-27. Speicheransichtsberechtigungen

Rechtsname	Beschreibung	Erforderlich bei
Speicheransichten.Dienst konfigurieren	Erlaubt berechtigten Benutzern die Verwendung aller Speicherüberwachungsdienst-APIs. Verwenden Sie Speicheransichten.Anzeigen für schreibgeschützte Rechte für Speicherüberwachungsdienst-APIs.	Root-vCenter Server
Speicheransichten.Anzeigen	Erlaubt berechtigten Benutzern die Verwendung schreibgeschützter Speicherüberwachungsdienst-APIs.	Root-vCenter Server

Rechte für Aufgaben

Rechte für Aufgaben steuern die Fähigkeit von Erweiterungen, Aufgaben für vCenter Server zu erstellen und zu aktualisieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 11-28. Rechte für Aufgaben

Rechtsname	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.

VRM-Richtlinienberechtigungen

VRM-Richtlinienrechte 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 Ordner Ebene 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

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

Rechtename	Beschreibung	Erforderlich bei
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
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

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

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Konfiguration. Umbenennen	Ermöglicht das Umbenennen einer virtuellen Maschine oder das Ändern zugeordneter Anmerkungen für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration. Gastinformationen zurücksetzen	Ermöglicht das Bearbeiten der Gastbetriebssystem-Informationen für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration. Anmerkung festlegen	Ermöglicht das Hinzufügen oder Bearbeiten einer Anmerkung für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration. 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. Virtuelle Maschine entsperren	Ermöglicht das Entschlüsseln einer virtuellen Maschine.	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 Ordnebene 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.Gastvorgänge. Aliasspeicher im Gast ändern	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die das Ändern des Alias für die virtuelle Maschine beinhalten.	virtuelle Maschinen
Virtuelle Maschine.Gastvorgänge. Aliasspeicher im Gast abfragen	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die das Abfragen des Alias für die virtuelle Maschine beinhalten.	virtuelle Maschinen
Virtuelle Maschine.Gastvorgänge. 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 Benutzerschnittstellenelemente auf dem vSphere Web Client zugeordnet.	virtuelle Maschinen
Virtuelle Maschine.Gastvorgänge. Programmausführung im Gastbetriebssystem	Ermöglicht Gastvorgänge auf virtuelle Maschinen, die das Ausführen eines Programms in der virtuellen Maschine einschließen. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Web Client zugeordnet.	virtuelle Maschinen
Virtuelle Maschine.Gastvorgänge. Gastvorgangsabfragen	Ermöglicht Gastvorgänge auf virtuelle Maschinen, die Abfragen des Gastbetriebssystems einschließen, wie z. B. das Auflisten von Dateien im Gastbetriebssystem. Diesem Recht sind keine Benutzerschnittstellenelemente 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 Ordner Ebene 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

Rechtsname	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

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
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

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
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

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
Virtuelle Maschine.Interaktion.Geräteverbindung	Ermöglicht die Änderung des Verbindungsstatus der virtuellen Geräte einer virtuellen Maschine, die getrennt werden können.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Fault Tolerance deaktivieren	Ermöglicht die Deaktivierung der sekundären virtuellen Maschine für eine virtuelle Maschine mit Fault Tolerance.	virtuelle Maschinen

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
Virtuelle Maschine.Interaktion.Drag & Drop	Ermöglicht das Ziehen und Ablegen von Dateien zwischen einer virtuellen Maschine und einem Remoteclient.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Fault Tolerance aktivieren	Ermöglicht die Aktivierung der sekundären virtuellen Maschine für eine virtuelle Maschine mit Fault Tolerance.	virtuelle Maschinen

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Interaktion.Verwaltung des Gastbetriebssystems durch VIX API	Ermöglicht die Verwaltung des Betriebssystems der virtuellen Maschinen 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/Wiederaufnehmen	Ermöglicht das Anhalten oder Fortsetzen der virtuellen Maschinen.	virtuelle Maschinen

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
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

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
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
Virtuelle Maschine.Interaktion.Fault Tolerance fortsetzen	Ermöglicht die Fortsetzung von Fault Tolerance für eine virtuelle Maschine.	virtuelle Maschinen

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
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

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtsname	Beschreibung	Erforderlich bei
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

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtsname	Beschreibung Erforderlich bei
Virtuelle Maschine.Interaktion.Fault Tolerance ausschalten	Ermöglicht die Deaktivierung von Fault Tolerance für eine virtuelle Maschine.

Tabelle 11-31. Interaktion virtueller Maschinen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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 Ordner Ebene 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

Rechtsname	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 ausgeführt 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 ausgeführt 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 virtuellen Maschinen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordner Ebene 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.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
Virtuelle Maschine.Bereitstellung.Anpassungsspezifikation ändern	Ermöglicht das Erstellen, Ändern oder Löschen von Anpassungsspezifikationen.	Root-vCenter Server

Tabelle 11-33. Rechte für das Bereitstellen virtueller Maschinen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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 Ordner Ebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis In vSphere 6.0 sollten Sie dieses Recht nicht mit dem vSphere Web Client zuweisen oder entfernen.

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.Polling 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.
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 Ordnebene 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

Rechtsname	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 Ordnebene 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 Ordner Ebene 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 ausgeführt 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
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 Ordner Ebene 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 ausgeführt 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
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 ausgeführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	vApps

Tabelle 11-38. vApp-Rechte (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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 ausgeführt 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 Ordnebene 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