vSphere-Sicherheit

Update 3

VMware vSphere 8.0
VMware ESXi 8.0
vCenter Server 8.0

vmware
by Broadcom

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

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

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

Inhalt

Info zu vSphere Security 15

1 Sicherheit in der vSphere-Umgebung 18
- Absichern des ESXi-Hypervisors 18
- Sichern von vCenter Server-Systemen und zugehörigen Diensten 21
- Sichern von virtuellen Maschinen 22
- Schützen der virtuellen Netzwerkebene 24
- Sichern von Kennwörtern in Ihrer vSphere-Umgebung 26
- Best Practices und Ressourcen für die Sicherheit für vCenter Server und ESXi 27

2 vSphere-Berechtigungen und Benutzerverwaltungsaufgaben 29
- Grundlegende Informationen zur Autorisierung in vSphere 30
  - Hierarchische Vererbung von Berechtigungen in vSphere 34
- Funktionsweise mehrerer Berechtigungseinstellungen in vSphere 37
  - Beispiel 1: Berechtigungsübernahme von mehreren Gruppen 37
  - Beispiel 2: Untergeordnete Berechtigungen, die übergeordnete Berechtigungen außer Kraft setzen 38
  - Beispiel 3: Benutzerrolle, die Gruppenrolle außer Kraft setzt 39
- Verwalten von Berechtigungen für vCenter Server-Komponenten 40
  - Hinzufügen einer Berechtigung zu einem Bestandslistenobjekt 40
  - Ändern oder Entfernen von Berechtigungen für ein Bestandslistenobjekt 41
  - Ändern der Einstellungen für die vCenter Server-Benutzervalidierung 42
- Verwenden globaler vCenter Server-Berechtigungen 43
  - Hinzufügen einer globalen Berechtigung 43
  - vCenter Server-Berechtigungen für Tag-Objekte 44
- Verwenden von vCenter Server-Rollen zum Zuweisen von Rechten 46
  - Erstellen einer benutzerdefinierten vCenter Server-Rolle 49
- Verwenden des Rechte-Recorders 50
  - Aktivieren des Berechtigungs-Recorders 51
- Best Practices für Rollen und Berechtigungen in vCenter Server 52
- Erforderliche vCenter Server-Rechte für allgemeine Aufgaben 53

3 Sichern der ESXi-Hosts 58
- Allgemeine ESXi-Sicherheitsempfehlungen 59
  - ESXi – Erweiterte Systemeinstellungen 61
  - Konfigurieren von ESXi-Hosts mit Hostprofilen 65
  - Verwalten von ESXi-Hostkonfigurationseinstellungen mithilfe von Skripts 66
  - Kennwörter und Kontosperrung für ESXi 67

Erzeugung des kryptografischen Schlüssels in ESXi 70
SSH-Sicherheit in ESXi 72
Hochladen eines SSH-Schlüssels anhand von HTTPS PUT 72
PCI- und PCIe-Geräte sowie ESXi 73
Deaktivieren des vSphere-Browsers für verwaltete Objekte 74
ESXi-Netzwerksicherheitsempfehlungen 75
Ändern von ESXi-Web-Proxy-Einstellungen 75
vSphere Auto Deploy-Sicherheitsüberlegungen 76
Steuern des Zugriffs für CIM-basierte Hardwareüberwachungstools 77
Empfohlene Vorgehensweisen für die Sicherheit von vSphere Distributed Services Engine 78
Steuern der ESXi-Entropie 79
Verwalten von Zertifikaten für ESXi-Hosts 81
ESXi-Host-Upgrades und Zertifikate 84
Moduswechsel-Workflows für Zertifikate in ESXi 85
Standardeinstellungen für ESXi-Zertifikate 87
Ändern der Standardeinstellungen für ESXi-Zertifikate 89
Anzeigen von Informationen zum Ablauf von Zertifikaten für ESXi-Hosts 89
Verlängern oder Aktualisieren von ESXi-Zertifikaten 91
Ändern des ESXi-Zertifikatmodus 93
Ersetzen des ESXi-Standardzertifikats durch ein benutzerdefiniertes Zertifikat 94
Generieren einer Zertifikatssignieranforderung für ein benutzerdefiniertes Zertifikat mithilfe von vSphere Client 96
Ersetzen des Standardzertifikats durch ein benutzerdefiniertes Zertifikat mithilfe des vSphere Client 96
Ersetzen des Standardzertifikats und -schlüssels über die ESXi Shell 98
Ersetzen eines Standardzertifikats mit HTTPS PUT 98
Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS (Benutzerdefinierte Zertifikate) 99
Festlegen von Auto Deploy als untergeordnete Zertifizierungsstelle 100
Verwenden benutzerdefinierter Zertifikate mit Auto Deploy 102
Wiederherstellen der ESXi-Zertifikats- und -Schlüsseldateien, wenn die Zertifikatsersetzung fehlschlägt 107
Anpassen der ESXi-Hostsicherheit 108
Konfigurieren der ESXi Firewall 108
Verwalten von ESXi-Firewalleinstellungen 109
Hinzufügen von zulässigen IP-Adressen für einen ESXi-Host 110
Ein- und ausgehende Firewall-Ports für ESXi-Hosts 111
NFS-Client-Firewallverhalten 111
Verwenden von ESXCLI-Firewall-Befehlen zum Konfigurieren des ESXi-Verhaltens 112
Aktivieren oder Deaktivieren eines ESXi-Diensts 113
Konfigurieren und Verwalten des Sperrmodus auf ESXi-Hosts 116
Verhalten im Sperrmodus 116

Aktivieren des Sperrmodus über den vSphere Client 118
Deaktivieren des Sperrmodus über den vSphere Client 119
Aktivieren oder Deaktivieren des normalen Sperrmodus über die Benutzerschnittstelle der direkten Konsole 119
Angeben von Konten mit Zugriffsrechten im Sperrmodus 120
Durchführen sicherer Updates mithilfe von vSphere-Installationspaketen 122
Verwalten der Akzeptanzebenen von ESXi-Hosts und vSphere-Installationspaketen 123
Zuweisen von Rechten für ESXi-Hosts 126
Verwenden von Active Directory zum Verwalten von ESXi-Benutzern 128
Konfigurieren eines ESXi-Hosts für die Verwendung von Active Directory 129
Hinzufügen eines ESXi-Hosts zu einer Verzeichnisdienst-Domäne 130
Anzeigen der Verzeichnisdiensteinstellungen für einen ESXi-Host 131
Verwenden des vSphere Authentication Proxy 131
Starten des vSphere Authentication Proxy-Diensts 132
Hinzufügen einer Domäne zu vSphere Authentication Proxy mit dem vSphere Client 133
Hinzufügen einer Domäne zu vSphere Authentication Proxy mit dem Befehl „camconfig“ 134
Verwenden des vSphere Authentication Proxy zum Hinzufügen eines Hosts zu einer Domäne 135
Aktivieren von Clientauthentifizierung für vSphere Authentication Proxy 136
Importieren des vSphere Authentication Proxy-Zertifikats in den ESXi-Host 137
Erstellen eines neuen Zertifikats für vSphere Authentication Proxy 137
Einrichten von vSphere Authentication Proxy für die Verwendung von benutzerdefinierten Zertifikaten 138
Konfigurieren und Verwalten der Smartcard-Authentifizierung für ESXi 140
Aktivieren der Smartcard-Authentifizierung 141
Deaktivieren der Smartcard-Authentifizierung 142
Authentifizieren mit Benutzernamen und Kennwort bei Verbindungsproblemen 142
Verwenden der Smartcard-Authentifizierung im Sperrmodus 143
Verwenden der ESXi Shell 143
Festlegen der Zeitüberschreitungswerts für Leerlauf für die ESXi Shell mithilfe des vSphere Client 145
Festlegen eines Zeitüberschreitungswerts für Verfügbarkeit für die ESXi Shell mithilfe des vSphere Client 145
Festlegen von Zeitüberschreitungswerten für Verfügbarkeit oder Leerlauf für die ESXi Shell mithilfe der DCUI 146
Aktivieren des Zugriffs auf ESXi Shell mithilfe des vSphere Client 147
Aktivieren des Zugriffs auf die ESXi Shell mithilfe der DCUI 148
Anmelden bei der ESXi Shell zur Fehlerbehebung 149
UEFI Secure Boot für ESXi-Hosts 149
Ausführen des Secure Boot-Validierungsskripts nach dem ESXi-Upgrade 151
Sichern von ESXi-Hosts mit Trusted Platform Module 152
Überprüfen des Integritätsnachweis-Status eines ESXi-Hosts 154
Beheben von Problemen beim ESXi-Hostnachweis 155

ESXi-Protokolldateien 155
Konfiguration von Syslog auf ESXi-Hosts 156
ESXi-Syslog-Optionen 157
Speicherorte der ESXi-Protokolldateien 163
Sichern des Fault Tolerance-Protokollierungsdatenverkehrs 165
Aktivieren der Fault Tolerance-Verschlüsselung 165
Verwalten von ESXi-Überwachungsdatensätzen 167
Sichern der ESXi-Konfiguration 167
Verwalten einer sicheren ESXi-Konfiguration 171
Auflisten der Inhalte des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration 171
Rotieren des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration 172
Fehlerbehebung und Wiederherstellung der sicheren ESXi-Konfiguration 173
Wiederherstellen der sicheren ESXi-Konfiguration 173
Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration 174
Aktivieren oder Deaktivieren der execInstalledOnly-Erzwingung für eine sichere ESXi-Konfiguration 177
Deaktivieren der internen Laufzeitoption „execInstalledOnly“ 180

4 Sichern von vCenter Server-Systemen 182
Best Practices für die vCenter Server-Zugriffssteuerung 182
Festlegen der vCenter Server-Kennwortrichtlinie 184
Entfernen abgelaufener oder widerrufener Zertifikate und Protokolle fehlgeschlagener Installationen 185
Begrenzen der vCenter Server-Netzwerkkonnektivität 185
Bewerten der Verwendung von Linux-Clients mit CLIs und SDKs 186
Überprüfen von vSphere Client-Plug-Ins 186
Empfohlene Vorgehensweisen für die Sicherheit von vCenter Server 187
Kennwortanforderungen und Sperrverhalten für vCenter 188
Überprüfen der Fingerabdrücke bei Legacy-ESXi-Hosts 189
Erforderliche Ports für vCenter Server 190

5 Sichern von virtuellen Maschinen 191
Aktivieren oder Deaktivieren von UEFI Secure Boot für eine virtuelle Maschine 191
Virtuelle Maschine – Empfohlene Vorgehensweisen für die Sicherheit 193
Allgemeiner Schutz für virtuelle Maschinen 194
Verwendung von Vorlagen zum Bereitstellen von virtuellen Maschinen 195
Beschränken der Verwendung der VM-Konsole auf ein Minimum 195
Verhindern, dass virtuelle Maschinen Ressourcen in Besitz nehmen 196
Deaktivieren unnötiger Funktionen innerhalb von virtuellen Maschinen 197
Entfernen nicht benötigter Hardwaregeräte von virtuellen Maschinen 197
Deaktivieren nicht verwendeter Anzeigefunktionen auf virtuellen Maschinen 198

Deaktivieren von Kopier- und Einfügevorgängen zwischen Gastbetriebssystem und Remotekonsole 199

Begrenzen der Offenlegung sensibler Daten, die in die Zwischenablage der Konsole der virtuellen Maschine kopiert wurden 200

Beschränken der Ausführung von Befehlen durch Benutzer innerhalb einer virtuellen Maschine 200

Verhindern, dass ein Benutzer oder Prozess auf einer virtuellen Maschine die Verbindung zu Geräten trennt 201

Verhindern, dass Gastbetriebssystemprozesse Konfigurationsnachrichten an den Host senden 202

Vermeiden der Verwendung unabhängiger, nicht dauerhafter Festplatten mit virtuellen Maschinen 202

Sichern von virtuellen Maschinen mit Intel Software Guard-Erweiterungen 203

Erste Schritte mit vSGX 204

Aktivieren von vSGX auf einer virtuellen Maschine 205

Aktivieren von vSGX auf einer vorhandenen virtuellen Maschine 206

Entfernen von vSGX von einer virtuellen Maschine 207

Sichern von virtuellen Maschinen mit AMD Secure Encrypted Virtualization-Encrypted State 207

vSphere und AMD-SEV-ES (Secure Encrypted Virtualization-Encrypted State) 208

Hinzufügen von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) zu einer virtuellen Maschine mithilfe des vSphere Client 209

Hinzufügen von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) zu einer virtuellen Maschine mithilfe der Befehlszeile 210

Aktivieren von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer vorhandenen virtuellen Maschine mithilfe des vSphere Client 211

Aktivieren von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer virtuellen Maschine mithilfe der Befehlszeile 213

Deaktivieren von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer virtuellen Maschine mithilfe des vSphere Client 214

Deaktivieren von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer virtuellen Maschine mithilfe der Befehlszeile 214

6 Verschlüsselung virtueller Maschinen 216

Vergleich von vSphere-Schlüsselanbietern 217

Wie vSphere Virtual Machine Encryption Ihre Umgebung schützt 220

vSphere Virtual Machine Encryption-Komponenten 226

Prozessablauf bei der Verschlüsselung 228

Verschlüsseln von virtuellen Festplatten 232

Fehler bei der Verschlüsselung von virtuellen Maschinen 234

Voraussetzungen und erforderliche Berechtigungen für VM-Verschlüsselungsaufgaben 235

Verschlüsseltes vSphere vMotion 237

Virtuelle Maschine – Empfohlene Vorgehensweisen für die Verschlüsselung 241

Vorbehalte bei der Verschlüsselung von virtuellen Maschinen 245

Interoperabilität bei der Verschlüsselung von virtuellen Maschinen 246

vSphere-Schlüsselpersistenz auf ESXi-Hosts 250

7 Konfigurieren und Verwalten eines Standardschlüsselanbieters 252

Definition eines Standardschlüsselanbieters 252

Einrichten des Standardschlüsselanbieters 253

Hinzufügen eines Standardschlüsselanbieters mithilfe des vSphere Client 253

Herstellen einer vertrauenswürdigen Standardschlüsselanbieter-Verbindung durch den Austausch von Zertifikaten 255

Verwenden der Option „Root-CA-Zertifikat“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters 256

Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters 257

Verwenden der Option „Zertifikat und privaten Schlüssel hochladen“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters 258

Verwenden der Option „Neue Zertifikatssignierungsanforderung“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters 259

Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter 260

Einrichten separater Schlüsselanbieter für verschiedene Benutzer 260

Löschen eines Standardschlüsselanbieters 261

8 Konfigurieren und Verwalten eines vSphere Native Key Providers 263

vSphere Native Key Provider – Übersicht 263

vSphere Native Key Provider – Prozessablauf 267

Konfigurieren eines vSphere Native Key Providers 268

Sichern eines vSphere Native Key Providers 269

Wiederherstellen eines vSphere Native Key Providers 271

Wiederherstellen eines vSphere Native Key Providers mithilfe des vSphere Client 271

Aktualisieren eines vSphere Native Key Providers 272

Löschen eines vSphere Native Key Providers 273

9 vSphere Trust Authority 275

vSphere Trust Authority – Konzepte und Funktionen 275

So schützt vSphere Trust Authority Ihre Umgebung 275

Vertrauenswürdige vSphere Trust Authority-Infrastruktur 279

vSphere Trust Authority – Prozessabläufe 282

vSphere Trust Authority – Topologie 286

Voraussetzungen und notwendige Berechtigungen für vSphere Trust Authority 287

vSphere Trust Authority – Best Practices, Einschränkungen und Interoperabilität 290

vSphere Trust Authority – Lebenszyklus 291

Konfigurieren von vSphere Trust Authority 294

Einrichten Ihrer Workstation zum Konfigurieren von vSphere Trust Authority 297

Aktivieren des Trust Authority-Administrators 298

Aktivieren des Trust Authority-Status 299

Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server 301

Exportieren und Importieren eines TPM Endorsement Key-Zertifikats 305
Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster 311
Erstellen des Schlüsselanbieters im Trust Authority-Cluster 314
Hochladen des Clientzertifikats zum Herstellen einer vertrauenswürdigen Verbindung des vertrauenswürdigen Schlüsselanbieters 321
Zertifikat und privaten Schlüssel zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters hochladen 323
Eine Zertifikatssignieranforderung zum Herstellen einer vertrauenswürdigen Schlüsselanbieter-Verbindung erstellen 325
Exportieren der Informationen des Trust Authority-Clusters 327
Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts 329
Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe des vSphere Client 333
Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe der Befehlszeile 334
Verwalten vSphere Trust Authority in Ihrer vSphere-Umgebung 336
Starten, Stoppen und Neustarten von vSphere Trust Authority-Diensten 336
Anzeigen der Trust Authority-Hosts 337
Anzeigen des Status des vSphere Trust Authority-Clusters 337
Neustarten des Diensts für vertrauenswürdige Hosts 338
Hinzufügen und Entfernen von vSphere Trust Authority-Hosts 338
Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mit dem vSphere Client 338
Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mithilfe der Befehlszeile 340
Stilllegen vertrauenswürdiger Hosts in einem vertrauenswürdigen Cluster 341
Sichern der vSphere Trust Authority-Konfiguration 342
Ändern des primären Schlüssels eines vertrauenswürdigen Schlüsselanbieters 343
Nachweisberichte für vertrauenswürdige Hosts 344
Anzeigen des Nachweisstatus des vertrauenswürdigen Clusters 345
Beheben von Problemen beim Nachweis des vertrauenswürdigen Hosts 346
Prüfen und Standardisieren der Integrität eines vertrauenswürdigen Clusters 347
Überprüfen der Integrität des vertrauenswürdigen Clusters 349
Standardisieren eines vertrauenswürdigen Clusters 350

10 Verwenden der Verschlüsselung in Ihrer vSphere-Umgebung 351
Erstellen einer Speicherrichtlinie für die Verschlüsselung. 352
Explizites Aktivieren des Hostverschlüsselungsmodus 353
Deaktivieren des Hostverschlüsselungsmodus mithilfe der API 353
Erstellen einer verschlüsselten virtuellen Maschine 355
Klonen einer verschlüsselten virtuellen Maschine 357
Verschlüsseln einer bestehenden virtuellen Maschine oder virtuellen Festplatte 360
Entschlüsseln einer verschlüsselten virtuellen Maschine oder virtuellen Festplatte 361
Ändern der Verschlüsselungsrichtlinie für virtuelle Festplatten 363

Beheben von Problemen in Bezug auf fehlende Verschlüsselungsschlüssel 364
Entsperren von gesperrten virtuellen Maschinen 366
Beheben von Problemen im Zusammenhang mit dem Verschlüsselungsmodus des ESXi-Hosts 367
Erneutes Aktivieren des ESXi-Hostverschlüsselungsmodus 368
Festlegen des Schwellenwerts für den Ablauf von Schlüsselserverzertifikaten 369
vSphere VM-Verschlüsselung und Core-Dumps 370
Erfassen eines vm-support-Pakets für einen ESXi-Host, auf dem Verschlüsselung verwendet wird 371
Entschlüsseln oder erneutes Verschlüsseln eines verschlüsselten Core-Dump 373
Aktivieren und Deaktivieren von Schlüsselpersistenz auf einem ESXi-Host 374
Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe des vSphere Client 375
Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe der CLI 376
Festlegen des Standardschlüsselanbieters mithilfe des vSphere Client 377
Festlegen des Standardschlüsselanbieters über die Befehlszeile 378

11 Sichern von virtuellen Maschinen mit Virtual Trusted Platform Module 380
Was ist ein Virtual Trusted Platform Module? 380
Erstellen einer virtuellen Maschine mit einem Virtual Trusted Platform Module 382
Hinzufügen des virtuellen Trusted Platform Module zu einer vorhandenen virtuellen Maschine 384
Entfernen eines virtuellen Trusted Platform Module von einer virtuellen Maschine 385
Angeben vTPM-fähiger virtueller Maschinen 386
Anzeigen von Zertifikaten des Virtual Trusted Platform Module-Geräts 386
Exportieren und Ersetzen von Virtual Trusted Platform Module-Gerätezertifikaten 387

12 Sichern von Windows-Gastbetriebssystemen mit virtualisierungsbasierter Sicherheit 389
Best Practices für die Sicherheit auf Basis der vSphere-Virtualisierung 390
Aktivieren der virtualisierungsbasierten Sicherheit auf einer virtuellen Maschine 391
Aktivieren der virtualisierungsbasierten Sicherheit auf einer vorhandenen virtuellen Maschine 393
Aktivieren von virtualisierungsbasierter Sicherheit auf dem Gastbetriebssystem 394
Deaktivieren von virtualisierungsbasierter Sicherheit 394
Identifizieren von VBS-fähigen virtuellen Maschinen 395

13 Sichern der vSphere-Netzwerke 396
Absichern des Netzwerks mit Firewalls 398
Firewalls in Konfigurationen mit vCenter Server 399
Herstellen einer Verbindung mit einem vCenter Server über eine Firewall 400
Verbinden von ESXi-Hosts über Firewalls 400
Firewalls für Konfigurationen ohne vCenter Server 400

Herstellen einer Verbindung mit der VM-Konsole über eine Firewall 401
Sichern des physischen Switches auf ESXi-Hosts 402
Sichern von Standard-Switch-Ports durch Sicherheitsrichtlinien 403
Sichern von vSphere Standard-Switches 403
MAC-Adressänderungen 404
Gefälschte Übertragungen 405
Betrieb im Promiscuous-Modus 406
Schutz von Standard-Switches und VLANs 406
Sichern von vSphere Distributed Switches und verteilten Portgruppen 408
Absichern virtueller Maschinen durch VLANs 409
Sicherheitsempfehlungen für VLANs 410
Sichern von VLANs 411
Erstellen mehrerer Netzwerke auf einem einzelnen ESXi-Host 411
Verwenden von Internet Protocol Security auf ESXi-Hosts 414
Auflisten der verfügbaren Sicherheitsverbindungen auf ESXi-Hosts 414
Hinzufügen einer IPsec-Sicherheitsverbindung zu einem ESXi-Host 415
Entfernen einer IPsec-Sicherheitsverbindung auf einem ESXi-Host 416
Auflisten der verfügbaren IPsec-Sicherheitsrichtlinien auf einem ESXi-Host 416
Erstellen einer IPSec-Sicherheitsrichtlinie auf einem ESXi-Host 416
Entfernen einer IPsec-Sicherheitsrichtlinie auf einem ESXi-Host 418
Sicherstellen der ordnungsgemäßen SNMP-Konfiguration auf ESXi-Hosts 418
vSphere Networking, empfohlene Vorgehensweisen für die Sicherheit 419
Allgemeine Empfehlungen für die vSphere-Netzwerksicherheit 419
Bezeichnungen von vSphere-Netzwerkkomponenten 421
Dokumentieren und Überprüfen der vSphere-VLAN-Umgebung 421
Einführung von Netzwerkisolierungspraktiken in vSphere 422
Bedarfsgerechtes Verwenden von virtuellen Switches mit der vSphere Network Appliance-API 424

14 Empfohlene Vorgehensweisen für mehrere vSphere-Komponenten 425
Synchronisieren der Systemuhren im vSphere-Netzwerk 425
Synchronisieren der ESXi-Systemuhren mit einem NTP-Server 427
Konfigurieren der Einstellungen für die Uhrzeitsynchronisierung in vCenter Server 427
Verwenden der Uhrzeitsynchronisierung von VMware Tools 428
Hinzufügen oder Ersetzen von NTP-Servern in der vCenter Server-Konfiguration 428
Synchronisieren der Uhrzeit in vCenter Server mit einem NTP-Server 429
Speichersicherheit, empfohlene Vorgehensweisen 430
Absichern von iSCSI-Speicher 430
Schützen von iSCSI-Geräten 430
Schützen eines iSCSI-SAN 431
Maskieren von SAN-Ressourcen und Einteilen derselben in Zonen 432
Verwenden von Kerberos für NFS 4.1 432

Überprüfen, ob das Senden von Hostleistungsdaten an Gastbetriebssysteme deaktiviert ist 434
Einstellen von Zeitüberschreitungen für die ESXi Shell und den vSphere Client 434

15 vSphere-TLS-Konfiguration 436
Verwalten der vSphere-TLS 440
Anzeigen des TLS-Profils eines ESXi-Hosts mit vSphere Client 441
Anzeigen des TLS-Profils eines ESXi-Hosts mithilfe der CLI 441
Ändern des TLS-Profils eines ESXi-Hosts mithilfe des vSphere Client 442
Ändern des TLS-Profils eines ESXi-Hosts mithilfe der CLI 443
Bearbeiten der Parameter im MANUAL TLS-Profil in der CLI 443
Verwalten des TLS-Profils eines vCenter Server-Hosts 445

16 Definierte Rechte 446
Alarmrechte 449
Rechte für Auto Deploy und Image-Profile 450
Zertifikatsrechte 451
Berechtigungen der Zertifizierungsstelle 451
Berechtigungen der Zertifikatsverwaltung 452
CNS-Rechte 454
Rechte für Computing-Richtlinien 454
Rechte für Inhaltsbibliotheken 454
Rechte für Verschlüsselungsvorgänge 461
dvPort-Gruppenrechte 466
Rechte für Distributed Switches 467
Rechte für Datencenter 468
Berechtigungen für Datenspeicher 470
Rechte für Datenspeicher-Cluster 472
ESX Agent Manager-Rechte 472
Rechte für Erweiterungen 473
Rechte für Bereitstellungsfunktion externer Statistiken 474
Rechte für Ordner 474
Globale Rechte 475
Interaktion mit den Gastdaten-Veröffentlichungsrechten 477
Rechte für den verknüpften Hybridmodus 477
Rechte für Bereitstellungsfunktion für Aktualisierungen des Systemzustands 478
Host-CIM-Rechte 478
Rechte für die Hostkonfiguration 478
Host-Entropie-Pool-Rechte 481
Intel Software Guard Extensions-Hostrechte 481
Rechte für die Hostbestandsliste 482
Rechte für lokale Hostoperationen 483

Host-Statistikrechte 484
Trusted Platform Module (TPM)-Hostrechte 484
vSphere Replication-Rechte von Hosts 485
Hostprofil-Berechtigungen 485
vCenter Server-Profilrechte 486
vSphere Namespaces-Rechte 486
Netzwerkberechtigungen 488
NSX-Rechte 489
VMware Observability-Rechte 489
OvfManager-Rechte 489
Rechte für die Interaktion mit Partner-REST-Daemons 489
Leistungsrechte 490
Plug-In-Rechte 490
Rechte für die Replizierung als Dienst 491
Rechte für Berechtigungen 491
Rechte für VM-Speicherrichtlinien 492
Rechte für Ressourcen 492
Rechte für geplante Aufgaben 494
Sitzungsrechte 495
Speicheransichtsberechtigungen 496
Rechte für Supervisor-Dienste 496
Rechte für Aufgaben 497
Mandantenmanagerrechte 497
Transfer Service-Rechte 498
Rechte für VcTrusts/VcIdentity 498
Rechte für „Administrator der vertrauenswürdigen Infrastruktur“ 499
vApp-Rechte 501
Rechte für VcIdentityProviders 504
Rechte für die Konfiguration von VMware vSphere Lifecycle Manager 505
Gewünschte Rechte für die Konfigurationsverwaltung von VMware vSphere Lifecycle Manager 506
Rechte für ESXi-Integritätsperspektiven für VMware vSphere Lifecycle Manager 507
Rechte für VMware vSphere Lifecycle Manager-Depots 508
Allgemeine Rechte für VMware vSphere Lifecycle Manager 508
Rechte für die Hardwarekompatibilität von VMware vSphere Lifecycle Manager 509
Rechte für VMware vSphere Lifecycle Manager-Images 509
Rechte für die Standardisierung von VMware vSphere Lifecycle Manager-Images 512
Rechte für VMware vSphere Lifecycle Manager-Einstellungen 512
Rechte für die Verwaltung von VMware vSphere Lifecycle Manager-Baselines 513
Rechte zum Verwalten von Patches und Upgrades für VMware vSphere Lifecycle Manager 513
Rechte zum Hochladen von Dateien für VMware vSphere Lifecycle Manager 514
Rechte zum Ändern der VM-Konfiguration 515

Rechte für Vorgänge als Gast auf virtuellen Maschinen 519
Rechte für die Interaktion virtueller Maschinen 521
Rechte zum Bearbeiten der Bestandsliste einer virtuellen Maschine 525
Rechte für das Bereitstellen virtueller Maschinen 527
Rechte für die Dienstkonfiguration der virtuellen Maschine 529
Rechte für die Snapshot-Verwaltung von virtuellen Maschinen 530
vSphere Replication-Rechte der VM 531
Rechte für VM-Klassen 531
vSAN-Rechte 532
Rechte für vSAN-Statistiken 532
vSphere-Zonen-Rechte 532
vService-Rechte 533
vSphere-Tag-Berechtigungen 534
vSphere Client-Rechte 535
vSphere Data Protection-Rechte 535
vSphere Stats-Rechte 535

17 vSphere Hardening und Übereinstimmung 537
Sicherheit vs. Übereinstimmung in der vSphere-Umgebung 537
Referenz zu vSphere-Sicherheitskontrollen 540
vSphere-Systemdesign-Sicherheitskontrollenreferenz 542
Referenz zu vSphere-Hardware-Sicherheitskontrollen 549
Referenz der ESXi-Sicherheitskontrollen 556
Referenz der vCenter Server-Sicherheitskontrollen 612
Referenz zu Sicherheitskontrollen für virtuelle Maschinen 642
Sicherheitskontrollen des Gastbetriebssystems 656
Referenz der vSAN-Sicherheitskontrollen 668
Informationen zum National Institute of Standards and Technology 671
Informationen zu DISA STIGs 672
Über NERC CIP 672
Informationen zu VMware Security Development Lifecycle 673
Überwachungsprotokollierung in vSphere 673
Single Sign-On-Audit-Ereignisse 674
Grundlegendes zur Sicherheit und Übereinstimmung – nächste Schritte 675
vCenter Server und FIPS 676
In ESXi verwendete FIPS-Module 677
Aktivieren und Deaktivieren von FIPS auf der vCenter Server Appliance 677
Überlegungen bei der Verwendung von FIPS 678

Info zu vSphere Security

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

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

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

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

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

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

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

Verwandte Dokumentation

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

Zusätzlich zu diesen Dokumenten veröffentlicht VMware das *vSphere Security Configuration Guide* (früher bekannt als *Hardening Guide*) für jede vSphere-Version, die unter https://core.vmware.com/security verfügbar ist. Das Handbuch *vSphere Security Configuration Guide* enthält Leitlinien zu Sicherheitseinstellungen, die vom Kunden festgelegt werden können bzw. sollten, und zu von VMware bereitgestellten Sicherheitseinstellungen, für die der Kunde prüfen sollte, ob sie noch auf die jeweiligen Standardwerte festgelegt sind.

Was ist mit Platform Services Controller (PSC) geschehen?

Ab vSphere 7.0 muss für die Bereitstellung einer neuen Version von vCenter Server oder das Upgrade auf vCenter Server 7.0 die vCenter Server Appliance verwendet werden. Dies ist eine vorkonfigurierte virtuelle Maschine, die für die Ausführung von vCenter Server optimiert ist. Der neue vCenter Server enthält alle Platform Services Controller-Dienste, wobei die Funktionen und Workflows – darunter Authentifizierung, Zertifikatsverwaltung, Tags und Lizenzierung – beibehalten wurden. Es ist nicht mehr erforderlich und auch nicht mehr möglich, eine externe Platform Services Controller-Instanz bereitzustellen und zu verwenden. Alle Platform Services Controller-Dienste sind in vCenter Server konsolidiert, sodass die Bereitstellung und Verwaltung vereinfacht werden.

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

Zielgruppe

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

Zertifizierungen

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

Sicherheit in der vSphere-Umgebung

1

Die Komponenten einer vSphere-Umgebung sind ab Werk durch mehrere Merkmale wie Authentifizierung, Autorisierung, Firewalls auf jedem ESXi-Host usw. gesichert. Sie können das Standard-Setup auf viele Arten ändern. Sie können beispielsweise Berechtigungen für vCenter Server-Objekte festlegen, Firewallports öffnen oder die Standardzertifikate ändern. Sie können Sicherheitsmaßnahmen für verschiedene vSphere-Objekte ergreifen, wie beispielsweise für vCenter Server-Systeme, ESXi-Hosts, virtuelle Maschinen sowie Netzwerk- und Speicherobjekte.

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

Lesen Sie als Nächstes die folgenden Themen:

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

Absichern des ESXi-Hypervisors

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

Sie können mithilfe der folgenden Aktionen den Schutz von ESXi-Hosts, die von vCenter Server verwaltet werden, noch verbessern. Die Sicherheitsüberlegungen für eigenständige Hosts sind ähnlich, obwohl die Verwaltungsaufgaben sich möglicherweise unterscheiden. Informationen finden Sie in der Dokumentation *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

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 für das Hostobjekt über das vCenter Server-System fest, das den Host verwaltet.

Weitere Informationen finden Sie unter Verwenden der ESXi Shell.

Verwenden von benannten Benutzern und der geringsten Berechtigung

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

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

Minimieren der Anzahl offener ESXi-Firewallports

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

Weitere Informationen hierzu finden Sie unter Konfigurieren der ESXi Firewall.

Automatisieren der ESXi-Hostverwaltung

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

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

Verwenden des ESXi-Sperrmodus

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

Weitere Informationen hierzu finden Sie unter Konfigurieren und Verwalten des Sperrmodus auf ESXi-Hosts.

Prüfen der VIB-Paketintegrität

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

Weitere Informationen hierzu finden Sie unter Verwalten der Akzeptanzebenen von ESXi-Hosts und vSphere-Installationspaketen.

Verwalten von ESXi-Zertifikaten

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

Weitere Informationen hierzu finden Sie unter Verwalten von Zertifikaten für ESXi-Hosts.

Überlegungen zur Smartcard-Authentifizierung für ESXi

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

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

Überlegungen zum Sperren von ESXi-Konten

Das Sperren von Konten für den Zugriff über SSH und das vSphere Web Services SDK wird unterstützt. Standardmäßig wird das Konto nach maximal fünf fehlgeschlagenen Anmeldeversuchen gesperrt. Das Konto wird standardmäßig nach 15 Minuten entsperrt.

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

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

Sichern von vCenter Server-Systemen und zugehörigen Diensten

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

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

vCenter Server verwendet verschlüsselte Kommunikation

Standardmäßig ist die gesamte Datenkommunikation zwischen dem vCenter Server-System und den anderen vSphere-Komponenten verschlüsselt. Der Konfiguration Ihrer Umgebung entsprechend kann ein Teil des Datenverkehrs unverschlüsselt sein. Sie können z. B. unverschlüsseltes SMTP für E-Mail-Warnungen und unverschlüsseltes SNMP für die Überwachung konfigurieren. DNS-Datenverkehr ist ebenfalls unverschlüsselt. vCenter Server überwacht Port 80 (TCP) und Port 443 (TCP). Port 443 (TCP) ist der branchenübliche Port für HTTPS (sicheres HTTP) und über eine TLS-Verschlüsselung geschützt. Weitere Informationen hierzu finden Sie unter Kapitel 15 vSphere-TLS-Konfiguration. Port 80 (TCP) ist der branchenübliche HTTP-Port und verwendet keine Verschlüsselung. Port 80 dient dazu, Anforderungen von Port 80 an Port 443 umzuleiten, wo sie sicher sind.

Erhöhen der Sicherheit von vCenter Server-Systemen

Der erste Schritt zum Schutz Ihrer vCenter Server-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.

Weitere Informationen zum vSphere-Zertifikatmodell

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

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

Konfigurieren von vCenter Single Sign On

vCenter Server und die zugehörigen Dienste sind durch vCenter Single Sign On und dessen Authentifizierungsframework geschützt. Bei der erstmaligen Installation der Software geben Sie ein Kennwort für den Administrator der vCenter Single Sign-On-Domäne an (standardmäßig administrator@vsphere.local). Nur diese Domäne ist anfangs als Identitätsquelle verfügbar. Sie können einen externen Identitätsanbieter wie Microsoft Active Directory Federation Services (AD FS) für die Verbundauthentifizierung hinzufügen. Sie können weitere Identitätsquellen (entweder Active Directory oder LDAP) hinzufügen und eine Standardidentitätsquelle bestimmen. Benutzer, die sich bei diesen Identitätsquellen authentifizieren können, können auch Objekte anzeigen und Aufgaben ausführen, sofern sie die entsprechende Berechtigung besitzen. Weitere Informationen finden Sie in der Dokumentation *vSphere-Authentifizierung*.

Hinweis Es wird empfohlen, die Verbundauthentifizierung zu verwenden, da in vSphere künftig die tokenbasierte Authentifizierung verwendet wird. vCenter Server verwendet weiterhin lokale Konten für Administratorzugriff und Fehlerbehebung.

Zuweisen von vCenter Server-Rollen zu benannten Benutzern oder Gruppen

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

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

Einrichten von Precision Time Protocol oder Network Time Protocol

Richten Sie Precision Time Protocol (PTP) oder Network Time Protocol (NTP) für jeden Knoten in Ihrer Umgebung ein. Die vSphere-Zertifikatinfrastruktur erfordert einen genauen Zeitstempel und funktioniert nicht ordnungsgemäß, wenn die Knoten nicht synchronisiert sind.

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

Sichern von virtuellen Maschinen

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

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 nicht benötigter Funktionen der virtuellen Maschine

Achten Sie darauf, ungenutzte Funktionen zu deaktivieren, um mögliche Angriffsflächen 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 VM-Vorlagen und skriptbasierte Verwaltung

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

Wenn Sie nach der Erstbereitstellung die Einstellungen der virtuellen Maschine ändern möchten, sollten Sie PowerCLI-Skripts verwenden. In dieser Dokumentation wird hauptsächlich die Durchführung von Aufgaben mit dem vSphere Client erläutert. Verwenden Sie eventuell Skripts anstelle des vSphere Client, um für die Konsistenz Ihrer Umgebung zu sorgen. In großen Umgebungen können Sie virtuelle Maschine in Ordner gruppieren, um das Scripting zu erleichtern.

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

Beschränken der Verwendung der VM-Konsole auf ein Minimum

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

Überlegungen zu UEFI Secure Boot für virtuelle Maschinen

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

Schützen der virtuellen Netzwerkebene

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

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

Isolieren des Netzwerkdatenverkehrs

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

Weitere Informationen hierzu finden Sie unter ESXi-Netzwerksicherheitsempfehlungen.

Schützen virtueller Netzwerkelemente durch Firewalls

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

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

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

Netzwerksicherheitsrichtlinien

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

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

Schützen von VM-Netzwerken

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

- Das installierte Gastbetriebssystem
- Ob die virtuellen Maschinen in einer vertrauenswürdigen Umgebung betrieben werden

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

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

Schützen Ihrer Umgebung durch VLANs

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

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

Schützen der Verbindungen zum virtualisierten Speicher

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

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

Weitere Informationen hierzu finden Sie unter Speichersicherheit, empfohlene Vorgehensweisen.

Bewerten der Verwendung von Internet Protocol Security

ESXi unterstützt Internet Protocol Security (IPSec) über IPv6. IPSec über IPv4 ist nicht möglich.

Weitere Informationen hierzu finden Sie unter Verwenden von Internet Protocol Security auf ESXi-Hosts.

Sichern von Kennwörtern in Ihrer vSphere-Umgebung

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

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

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

Kennwort für den vCenter Single Sign On-Administrator

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

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

Kennwörter für andere Benutzer der vCenter Single Sign-On-Domäne

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

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

Kennwörter für Benutzer aus anderen Identitätsquellen

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

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

Kennwörter für DCUI-Benutzer der vCenter Server

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

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

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

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

Best Practices und Ressourcen für die Sicherheit für vCenter Server und ESXi

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

Dieses Handbuch enthält Best Practices für die verschiedenen Komponenten Ihrer vSphere-Infrastruktur. Dieses Handbuch ist eine von mehreren Ressourcen, die Sie für eine sichere Umgebung verwenden müssen.

vSphere-Sicherheitsressourcen

Weitere Informationen zu spezifischen Aspekten der vSphere-Sicherheit finden Sie im folgenden Inhalt dieses Handbuchs.

Tabelle 1-1. Empfohlene Vorgehensweisen für die Sicherheit

vSphere-Komponente	Ressource
ESXi-Host	Kapitel 3 Sichern der ESXi-Hosts
vCenter Server-System	Kapitel 4 Sichern von vCenter Server-Systemen
Virtuelle Maschine	Virtuelle Maschine – Empfohlene Vorgehensweisen für die Sicherheit
vSphere-Netzwerk	vSphere Networking, empfohlene Vorgehensweisen für die Sicherheit

Sicherheitsressourcen von VMware im Internet

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

Tabelle 1-2. Sicherheitsressourcen von VMware im Internet

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

vSphere-Berechtigungen und Benutzerverwaltungsaufgaben

2

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

Eine Übersicht über die Zuweisung von Rollen und Berechtigungen mithilfe des vSphere Client finden Sie im folgenden Video.

 (Zuweisen von Rollen und Berechtigungen mithilfe von vSphere Client)

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

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

Als Administratorbenutzer haben Sie folgende Möglichkeiten:

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

Lesen Sie als Nächstes die folgenden Themen:

- Grundlegende Informationen zur Autorisierung in vSphere
- Funktionsweise mehrerer Berechtigungseinstellungen in vSphere
- Verwalten von Berechtigungen für vCenter Server-Komponenten
- Verwenden globaler vCenter Server-Berechtigungen

- Verwenden von vCenter Server-Rollen zum Zuweisen von Rechten
- Verwenden des Rechte-Recorders
- Best Practices für Rollen und Berechtigungen in vCenter Server
- Erforderliche vCenter Server-Rechte für allgemeine Aufgaben

Grundlegende Informationen zur Autorisierung in vSphere

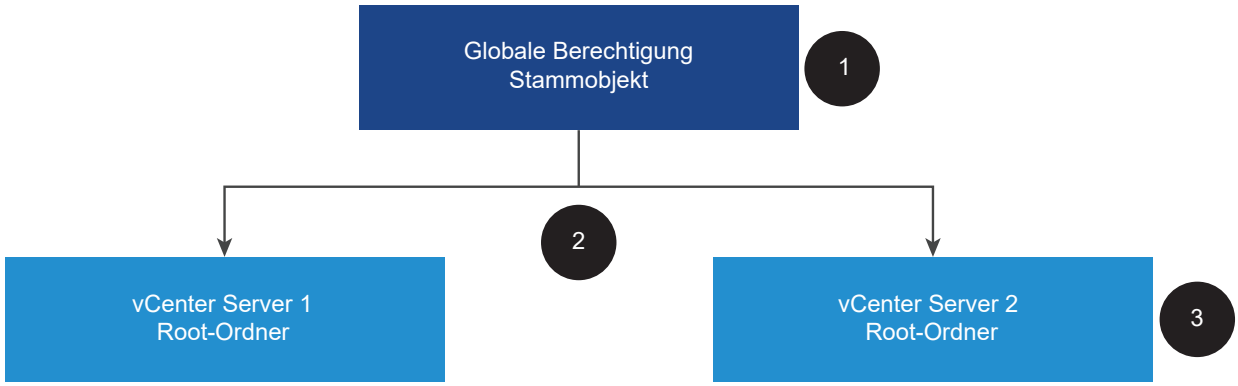
vSphere unterstützt mehrere Modelle, um zu ermitteln, ob ein Benutzer eine Aufgabe ausführen darf. Die Gruppenmitgliedschaft in einer vCenter Single Sign-On-Gruppe entscheidet, was Sie tun dürfen. Ihre Rolle für ein Objekt oder Ihre globale Berechtigung legt fest, ob Sie andere Aufgaben durchführen dürfen.

Funktionsweise von Berechtigungen in vSphere

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

Die folgende Abbildung veranschaulicht die Funktionsweise globaler und lokaler Berechtigungen.

Abbildung 2-1. Globale und lokale Berechtigungen



In dieser Abbildung:

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

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

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

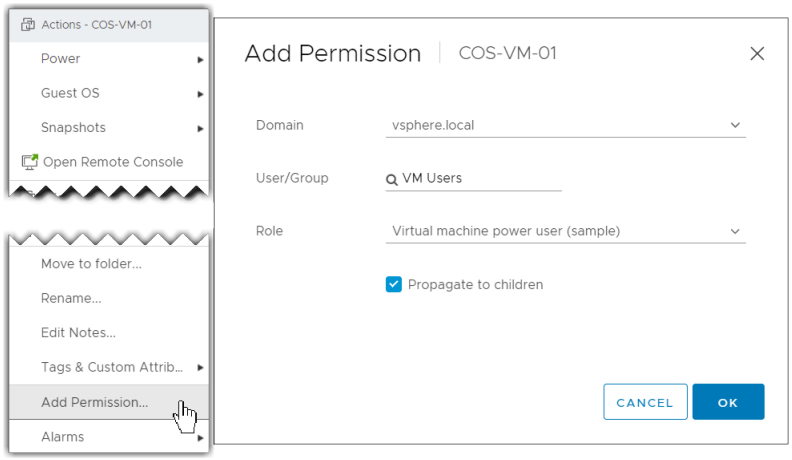
vCenter Server-Berechtigungen

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

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

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

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



Globale Berechtigungen

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

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

Gruppenmitgliedschaft in vCenter Single Sign-On-Gruppen

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

Berechtigungen für lokale ESXi-Hosts

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

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

Einblick in das objektbezogene Berechtigungsmodell

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

Die folgenden Konzepte sind wichtig.

Berechtigungen

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

Benutzer und Gruppen

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

Berechtigungen

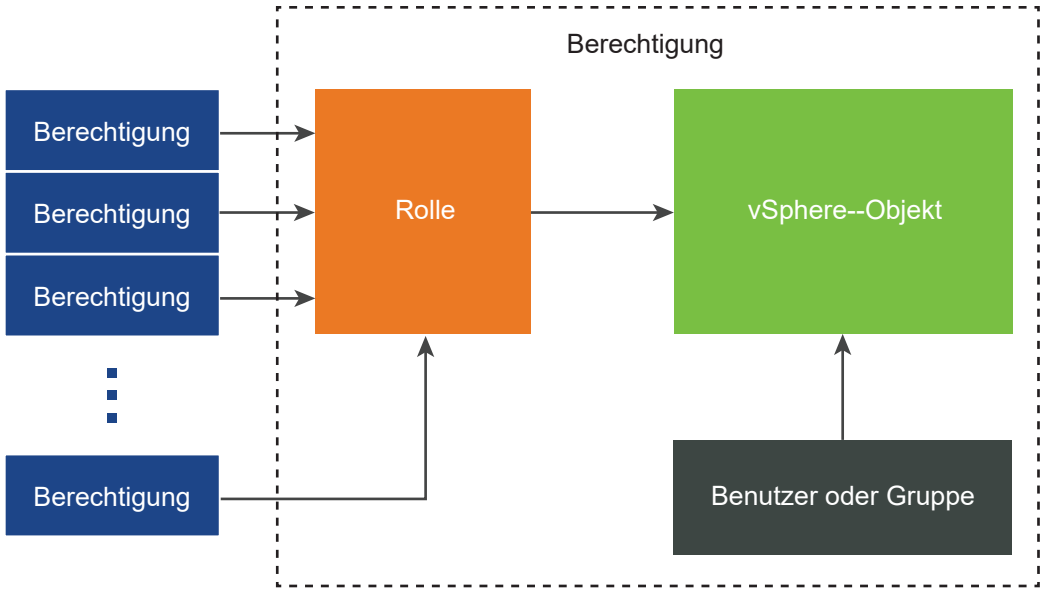
Rechte sind detaillierte Zugriffssteuerungsoptionen. Sie können diese Rechte nach Rollen gruppieren, die dann Benutzern oder Gruppen zugeordnet werden können.

Rollen

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

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

Abbildung 2-3. vSphere-Berechtigungen



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

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

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

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

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

Siehe folgende Informationen.

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

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

Was ist vCenter Server-Benutzervalidierung?

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

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

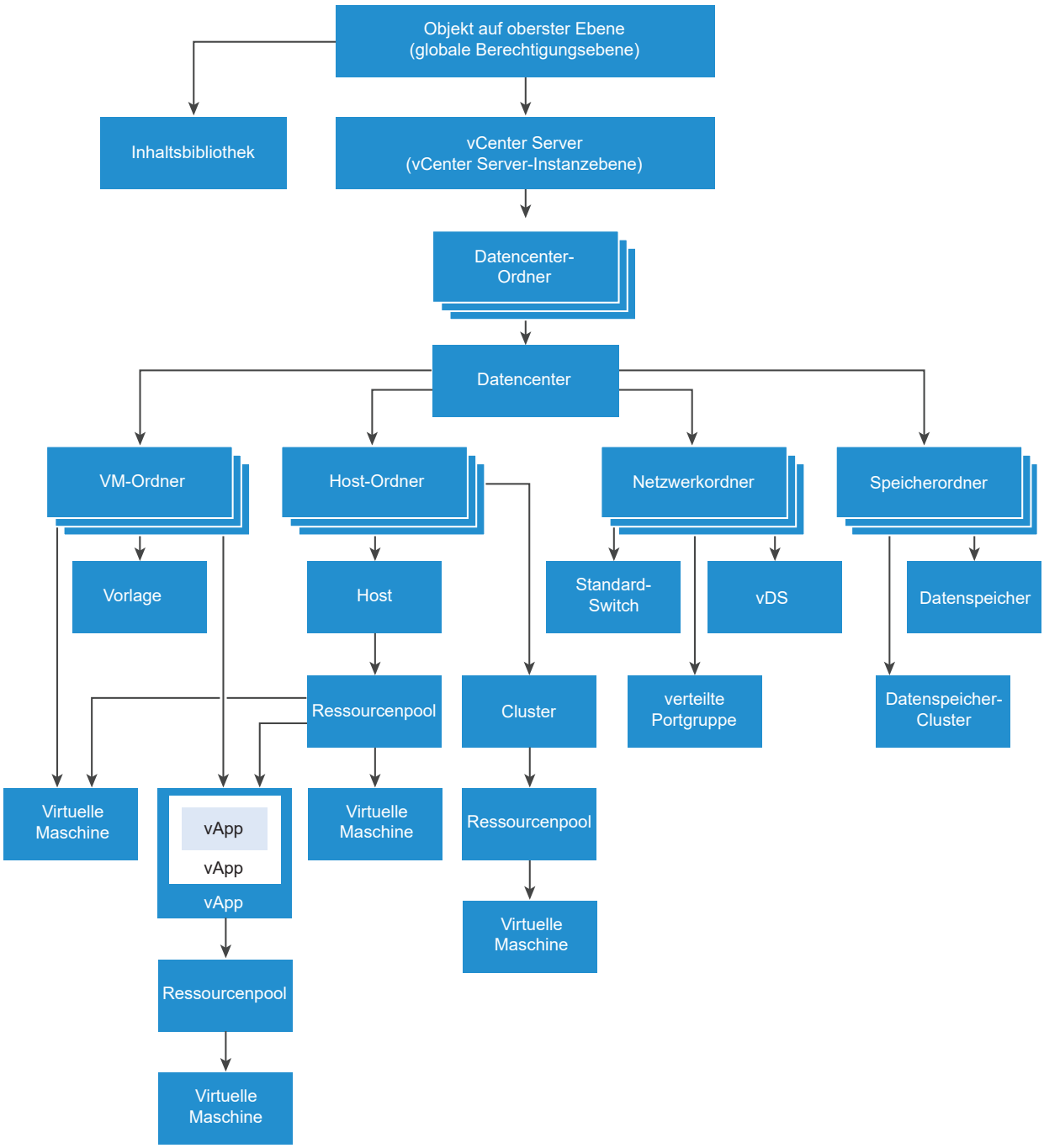
Hierarchische Vererbung von Berechtigungen in vSphere

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

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

Hinweis Globale Berechtigungen unterstützen das lösungsübergreifende Zuweisen von Berechtigungen von einem globalen Stammobjekt aus. Weitere Informationen hierzu finden Sie unter Verwenden globaler vCenter Server-Berechtigungen.

Abbildung 2-4. vSphere-Bestandslistenhierarchie



Über diese Abbildung:

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

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

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

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

In der Hierarchie gibt es verschiedene Formen von Berechtigungen.

Verwaltete Elemente

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

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

Globale Entitäten

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

- Benutzerdefinierte Felder
- Lizenzen
- Rollen
- Statistikintervalle
- Sitzungen

Funktionsweise mehrerer Berechtigungseinstellungen in vSphere

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

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

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

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

Beispiel 1: Berechtigungsübernahme von mehreren Gruppen

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

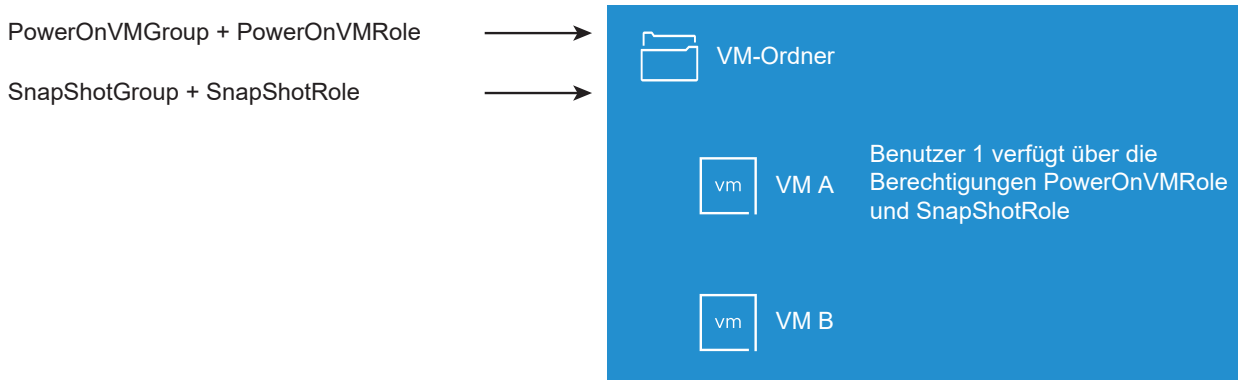
In diesem Beispiel werden zwei verschiedenen Gruppen zwei Berechtigungen für das gleiche Objekt zugewiesen.

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

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

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

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



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

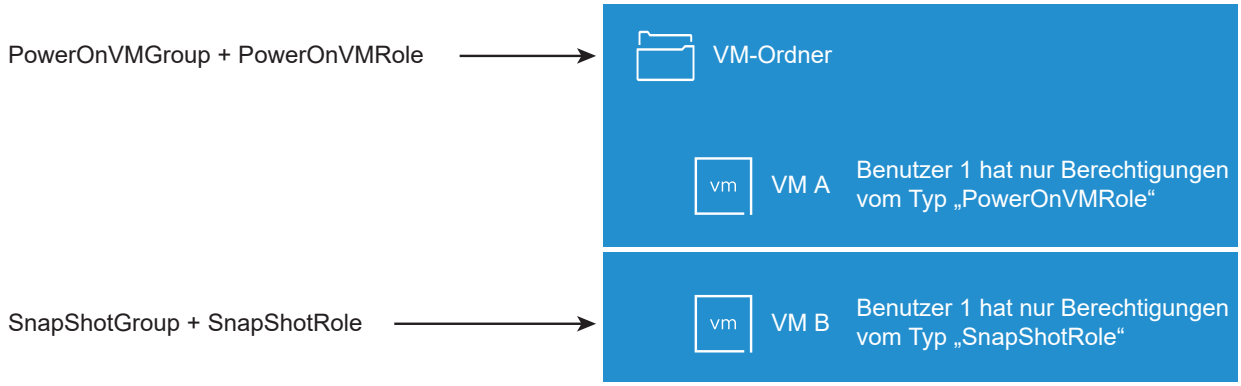
Dieses Beispiel zeigt, wie Berechtigungen, die einem untergeordneten Objekt zugewiesen wurden, die Berechtigungen, die einem übergeordneten Objekt zugewiesen wurden, außer Kraft setzen. Sie können dieses Verhalten dazu verwenden, um den Benutzerzugriff auf bestimmte Bereiche der Bestandsliste einzuschränken.

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

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

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

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



Beispiel 3: Benutzerrolle, die Gruppenrolle außer Kraft setzt

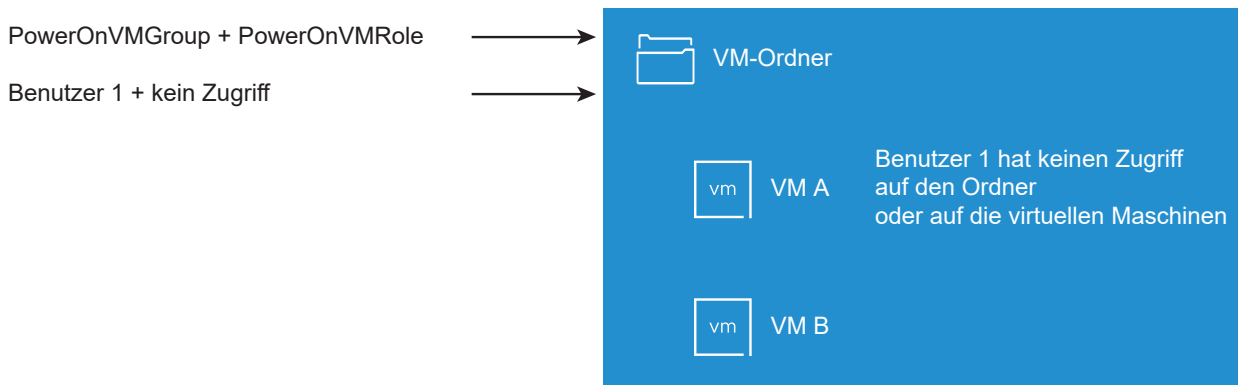
Dieses Beispiel zeigt, wie die einem individuellen Benutzer direkt zugewiesene Rolle die Rechte einer Rolle überschreibt, die einer Gruppe zugeordnet ist.

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

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

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

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



Verwalten von Berechtigungen für vCenter Server-Komponenten

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

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

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

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

Hinzufügen einer Berechtigung zu einem Bestandslistenobjekt

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

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

Voraussetzungen

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

Verfahren

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

3 Klicken Sie auf **Hinzufügen**.

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

5 Wenn Sie im Dropdown-Menü **Domäne** den Eintrag **VMware-ID** auswählen, geben Sie den Benutzer- oder Gruppennamen ein.

Hinweis Geben Sie die E-Mail-Adresse des CSP-Kontos in das Feld **Benutzername** ein. CSP-Konten können in der VMwareID-Domäne nicht durchsucht werden.

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

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

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

Das System sucht nach Benutzer- und Gruppennamen.

c Wählen Sie den Benutzer oder die Gruppe aus.

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

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

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

9 Klicken Sie auf **OK**.

Ändern oder Entfernen von Berechtigungen für ein Bestandslistenobjekt

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

Verfahren

1 Navigieren Sie zum Objekt im Objektnavigator des vSphere Client.

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

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

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

Ändern der Einstellungen für die vCenter Server-Benutzervalidierung

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

Diese Einstellungen gelten für vCenter Single Sign On-Identitätsquellen und nicht für eine externe Identitätsquelle, wie z. B. Active Directory, die vCenter Server zugeordnet sein könnten.

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

Verfahren

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

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

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

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

Option	Beschreibung
Benutzerverzeichnis - Zeitüberschreitung	Zeitüberschreitungsintervall (in Sekunden) für die Suche nach dieser vCenter Server-Installation.
Abfragegrenze	Aktivieren Sie die Option, um die maximale Anzahl von Benutzern und Gruppen festzulegen, die vCenter Server anzeigt.
Größe der Abfragegrenze	Maximale Anzahl der Benutzer und Gruppen der ausgewählten Domäne, die von vCenter Server im Dialogfeld **Benutzer oder Gruppen auswählen** angezeigt werden. Bei Eingabe des Werts 0 (Null) werden alle Benutzer und Gruppen angezeigt.

Verwenden globaler vCenter Server-Berechtigungen

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

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

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

Tabelle 2-1. Unterschiede zwischen vCenter Server-Berechtigungen und globalen Berechtigungen

Berechtigungstyp	Beschreibung
vCenter Server	vCenter Server-Berechtigungen gelten für bestimmte Objekte in der Bestandslistenhierarchie, z. B. Hosts, virtuelle Maschinen, Datenspeicher usw. Beim Zuweisen von vCenter Server-Berechtigungen geben Sie an, dass ein Benutzer oder eine Gruppe über eine Rolle (eine Reihe von Rechten) für das Objekt verfügt.
Global	Mithilfe von globalen Berechtigungen werden einem Benutzer oder einer Gruppe Rechte zum Anzeigen oder Verwalten aller Objekte in allen Bestandslistenhierarchien Ihrer Bereitstellung erteilt. Globale Berechtigungen gelten auch für globale Objekte wie Tags und Inhaltsbibliotheken. Weitere Informationen hierzu finden Sie unter vCenter Server-Berechtigungen für Tag-Objekte. Wenn Sie eine globale Berechtigung zuweisen und „Weitergeben“ nicht auswählen, haben die Benutzer oder Gruppen, denen diese Berechtigung zugeordnet ist, keinen Zugriff auf die Objekte in der Hierarchie. Sie haben nur Zugriff auf bestimmte globale Funktionen wie etwa das Erstellen von Rollen.

Hinzufügen einer globalen Berechtigung

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

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

Voraussetzungen

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

Verfahren

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

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

3 Klicken Sie auf **Hinzufügen**.

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

5 Wenn Sie in vSphere+-Umgebungen im Dropdown-Menü **Domäne** den Eintrag **VMware-ID** auswählen, geben Sie den Namen des CSP-Kontos in das Feld **Benutzername** ein.

Hinweis Geben Sie die E-Mail-Adresse des CSP-Kontos in das Feld **Benutzername** ein. CSP-Konten können in der VMwareID-Domäne nicht durchsucht werden.

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

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

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

   Das System sucht nach Benutzer- und Gruppennamen.

   c Wählen Sie den Benutzer oder die Gruppe aus.

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

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

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

9 Klicken Sie auf **OK**.

vCenter Server-Berechtigungen für Tag-Objekte

In der Objekthierarchie von vCenter Server sind Tag-Objekte keine untergeordneten Objekte von vCenter Server, sondern werden auf der obersten Ebene von vCenter Server erstellt. In Umgebungen mit mehreren vCenter Server-Instanzen werden Tag-Objekte von vCenter Server-

Instanzen gemeinsam genutzt. Die Berechtigungen für Tag-Objekte unterscheiden sich von Berechtigungen für andere Objekte in der Objekthierarchie von vCenter Server.

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

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

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

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

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

Globale Berechtigungen ergänzen Berechtigungen für Tag-Objekte

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

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

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

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

Berechtigungen auf Tag-Ebene können globale Berechtigungen erweitern

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

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

Tabelle 2-4. 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 vCenter Server-Rollen zum Zuweisen von Rechten

In vCenter Server ist eine Rolle ein vordefinierter Satz von Rechten, der Rechte zum Ausführen von Aktionen und Leseeigenschaften definiert. Sie erstellen Berechtigungen, indem Sie einem Benutzer oder einer Gruppe für ein Objekt eine Rolle zuweisen. vCenter Server bietet standardmäßig System- und Beispielrollen. Sie können auch benutzerdefinierte Rollen erstellen.

Zuweisen von Berechtigungen in vCenter Server

Beim Zuweisen von Berechtigungen in vCenter Server weisen Sie einen Benutzer oder einer Gruppe einer Rolle zu und verknüpfen diese Zuweisung mit einem Bestandslistenobjekt. Sie können beispielsweise die Beispielrolle „VM-Benutzer“ verwenden, um einem Benutzer das Lesen und Ändern von Attributen der virtuellen Maschine zu ermöglichen

Ein Benutzer oder eine Gruppe kann verschiedene Rollen für verschiedene Objekte in der Bestandsliste aufweisen. Nehmen Sie z. B. an, dass zwei Ressourcenpools in Ihrer Bestandsliste vorhanden sind: Pool A und Pool B. Sie können der Gruppe „Vertrieb“ die VM-Benutzerbeispielrolle auf Pool A und die Nur-Lese-Rolle auf Pool B zuweisen. Mit diesen Zuweisungen können die Benutzer der Gruppe „Vertrieb“ die virtuellen Maschinen in Pool A einschalten, aber die virtuellen Maschinen in Pool B nur anzeigen.

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

Definition der vordefinierten vCenter Server-Rollen

vCenter Server bietet vordefinierte Rollen, wie in der folgenden Tabelle dargestellt.

Tabelle 2-5. Vordefinierte vCenter Server-Rollen

Rollentyp	Rollennamen	Beschreibung
System	„Administrator“, „Nur lesen“ und „Kein Zugriff“.	Systemrollen sind dauerhaft. Sie können weder Systemrollen löschen noch die mit diesen Rollen verknüpften Rechte bearbeiten. Die Systemrollen sind hierarchisch organisiert. Jede Rolle enthält die Rechte der vorhergehenden Rolle. So übernimmt beispielsweise die Rolle „Administrator“ die Rechte der Rolle „Nur lesen“. Weitere Informationen zu Systemrollen finden Sie im folgenden Abschnitt.
Beispiel	vSphere bietet eine Reihe von Beispielrollen, z. B. AutoUpdateUser, Ressourcenpooladministrator und VM-Benutzer.	vSphere bietet Beispielrollen für einige gängige Aufgabenkombinationen. Diese Rollen können Sie klonen, abändern oder entfernen. **Hinweis** Um die vordefinierten Einstellungen einer Rolle nicht zu verlieren, sollten Sie die Rolle zunächst klonen und die gewünschten Änderungen dann am Klon vornehmen. Das Beispiel kann nicht auf die Standardeinstellungen zurückgesetzt werden.

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

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

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.

vCenter Server-Systemrollen

Systemrollen können nicht geändert oder gelöscht werden.

Administratorrolle

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

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

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

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

Rolle „Nur Lesen“

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

Rolle „Kein Zugriff“

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

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

Benutzerdefinierte Rollen in vCenter Server und ESXi

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

Benutzerdefinierte Rolle in vCenter Server (empfohlen)

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

Benutzerdefinierte Rollen in ESXi

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

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

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

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

Erstellen einer benutzerdefinierten vCenter Server-Rolle

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

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

Voraussetzungen

Stellen Sie sicher, dass Sie im vCenter Server-System, auf dem Sie die Rolle erstellen, über Administratorrechte verfügen.

Verfahren

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

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

3 Erstellen Sie die Rolle.

Option	Beschreibung
So erstellen Sie eine Rolle:	a Klicken Sie auf **Neu**. b Geben Sie einen Namen für die neue Rolle ein. c Aktivieren und deaktivieren Sie Rechte für die Rolle. Führen Sie einen Bildlauf durch die Berechtigungskategorien durch und wählen Sie alle Rechte oder eine Teilmenge der Rechte für diese Kategorie aus. Sie können alle, ausgewählte oder nicht ausgewählte Kategorien anzeigen. Sie können auch alle, ausgewählte oder nicht ausgewählte Berechtigungen anzeigen. Weitere Informationen hierzu finden Sie unter Kapitel 16 Definierte Rechte. d Klicken Sie auf **Erstellen**.
Erstellen der Rolle durch Klonen	a Wählen Sie eine Rolle aus und klicken Sie auf **Klonen**. b Geben Sie einen Namen für die Rolle ein. c Klicken Sie auf **OK**. **Hinweis** Wenn Sie eine geklonte Rolle erstellen, können Rechte nicht geändert werden. Zum Ändern von Berechtigungen wählen Sie die geklonte Rolle aus und klicken auf **Bearbeiten**.

Nächste Schritte

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

Verwenden des Rechte-Recorders

In vSphere sind Rechte detaillierte Zugriffssteuerungen, die in Rollen gruppiert und Benutzern oder Gruppen zugeordnet werden können. Mit dem Rechte-Recorder können Sie den Mindestsatz an Rechten ermitteln, die zum Ausführen eines vCenter Server-Workflows erforderlich sind.

Um einen bestimmten Satz von Vorgängen auszuführen, ist es sehr schwierig, den minimalen Satz von Rechten zu ermitteln, die vom Benutzer benötigt werden. Die Rechte verfügen nicht über eine 1:1-Zuordnung mit dem spezifischen Workflow, der in der Regel aus mehreren Aufrufen verschiedener APIs besteht, die auf dem jeweiligen Objekt ausgeführt werden. Infolgedessen hat der Benutzer entweder mehr oder zu wenig Zugriff auf die Umgebung. Mit dem Ziel, die Sicherheit der Umgebung zu gewährleisten, hilft Ihnen die Funktion „Rechte-Recorder“ dabei,

die Mindestanzahl an Rechten zu ermitteln, die zur Ausführung eines vCenter Server-Workflows erforderlich sind. Damit können Sie die Rechte überwachen und abfragen, die während der Durchführung eines Vorgangs überprüft wurden. Rechte-Recorder wird mithilfe eines REST API implementiert.

Hinweis Diese Funktion ist als API verfügbar und unterstützt nur Workflows, die von einem Skript ausgeführt werden. „Rechte-Recorder“ wird auf der Benutzeroberfläche nicht unterstützt.

Durch Abfragen der ListAPI können Sie Listen von Überprüfung von Rechten zusammen mit den entsprechenden Sitzungen, Benutzern, verwalteten Objekten und Vorgangs-IDs (opIDs) abrufen. Sie können die entsprechenden Filter verwenden, um Rechtefür einen bestimmten Workflow zu erhalten.

Angenommen, Benutzer A muss eine VM erstellen. Zum Erstellen einer VM sind bestimmte Rechte erforderlich. Benutzer A muss Rechte beim Systemadministrator anfordern. Der Systemadministrator kann den Rechte-Recorder aktivieren und den Vorgang zum Erstellen einer VM ausführen. Während der Überprüfung der Rechte werden die Daten für die Rechte gespeichert, die während des Vorgangs „VM erstellen“ überprüft wurden. Die Daten enthalten PrivilegeID, sessionID, OpID usw. In diesem Beispiel verwendet dieser Systemadministrator die Filter, um Berechtigungen für den Workflow „VM erstellen“ zu erhalten. Der Systemadministrator kann jetzt eine Rolle mit den erforderlichen Mindestrechten erstellen und sie dem Benutzer zuweisen.

Aktivieren des Berechtigungs-Recorders

Sie aktivieren den Berechtigungs-Recorder mithilfe des vSphere Clients, um die vCenter Server-Konfigurationsdatei `vpxd.cfg` zu ändern.

Voraussetzungen

Stellen Sie sicher, dass Sie über ausreichende Rechte zum Ausführen Ihres Workflows verfügen. Ein Benutzer mit Administratorrolle wird empfohlen.

Verfahren

1. Melden Sie sich beim vCenter Server mit dem vSphere Client an.
2. Navigieren Sie zur vCenter Server-Instanz.
3. Wählen Sie **Konfigurieren > Erweiterte Einstellungen**.
4. Klicken Sie auf **Einstellungen bearbeiten**.

5 Fügen Sie die Einstellungen hinzu.

Scrollen Sie nach unten und geben Sie im Feld **Name** den Namen der Einstellung und im Feld **Wert** den Wert für die angegebene Einstellung ein.

Einstellung	Beschreibung
config.vpxd.privCheck.bufferSize	Die Anzahl der Rechte, die im Arbeitsspeicher gehalten werden sollen. Der Standardwert ist 0. Wenn Sie den Standardwert nicht ändern, zeichnet der Recorder für Berechtigungsprüfungen keine Daten auf.
config.vpxd.privCheck.cleanupInterval	Das Intervall, nach dem Berechtigungsprüfungen auf nicht verwendete Sitzungen bereinigt werden. Der Standardwert beträgt 30 Minuten.

6 Klicken Sie auf **Hinzufügen** und **Speichern**.

Nächste Schritte

Weitere Informationen finden Sie unter Performing Privilege Checks Operations im *Programmierhandbuch für VMware vSphere Automation-SDKs*.

Best Practices für Rollen und Berechtigungen in vCenter Server

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

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

- Sofern möglich, weisen Sie eine Rolle nicht einzelnen Benutzern sondern einer Gruppe zu.
- Erteilen Sie Berechtigungen nur für die entsprechenden erforderlichen Objekte und weisen Sie Rechte nur den entsprechenden erforderlichen Benutzern oder Gruppen zu. Vergeben Sie möglichst wenige Berechtigungen, um das Verstehen und Verwalten Ihrer Berechtigungsstruktur zu erleichtern.
- Wenn Sie einer Gruppe eine restriktive Rolle zuweisen, überprüfen Sie, dass die Gruppe weder den Administrator noch Benutzer mit Administratorrechten enthält. Anderenfalls schränken Sie möglicherweise die Rechte von Administratoren in den Teilen der Bestandslistenhierarchie ungewollt ein, für die Sie der Gruppe die restriktive Rolle zugewiesen haben.
- Gruppieren Sie Objekte in Ordnern, um die Zuweisung von Berechtigungen zu vereinfachen. Um beispielsweise einer Hostgruppe die Änderungsberechtigung und einer anderen Hostgruppe die Anzeigeberechtigung zuzuweisen, platzieren Sie die jeweiligen Hostgruppen in einem Ordner.

- Gehen Sie vorsichtig vor, wenn Sie den vCenter Server-Stammobjekten eine Berechtigung hinzufügen. Benutzer mit Rechten auf der Root-Ebene haben Zugriff auf globale Daten auf vCenter Server, wie z. B. Rollen, benutzerdefinierte Attribute und vCenter Server-Einstellungen.
- Ziehen Sie die Aktivierung der Weitergabe in Betracht, wenn Sie einem Objekt Berechtigungen zuweisen. Durch die Weitergabe wird sichergestellt, dass neue Objekte in der Objekthierarchie Berechtigungen erben. Sie können z. B. eine Berechtigung zu einem Ordner der virtuellen Maschine zuweisen und die Weitergabe aktivieren, um sicherzustellen, dass die Berechtigung für alle virtuellen Maschinen im Ordner gilt.
- Verwenden Sie die Rolle „Kein Zugriff“, um bestimmte Bereiche der Hierarchie zu maskieren. Die Rolle „Kein Zugriff“ beschränkt den Zugriff auf die Benutzer oder Gruppen mit dieser Rolle. Im Fall von VMs und vAPPs gibt es jedoch zwei Weitergabeketten für Berechtigungen. Das Zuweisen einer weitergegebenen Berechtigung mit der Rolle „Kein Zugriff“ für eine der Ketten bedeutet nicht, dass die entsprechende vApp oder VM über keine Berechtigungen verfügt, die an sie weitergegeben werden.
- Änderungen an Lizenzen werden an alle verknüpften vCenter Server-Systeme in derselben vCenter Single Sign On-Domäne weitergegeben.
- Die Lizenzweitergabe erfolgt selbst dann, wenn der Benutzer nicht über Rechte auf allen vCenter Server-Systemen verfügt.

Erforderliche vCenter Server-Rechte für allgemeine Aufgaben

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

In der folgenden Tabelle werden allgemeine Aufgaben aufgelistet, die mehr als eine Berechtigung erfordern. Sie können Berechtigungen zu Bestandslistenobjekten hinzufügen, indem Sie einen Benutzer mit einer der vordefinierten Rollen oder mit mehreren Berechtigungen koppeln. Wenn Sie davon ausgehen, dass Sie eine Reihe von Rechten mehrmals zuweisen müssen, erstellen Sie benutzerdefinierte Rollen. Weitere Informationen zu den erforderlichen Rechten für allgemeine Aufgaben finden Sie unter Verwenden des Rechte-Recorders.

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

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

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

Tabelle 2-6. Erforderliche Berechtigungen für allgemeine Aufgaben

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

Tabelle 2-6. Erforderliche Berechtigungen für allgemeine Aufgaben (Fortsetzung)

Aufgabe	Erforderliche Berechtigungen	Gültige Rolle
Virtuelle Maschine aus einer Vorlage bereitstellen	Im Zielordner oder Datencenter: ■ **Virtuelle Maschine.Bestandsliste bearbeiten.Aus vorhandener erstellen** ■ **Virtuelle Maschine.Konfiguration ändern.Neue Festplatte hinzufügen**	Administrator
	In einer Vorlage oder einem Vorlagenordner: **Virtuelle Maschine.Bereitstellung.Vorlage bereitstellen**	Administrator
	Auf dem Zielhost, -cluster oder -ressourcenpool: ■ **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen** ■ **vApp.Importieren**	Administrator
	Auf dem Zieldatenspeicher oder -datenspeicherordner: **Datenspeicher.Speicher zuteilen**	Datenspeicherkonsument oder Administrator
	Im Netzwerk, dem die virtuelle Maschine zugewiesen wird: **Netzwerk.Netzwerk zuweisen**	Netzwerkkonsument oder Administrator
Erstellen eines Snapshots der virtuellen Maschine	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: **Virtuelle Maschine.Snapshot-Verwaltung.Snapshot erstellen**	Hauptbenutzer virtueller Maschinen oder Administrator
Verschieben einer virtuellen Maschine in einen Ressourcenpool	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: ■ **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen** ■ **Virtuelle Maschine.Bestandsliste bearbeiten.Verschieben**	Administrator
	Auf dem Zielressourcenpool: **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen**	Administrator
Installieren eines Gastbetriebssystems auf einer virtuellen Maschine	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: ■ **Virtuelle Maschine.Interaktion.Frage beantworten** ■ **Virtuelle Maschine.Interaktion.Konsoleninteraktion** ■ **Virtuelle Maschine.Interaktion.Geräteverbindung** ■ **Virtuelle Maschine.Interaktion.Ausschalten** ■ **Virtuelle Maschine.Interaktion.Einschalten** ■ **Virtuelle Maschine.Interaktion.Zurücksetzen** ■ **Virtuelle Maschine.Interaktion.CD-Medien konfigurieren** (wenn von einer CD installiert wird) ■ **Virtuelle Maschine.Interaktion.Diskettenmedien konfigurieren** (wenn von einer Diskette installiert wird) ■ **Virtuelle Maschine.Interaktion.VMware Tools installieren**	Hauptbenutzer virtueller Maschinen oder Administrator

Tabelle 2-6. Erforderliche Berechtigungen für allgemeine Aufgaben (Fortsetzung)

Aufgabe	Erforderliche Berechtigungen	Gültige Rolle
	Auf einem Datenspeicher, der das Installationsmedium mit dem ISO-Image enthält: **Datenspeicher.Datenspeicher durchsuchen** (wenn von einem ISO-Image auf einem Datenspeicher installiert wird) Auf dem Datenspeicher, auf den Sie das ISO-Image des Installationsmediums hochladen: ■ **Datenspeicher.Datenspeicher durchsuchen** ■ **Datenspeicher.Dateivorgänge auf niedriger Ebene**	Hauptbenutzer virtueller Maschinen oder Administrator
Migrieren einer virtuellen Maschine mit vMotion	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: ■ **Ressourcen.Eingeschaltete virtuelle Maschine migrieren** ■ **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen** (wenn das Ziel ein anderer Ressourcenpool als die Quelle ist)	Ressourcenpool-Administrator oder Administrator
	Auf dem Zielhost, -cluster oder -ressourcenpool (wenn anders als die Quelle): **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen**	Ressourcenpool-Administrator oder Administrator
Cold-Migration (Verlagern) einer virtuellen Maschine	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: ■ **Ressourcen.Ausgeschaltete virtuelle Maschine migrieren** ■ **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen** (wenn das Ziel ein anderer Ressourcenpool als die Quelle ist)	Ressourcenpool-Administrator oder Administrator
	Auf dem Zielhost, -cluster oder -ressourcenpool (wenn anders als die Quelle): **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen**	Ressourcenpool-Administrator oder Administrator
	Auf dem Zieldatenspeicher (wenn anders als die Quelle): **Datenspeicher.Speicher zuteilen**	Datenspeicherkonsument oder Administrator
Migrieren einer virtuellen Maschine mit Storage vMotion	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: **Ressourcen.Eingeschaltete virtuelle Maschine migrieren**	Ressourcenpool-Administrator oder Administrator
	Auf dem Zieldatenspeicher: **Datenspeicher.Speicher zuteilen**	Datenspeicherkonsument oder Administrator
Einen Host in einen Cluster verschieben	Auf dem Host: **Host.Bestandsliste.Host zu Cluster hinzufügen**	Administrator
	Auf dem Zielcluster: ■ **Host.Bestandsliste.Host zu Cluster hinzufügen** ■ **Host.Bestandsliste.Cluster ändern**	Administrator
Hinzufügen eines einzelnen Hosts zu einem Datencenter mithilfe des	Auf dem Host: **Host.Bestandsliste.Host zu Cluster hinzufügen**	Administrator

Tabelle 2-6. Erforderliche Berechtigungen für allgemeine Aufgaben (Fortsetzung)

Aufgabe	Erforderliche Berechtigungen	Gültige Rolle
vSphere Client oder Hinzufügen eines einzelnen Hosts zu einem Cluster mithilfe der PowerCLI oder API (Nutzung der addHost-API)	Auf dem Cluster: ■ **Host.Bestandsliste.Cluster ändern** ■ **Host.Bestandsliste.Host zu Cluster hinzufügen**	Administrator
	Im Datencenter: **Host.Bestandsliste.Eigenständigen Host hinzufügen**	Administrator
Hinzufügen mehrerer Hosts zu einem Cluster	Auf dem Cluster: ■ **Host.Bestandsliste.Cluster ändern** ■ **Host.Bestandsliste.Host zu Cluster hinzufügen**	Administrator
	Im übergeordneten Datencenter des Clusters (mit Weitergabe): ■ **Host.Bestandsliste.Eigenständigen Host hinzufügen** ■ **Host.Bestandsliste.Host verschieben** ■ **Host.Bestandsliste.Cluster ändern** ■ **Host.Konfiguration.Wartung**	Administrator
Verschlüsseln einer virtuellen Maschine	Eine Verschlüsselung ist nur in Umgebungen mit vCenter Server möglich. Zusätzlich muss für die meisten Verschlüsselungsaufgaben bei dem ESXi-Host der Verschlüsselungsmodus aktiviert sein. Der Benutzer, der diese Aufgaben durchführt, muss über die entsprechenden Berechtigungen verfügen. Eine Gruppe von Berechtigungen für **Kryptografievorgänge** ermöglicht eine detaillierte Steuerung. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für VM-Verschlüsselungsaufgaben.	Administrator
Schützen einer virtuellen Maschine (bei Verwendung von vSphere+ zum Schutz der virtuellen Maschine)	Im Datencenter, in dem die virtuelle Maschine bereitgestellt wird: ■ **vSphere Tagging.vSphere Tag zuweisen oder Zuweisung aufheben**	Administrator

Sichern der ESXi-Hosts

3

Die ESXi-Hypervisorarchitektur verfügt über viele integrierte Sicherheitsfunktionen wie CPU-Isolierung, Arbeitsspeicherisolierung und Geräteisolierung. Sie können Funktionen wie Sperrmodus, Zertifikatersetzung und Smartcard-Authentifizierung für verbesserte Sicherheit konfigurieren.

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

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

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

Ab vSphere 8.0 Update 1 führt ESXi zwei Reverse-Proxy-Dienste aus:

- VMware-Reverse-Proxy-Dienst, `rhttpproxy`
- Envoy

Envoy belegt Port 443, und alle eingehenden ESXi-Anfragen werden über Envoy weitergeleitet. Ab vSphere 8.0 Update 1 dient rhttpproxy als Konfigurationsverwaltungsserver für Envoy.

Lesen Sie als Nächstes die folgenden Themen:

- Allgemeine ESXi-Sicherheitsempfehlungen
- Verwalten von Zertifikaten für ESXi-Hosts
- Anpassen der ESXi-Hostsicherheit
- Zuweisen von Rechten für ESXi-Hosts
- Verwenden von Active Directory zum Verwalten von ESXi-Benutzern
- Verwenden des vSphere Authentication Proxy

- Konfigurieren und Verwalten der Smartcard-Authentifizierung für ESXi
- Verwenden der ESXi Shell
- UEFI Secure Boot für ESXi-Hosts
- Sichern von ESXi-Hosts mit Trusted Platform Module
- ESXi-Protokolldateien
- Sichern des Fault Tolerance-Protokollierungsdatenverkehrs
- Verwalten von ESXi-Überwachungsdatensätzen
- Sichern der ESXi-Konfiguration
- Deaktivieren der internen Laufzeitoption „execInstalledOnly“

Allgemeine ESXi-Sicherheitsempfehlungen

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

Was sind die integrierten ESXi-Sicherheitsfunktionen?

ESXi minimiert die Risiken für Ihre Hosts wie folgt:

- Die ESXi Shell-Schnittstelle und die SSH-Schnittstelle sind standardmäßig deaktiviert. Aktivieren Sie diese Schnittstellen erst, wenn Fehlerbehebungs- oder Supportaktivitäten durchgeführt werden müssen. Verwenden Sie für die täglichen Aktivitäten den vSphere Client, wobei die Aktivität der rollenbasierten Zugriffssteuerung und modernen Zugriffssteuerungsmethoden unterliegt.
- Nur einige Firewallports sind standardmäßig geöffnet. Sie können explizit Firewallports öffnen, die mit speziellen Diensten verknüpft sind.
- Standardmäßig sind alle Ports, die nicht für den Verwaltungszugriff auf den Host notwendig sind, geschlossen. Öffnen Sie Ports, falls Sie zusätzliche Dienste benötigen.
- 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 schwache Schlüssel deaktiviert und die Kommunikation der Clients wird durch SSL gesichert. Die genauen Algorithmen, die zum Sichern des Kanals verwendet werden, hängen vom SSL-Handshake ab. In ESXi erstellte Standardzertifikate verwenden PKCS#1 SHA-256 mit RSA-Verschlüsselung als Signaturalgorithmus.

- Ein interner Webdienst wird von ESXi zur Unterstützung des Zugriffs durch Webclients verwendet. Der Dienst wurde geändert, um nur Funktionen auszuführen, die ein Webclient für die Verwaltung und Überwachung benötigt. Daher ist ESXi nicht von den Webdienst-Sicherheitslücken betroffen, die für Tomcat in weiter gefassten Anwendungsbereichen gemeldet wurden.
- VMware überwacht alle Sicherheitswarnungen, die die Sicherheit von ESXi beeinträchtigen können, und gibt ggf. einen Sicherheits-Patch aus. Um Sicherheitswarnungen zu erhalten, können Sie die Mailingliste „VMware Security Advisories and Security Alerts“ abonnieren. Weitere Informationen finden Sie auf der Webseite unter http://lists.vmware.com/mailman/listinfo/security-announce.
- Unsichere Dienste, wie z. B. FTP und Telnet sind nicht installiert, und die Ports für diese Dienste sind standardmäßig geschlossen.
- Verwenden Sie UEFI Secure Boot, damit Hosts keine Treiber und Anwendungen laden können, die nicht kryptografisch signiert sind. Die Aktivierung von Secure Boot erfolgt im System-BIOS. Auf dem ESXi-Host sind keine zusätzlichen Konfigurationsänderungen erforderlich, z. B. für Festplattenpartitionen. Weitere Informationen hierzu finden Sie unter UEFI Secure Boot für ESXi-Hosts.
- Wenn Ihr ESXi-Host über einen TPM 2.0-Chip verfügt, aktivieren und konfigurieren Sie diesen im System-BIOS. In Zusammenarbeit mit Secure Boot bietet TPM 2.0 verbesserte Sicherheit und vertrauenswürdige Zuverlässigkeit, die in der Hardware verankert ist. Weitere Informationen hierzu finden Sie unter Sichern von ESXi-Hosts mit Trusted Platform Module.
- In ESXi 8.0 und höher können Sie den SSH-Prozess unter einer Sandbox-Domäne ausführen. Die Shell verfügt dann über eingeschränkte Berechtigungen und lässt nur den Zugriff auf eine begrenzte Teilmenge von Befehlen zu. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/87386.

Ergreifen weiterer ESXi-Sicherheitsmaßnahmen

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

Begrenzen des Zugriffs auf ESXi-Hosts

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 ESXi-Hosts zu

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

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

Verwenden Sie DCUI nur für die Fehlerbehebung

Greifen Sie als Root-Benutzer nur zur Fehlerbehebung von der DCUI oder der ESXi Shell auf den Host zu. Um Ihre ESXi-Hosts zu verwalten, verwenden Sie den vSphere Client (oder den VMware Host Client) oder eine der VMware-CLIs oder -APIs. Weitere Informationen hierzu finden Sie unter *ESXCLI – Konzepte und Beispiele*. Wenn Sie die ESXi Shell oder SSH verwenden, sollten Sie die zugriffsberechtigten Konten beschränken und Zeitüberschreitungswerte festlegen.

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

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

Hinweis Beachten Sie die Sicherheitshinweise von VMware unter http://www.vmware.com/security/.

ESXi – Erweiterte Systemeinstellungen

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

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

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

Erweiterte Systemeinstellung	Beschreibung	Standardwert
Annotations.WelcomeMessage	Zeigt vor der Anmeldung eine Begrüßungsnachricht im Host Client oder in der DCUI auf dem Standardbildschirm an. In der DCUI ersetzt die Begrüßungsnachricht Text, wie z. B. die IP-Adresse des Hosts.	(Leer)
Config.Etc.issue	Zeigt während einer SSH-Anmeldesitzung ein Banner an.	(Leer)

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

Erweiterte Systemeinstellung	Beschreibung	Standardwert
Config.Etc.motd	Zeigt die Meldung des Tages bei der SSH-Anmeldung an. **Hinweis** Um neue Zeilen oder Zeilenumbrüche in die Probleme und motd-Konfigurationen einzufügen, können Sie sowohl die vSphere API als auch die CLI verwenden. Beispiele dafür finden Sie unter https://williamlam.com/2021/03/adding-a-customized-notification-banner-in-the-vsphere-ui.html und https://williamlam.com/2015/02/easily-manage-esxi-vcsa-ssh-login-banner-motd-in-vsphere-6-0.html.	(Leer)
Config.HostAgent.vmacore.soap.sessionTimeout	Legt die Leerlaufzeit in Minuten fest, bevor das System eine VIM-API automatisch abmeldet. Mit dem Wert 0 (Null) wird die Leerlaufzeit deaktiviert. Diese Einstellung gilt nur für neue Sitzungen.	30 (Minuten)
Mem.MemEagerZero	Aktiviert das unwiderrufliche Löschen (Page Zeroing) der Benutzer-World- und Gastarbeitsspeicherseiten in den VMkernel-Betriebssystemen (einschließlich des VMM-Prozesses) nach dem Beenden einer virtuellen Maschine. Der Standardwert (0) verwendet Lazy Zeroing. Der Wert 1 verwendet Eager Zeroing.	0 (deaktiviert)

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

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

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

Erweiterte Systemeinstellung	Beschreibung	Standardwert
Security.PasswordHistory	Gibt die Anzahl der für jeden Benutzer zu speichernden Kennwörter an. Diese Einstellung verhindert doppelte oder ähnliche Kennwörter.	5
Security.PasswordMaxDays	Legt die maximale Anzahl an Tagen zwischen Kennwortänderungen fest.	99999
Security.PasswordQualityControl	Ändert die erforderliche Länge und die erforderliche Zeichenklasse oder erlaubt Kennwortsätze in der `Pam_passwdqc`-Konfiguration. Sie können Sonderzeichen in Kennwörtern verwenden. Kennwortlängen von mindestens 15 Zeichen sind möglich. Die Standardeinstellung erfordert drei Zeichenklassen und eine Mindestlänge von sieben Zeichen. Bei der Implementierung des DoD-Anhangs können Sie die Option `similar=deny` mit einer Kennwortmindestlänge kombinieren und die Anforderung durchsetzen, dass Kennwörter ausreichend unterschiedlich sind. Die Einstellung für den Kennwortverlauf wird nur für Kennwörter erzwungen, die über die VIM-API `LocalAccountManager.changePassword` geändert wurden. Zum Ändern des Kennworts muss der Benutzer über Administratorberechtigungen verfügen. Die Einstellung „PasswordQualityControl“ mit der Einstellung „PasswordMaxDays“ erfüllt die Anforderungen des DoD-Anhangs: `min=disabled,disabled,disabled,disabled,15 similar=deny`	retry=3 min=disabled,disabled,disabled, 7,7

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

Erweiterte Systemeinstellung	Beschreibung	Standardwert
UserVars.DcuiTimeOut	Legt die Leerlaufzeit in Sekunden fest, bevor das System die DCUI automatisch abmeldet. Mit dem Wert 0 (Null) wird die Zeitüberschreitung deaktiviert.	600 (10 Minuten)
UserVars.ESXiShellInteractiveTimeOut	Legt die Leerlaufzeit in Sekunden fest, bevor das System eine interaktive Shell automatisch abmeldet. Diese Einstellung wird nur für neue Sitzungen wirksam. Mit dem Wert 0 (Null) wird die Leerlaufzeit deaktiviert. Gilt sowohl für die DCUI als auch für die SSH-Shell.	0
UserVars.ESXiShellTimeOut	Legt die Zeit in Sekunden fest, die eine Anmelde-Shell auf die Anmeldung wartet. Mit dem Wert 0 (Null) wird die Zeitüberschreitung deaktiviert. Gilt sowohl für die DCUI als auch für die SSH-Shell.	0
UserVars.HostClientSessionTimeout	Legt die Leerlaufzeit in Sekunden fest, bevor das System den Host Client automatisch abmeldet. Mit dem Wert 0 (Null) wird die Leerlaufzeit deaktiviert.	900 (15 Minuten)
UserVars.HostClientWelcomeMessage	Zeigt bei der Anmeldung eine Begrüßungsnachricht im Host Client an. Die Nachricht wird nach der Anmeldung als „Hinweis“ angezeigt.	(Leer)

Konfigurieren von ESXi-Hosts mit Hostprofilen

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

Hostprofile stellen einen automatisierten und zentral verwalteten Mechanismus für die Hostkonfiguration und Konfigurationsübereinstimmung dar. Hostprofile können die Effizienz steigern, indem die Abhängigkeit von sich wiederholenden, manuellen Aufgaben reduziert wird. Hostprofile erfassen die Konfiguration eines vorkonfigurierten und validierten Referenzhosts, speichern die Konfiguration als verwaltetes Objekt und verwenden den darin enthaltenen Parametersatz, um das Netzwerk, den Speicher, die Sicherheit und andere Parameter auf Hostebene zu konfigurieren.

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

Verwalten von ESXi-Hostkonfigurationseinstellungen mithilfe von Skripts

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

vSphereumfasst mehrere Skriptsprachen für die ESXi-Hostverwaltung. VMware PowerCLI ist eine Windows PowerShell-Schnittstelle zur vSphere-API und enthält PowerShell-cmdlets für die Verwaltung von vSphere-Komponenten. ESXCLI enthält eine Reihe von Befehlen für die Verwaltung von ESXi-Hosts und virtuellen Maschinen. Unter https://developer.vmware.com finden Sie Referenzinformationen und Programmiertipps. Die vSphere-Administratordokumentation behandelt die Verwendung des vSphere Client für die Verwaltung.

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

Verfahren

1 Erstellen Sie eine benutzerdefinierte Rolle mit eingeschränkten Berechtigungen.

   Weitere Informationen finden Sie unter Erstellen einer benutzerdefinierten vCenter Server-Rolle.

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

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

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

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

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

Sprache	Befehle

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

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

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

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

Kennwörter und Kontosperrung für ESXi

Für ESXi-Hosts müssen Sie ein Kennwort mit vordefinierten Anforderungen verwenden. Mithilfe der erweiterten Systemeinstellung `Security.PasswordQualityControl` können Sie die erforderliche Länge und die erforderliche Zeichenklasse ändern sowie Kennwortsätze erlauben.

Sie können auch die Anzahl der Kennwörter festlegen, die für jeden Benutzer gespeichert werden soll. Verwenden Sie dazu die erweiterte Systemeinstellung `Security.PasswordHistory`.

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

ESXi-Kennwörter

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

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

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

Beispiele für ESXi-Kennwörter

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

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

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

Mit diesen Einstellungen sind die folgenden Kennwörter zulässig.

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

Die folgenden Beispielkennwörter entsprechen nicht den Anforderungen.

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

ESXi-Kennwortsatz

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

Beispielsweise können Sie diese Option wie folgt ändern.

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

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

Ändern der standardmäßigen Kennwortbeschränkungen

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

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

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

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

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

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

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

ESXi-Kontosperrverhalten

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

Konfigurieren des Anmeldeverhaltens

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

- `Security.AccountLockFailures`. Maximal zulässige Anzahl fehlgeschlagener Anmeldeversuche, bevor das Konto eines Benutzers gesperrt wird. Mit dem Wert „0“ wird das Sperren von Konten deaktiviert.
- `Security.AccountUnlockTime`. Die Anzahl der Sekunden, die ein Benutzer gesperrt wird.
- `Security.PasswordHistory`. Anzahl der für jeden Benutzer zu speichernden Kennwörter. Ab vSphere 8.0 Update 1 ist die Standardeinstellung fünf. Mit dem Wert „0“ wird der Kennwortverlauf deaktiviert.

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

Erzeugung des kryptografischen Schlüssels in ESXi

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

TLS-Schlüssel (Transport Layer Security)

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

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

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

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

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

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

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

SSH-Schlüssel

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

Die öffentlichen SSH-Schlüssel befinden sich in folgendem Speicherort:

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

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

Die privaten SSH-Schlüssel befinden sich in folgendem Speicherort:

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

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

Erstellung des kryptografischen TLS-Schlüssels

Die Konfiguration der Einrichtung des kryptografischen TLS-Schlüssels wird durch die Auswahl von TLS-Verschlüsselungs-Suites gesteuert, die ECC-basierte Schlüsselvereinbarungen mithilfe von Ecliptic Curve Diffie Hellman (ECDH) (gemäß NIST Special Publication 800-56A) auswählt.

Erstellung des kryptografischen SSH-Schlüssels

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

SSH-Sicherheit in ESXi

Die ESXi Shell-Schnittstelle und die SSH-Schnittstelle sind standardmäßig deaktiviert. Aktivieren Sie diese Schnittstellen erst, wenn Fehlerbehebungs- oder Supportaktivitäten durchgeführt werden müssen. Verwenden Sie für regelmäßige Aktivitäten den vSphere Client, wobei die Aktivitäten den Methoden der rollenbasierten und modernen Zugriffssteuerung unterliegen.

SSH-Konfiguration in ESXi

Die SSH-Konfiguration in ESXi verwendet die folgenden Einstellungen:

Version 1 SSH-Protokoll deaktiviert

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

Verbesserte Schlüsselqualität

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

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

ESXi-SSH-Schlüssel

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

Sie können HTTPS PUT verwenden, um den SSH-Schlüssel auf den Host zu kopieren.

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

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

Hochladen eines SSH-Schlüssels anhand von HTTPS PUT

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

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

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

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

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

Verfahren

1. Öffnen Sie die Schlüsseldatei in der Anwendung, die Sie für das Hochladen verwenden.
2. Veröffentlichen Sie die Datei an den folgenden Speicherorten.

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

PCI- und PCIe-Geräte sowie ESXi

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

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

Ihr Host ist möglicherweise auf eine der folgenden Weisen gefährdet.

- Das Gastbetriebssystem generiert möglicherweise einen nicht behebbaren PCI- oder PCIe-Fehler. Ein solcher Fehler beschädigt keine Daten, kann aber zum Absturz des ESXi-Hosts führen. Solche Fehler können aufgrund von Fehlern bzw. Inkompatibilitäten in den Hardwaregeräten auftreten, für die das Passthrough durchgeführt wird. Zu den weiteren Fehlergründen gehören Probleme mit Treibern im Gastbetriebssystem.
- Das Gastbetriebssystem startet möglicherweise einen DMA-Vorgang, der einen IOMMU-Seitenfehler auf dem ESXi-Host verursacht. Dieser Vorgang ist möglicherweise das Ergebnis eines DMA-Vorgangs, der eine Adresse außerhalb des virtuellen Maschinenspeichers anvisiert. Auf einigen Maschinen konfiguriert Host-Firmware IOMMU-Fehler, um durch ein nicht maskierbares Interrupt (NMI) einen schweren Fehler zu melden. Dieser schwerwiegende Fehler verursacht einen Absturz des ESXi-Hosts. Dieses Problem kann aufgrund von Problemen mit den Treibern im Gastbetriebssystem auftreten.
- Wenn das Betriebssystem auf dem ESXi-Host nicht das Neuzuordnen von Interrupts verwendet, injiziert das Gastbetriebssystem möglicherweise einen störenden Interrupt in den ESXi-Host auf einem beliebigen Vektor. ESXi verwendet derzeit das Neuzuordnen von Interrupts auf den Intel-Plattformen, wo diese Funktion verfügbar ist. Das Neuzuordnen von Interrupts stellt einen Teil des Intel VT-d-Funktionssatzes dar. ESXi verwendet das Neuzuordnen von Interrupts nicht auf AMD-Plattformen. Falsche Interrupts können zum Absturz des ESXi-Hosts führen. Theoretisch kann es weitere Möglichkeiten geben, diese fehlerhaften Interrupts auszunutzen.

Deaktivieren des vSphere-Browsers für verwaltete Objekte

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

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

Verfahren

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

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

ESXi-Netzwerksicherheitsempfehlungen

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

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

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

Ändern von ESXi-Web-Proxy-Einstellungen

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

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

- Richten Sie keine Zertifikate ein, in denen Kennwörter oder Kennwortsätze verwendet werden. ESXi unterstützt keine Web-Proxys mit Kennwörtern oder Kennwortsätzen (verschlüsselte Schlüssel). Wenn Sie einen Web-Proxy einrichten, der ein Kennwort oder einen Kennwortsatz benötigt, können die ESXi-Prozesse nicht korrekt gestartet werden.

- Zur Unterstützung von Verschlüsselung für Benutzernamen, Kennwörter und Pakete wird SSL standardmäßig für vSphere Web Services SDK-Verbindungen aktiviert. Wenn Sie diese Verbindungen so konfigurieren möchten, dass Übertragungen nicht verschlüsselt werden, deaktivieren Sie SSL für Ihre vSphere Web Services SDK-Verbindung, indem Sie die Verbindung von HTTPS auf HTTP umstellen.

  Deaktivieren Sie SSL nur dann, wenn Sie eine vollständig vertrauenswürdige Umgebung für die Clients geschaffen haben, d. h. Firewalls wurden installiert und die Übertragungen zum und vom Host sind vollständig isoliert. Die Deaktivierung von SSL kann die Leistung verbessern, da der für die Verschlüsselung notwendige Verarbeitungsaufwand nicht anfällt.
- Um den Missbrauch von ESXi-Diensten zu verhindern, kann auf die meisten internen ESXi-Dienste nur über Port 443, den für HTTPS-Übertragungen verwendeten Port, zugegriffen werden. Port 443 dient als Reverse-Proxy für ESXi. Sie können eine Liste der Dienste auf dem ESXi-Host auf einer HTTP-Begrüßungsseite sehen. Sie können direkt aber nur auf die Speicheradapterdienste zugreifen, wenn Sie über die entsprechenden Berechtigungen verfügen.

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

vSphere Auto Deploy-Sicherheitsüberlegungen

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

Netzwerksicherheit

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

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

Start-Image- und Hostprofilsicherheit

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

- Das Start-Image enthält immer die VIB-Pakete, aus denen das Image-Profil besteht.

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

    Verwenden Sie den vSphere Authentication Proxy, um zu verhindern, dass die Active Directory-Kennwörter offengelegt werden. Wenn Sie Active Directory mithilfe von Hostprofilen einrichten, werden die Kennwörter nicht geschützt.
- Die öffentlichen und privaten SSL-Schlüssel und das Zertifikat des Hosts sind im Start-Image enthalten.

Steuern des Zugriffs für CIM-basierte Hardwareüberwachungstools

Das CIM-System (Common Information Model) bietet eine Schnittstelle für Remote-Anwendungen zur Überwachung von Hardwareressourcen mithilfe eines Satzes von Standard-APIs. Um die Sicherheit der CIM-Schnittstelle sicherzustellen, sollten Sie diesen Remoteanwendungen nur den nötigen Mindestzugriff einräumen. Wenn Sie eine Remoteanwendung mit einem Root- oder Administratorkonto bereitstellen und die Anwendung manipuliert wird, besteht für die virtuelle Umgebung ein Sicherheitsrisiko.

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

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

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

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

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

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

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

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

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

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

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

Verfahren

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

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

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

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

3. Verlängern Sie das Ticket gegebenenfalls alle zwei Minuten.

Empfohlene Vorgehensweisen für die Sicherheit von vSphere Distributed Services Engine

Um die Sicherheit Ihrer ESXi-Umgebung zu maximieren, befolgen Sie die Best Practices für vSphere Distributed Services Engine.

Ab vSphere 8.0 ermöglicht vSphere Distributed Services Engine das Auslagern von Infrastrukturfunktionen von den CPUs eines Hosts oder eines Servers auf Datenverarbeitungseinheiten (DPUs, auch als SmartNICs bezeichnet), wodurch CPU-Zyklen für die Bereitstellung von Anwendungen freigegeben werden. Eine Einführung in vSphere Distributed Services Engine finden Sie in der *Installation und Einrichtung von VMware ESXi*-Dokumentation. Weitere Informationen zu vSphere Distributed Services Engine finden Sie in der *Verwalten des Lebenszyklus von Host und Cluster*-Dokumentation.

Grundsätzlich sollten Sie die Sicherheitsaspekte von vSphere Distributed Services Engine genauso behandeln wie die Sicherung Ihrer ESXi-Umgebung.

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

Steuern der ESXi-Entropie

In ESXi 8.0 und höher unterstützt die Implementierung der ESXi-Entropie die FIPS 140-3- und EAL4-Zertifizierungen. Kernel-Startoptionen steuern, welche Entropiequellen auf einem ESXi-Host aktiviert werden sollen.

Beim Computing bezieht sich der Begriff „Entropie“ auf zufällige Zeichen und Daten, die für die Verwendung in der Kryptografie erfasst werden, wie z. B. das Generieren von Verschlüsselungsschlüsseln zur Sicherung über ein Netzwerk übertragener Daten. Entropie ist für die Sicherheit erforderlich, um Schlüssel zu generieren und sicher über das Netzwerk zu kommunizieren. Entropie wird häufig aus einer Vielzahl von Quellen auf einem System erfasst.

Die Verwendung der FIPS-Entropie ist das Standardverhalten, wenn die folgenden Bedingungen zutreffen.

1 Die Hardware unterstützt RDSEED.

2 Die VMkernel-Startoption „disableHwrng“ ist nicht vorhanden oder FALSE.

3 Die VMkernel-Startoption „entropySources“ ist nicht vorhanden, 0 (Null) oder 4.

Warnung Wenn Sie einen ESXi-Host mit entropySources nur für externe Entropie konfigurieren (das heißt, entropySources ist auf 8 festgelegt), müssen Sie die externe Entropie weiterhin mithilfe der Entropie-API für den Host bereitstellen. Wenn die Entropie auf dem Host ausgeschöpft ist, reagiert der Host nicht mehr. Um diese Situation zu beheben, starten Sie den Host neu. Wenn der Host immer noch nicht reagiert, müssen Sie ESXi neu installieren.

Ab ESXi 8.0 Update 1 können Sie externe Entropiequellen in der Kickstart-Datei für die Skriptinstallation konfigurieren. Sie können ESXi in einer Hochsicherheitsumgebung so konfigurieren, dass Entropie aus externen Entropiequellen wie einem HSM (Hardware Security Module) verbraucht und unter Verwendung der skriptbasierten Installationsmethode ein Abgleich mit Standards wie BSI Common Criteria, EAL4 und NIST FIPS CMVP durchgeführt wird. Weitere Informationen zur Konfiguration von externen Entropiequellen finden Sie in der Dokumentation zu *Installation und Einrichtung von VMware ESXi*.

Sie können das ESXi-Entropie-Subsystem mithilfe der folgenden VMkernel-Startoptionen konfigurieren:

Tabelle 3-2. ESXi-Entropie – VMkernel-Startoptionen

VMkernel-Startoption	Optionstyp	Beschreibung	Standardwert
disableHwrng (verfügbar vor vSphere 8.0)	Boolean	Deaktiviert die RDRAND- und RDSEED-Entropiequellen, wenn diese auf TRUE festgelegt sind (überschreibt „entropySources“).	FALSE Aktiviert die Entropiequellen des Hardware-Zufallszahlengenerators, falls vorhanden.
entropySources (verfügbar ab vSphere 8.0)	Ganzzahl, Bitmaske	Gibt an, welche Entropiequellen aktiviert werden sollen. ■ 0 (Standard) Bitmaskenwerte: ■ 1=Interrupts ■ 2=RDRAND ■ 4=RDSEED ■ 8=entropyd (die Verwendung von EAL4-Entropie ist aktiviert) Durch die Angabe von entropySources=9 werden die Interrupts und die Userspace-Entropiequellen aktiviert und die Entropiequellen „RDRAND“ und „RDSEED“ deaktiviert.	0 (Null) Wenn RDSEED unterstützt wird, lautet die Standardeinstellung FIPS-Konformität. Andernfalls werden standardmäßig alle Entropiequellen außer entropyd verwendet.

Hinweis Bevor Sie eine Änderung vornehmen, um nur RDRAND-, RDSEED- oder beide Entropiequellen zu verwenden, überprüfen Sie die Dokumentation Ihres Anbieters, um sicherzustellen, dass Ihr ESXi-Host diese Konfigurationen unterstützt. Wenn Ihr Host diese Konfigurationen nicht unterstützt, benachrichtigt vCenter Server Sie mit einer Warnung, und der Host verwendet die Interrupt- und Userspace-Entropiequellen.

Voraussetzungen

Sie müssen auf dem ESXi-Host über Root-Zugriff verfügen.

Verfahren

1 Verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung auf dem ESXi-Host zu starten.

2 Melden Sie sich als „root“ an.

3 Legen Sie die gewünschten Entropie-VMkernel-Startoptionen fest.

   a So deaktivieren Sie die RDRAND- und RDSEED-Entropiequellen für „disableHwrng“:

   ```
   esxcli system settings kernel set -s disableHwrng -v TRUE
   ```

   b So legen Sie „entropySources“ fest:

   ```
   esxcli system settings kernel set -s entropySources -v entropy_source_value
   ```

   Die Werte, die Sie für „entropySources“ festlegen können, finden Sie in der obigen Tabelle.

Verwalten von Zertifikaten für ESXi-Hosts

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

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

Ab vSphere 8.0 Update 3 können Sie ESXi-Zertifikate ersetzen, ohne den Host in den Wartungsmodus zu versetzen und ohne den Host oder einzelne Dienste neu starten zu müssen.

Zertifikate und Zertifikatmodi

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

vCenter Server unterstützt die folgenden Zertifikate und Zertifikatmodi für ESXi-Hosts.

Tabelle 3-3. Zertifikatmodi für ESXi-Hosts

Zertifikatmodus	Beschreibung
VMware Certificate Authority (Standard)	Standardmäßig wird die VMware Certificate Authority als Zertifizierungsstelle (Certificate Authority, CA) für ESXi-Hostzertifikate verwendet. VMCA ist standardmäßig die Root-Zertifizierungsstelle, kann aber als Zwischenzertifizierungsstelle für eine andere Zertifizierungsstelle eingerichtet werden. Im **VMCA**-Modus können Sie Zertifikate von vSphere Client erneuern und aktualisieren. Er wird auch verwendet, wenn VMCA ein untergeordnetes Zertifikat ist.
Benutzerdefinierte Zertifizierungsstelle	Verwenden Sie diesen Modus, wenn Sie ausschließlich benutzerdefinierte, von einer Drittanbieter- oder Unternehmens-Zertifizierungsstelle signierte Zertifikate verwenden möchten. Im Modus **Benutzerdefiniert** sind Sie für die Verwaltung der Zertifikate verantwortlich. Ab vSphere 8.0 Update 3 können Sie benutzerdefinierte Zertifikate über vSphere Client verwalten. **Hinweis** Wenn Sie den Zertifikatmodus nicht zu „Benutzerdefinierte Zertifizierungsstelle“ (**Benutzerdefiniert**) ändern, kann VMCA benutzerdefinierte Zertifikate ersetzen, beispielsweise wenn Sie in vSphere Client die Option **Verlängern** auswählen.
Fingerabdruckmodus	vSphere 5.5 verwendete den **Fingerabdruck**-Modus, und dieser Modus ist in vSphere 6.x nach wie vor als Notfallmodus verfügbar. In diesem Modus prüft vCenter Server, ob das Zertifikat korrekt formatiert ist, jedoch nicht die Gültigkeit des Zertifikats. Selbst abgelaufene Zertifikate werden akzeptiert. Verwenden Sie diesen Modus nur, wenn Sie auf Probleme stoßen, die in den anderen beiden Modi nicht zu beheben sind. Einige Dienste aus vCenter Server 6.x und höher funktionieren möglicherweise im Fingerabdruckmodus nicht korrekt.

Informationen zum Ändern des Zertifikatmodus für die Verwendung eines anderen Zertifikatstyps finden Sie unter Moduswechsel-Workflows für Zertifikate in ESXi und Ändern des ESXi-Zertifikatmodus.

Ablauf des ESXi-Zertifikats

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

ESXi-Bereitstellung und -Zertifikate

Beim Start eines ESXi-Hosts von einem Installationsmedium besitzt der Host zunächst ein automatisch generiertes Zertifikat. Wenn Sie einen Host zum vCenter Server-System hinzufügen, stellt vCenter Server den Host mit einem von VMCA als Stammzertifizierungsstelle signiertes Zertifikat bereit.

Sie können auch benutzerdefinierte Zertifikate verwenden, die von einer Drittanbieter- oder Unternehmenszertifizierungsstelle für ESXi-Hosts signiert sind.

ESXi-Bereitstellung und -Zertifikate in Auto Deploy

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

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

Sie können Auto Deploy als untergeordnete Zertifizierungsstelle einer externen Zertifizierungsstelle festlegen. In diesem Fall werden die generierten Zertifikate mit dem Auto Deploy-SSL-Schlüssel signiert. Weitere Informationen finden Sie unter Festlegen von Auto Deploy als untergeordnete Zertifizierungsstelle.

In ESXi Version 8.0 und höher können Sie benutzerdefinierte Zertifikate (von einer Zertifizierungsstelle signierte Zertifikate) mit Auto Deploy verwenden. Wenn der Host gestartet wird, ordnet Auto Deploy das benutzerdefinierte Zertifikat entweder einer MAC-Adresse oder der BIOS-UUID des ESXi-Hosts zu. Weitere Informationen finden Sie unter Verwenden benutzerdefinierter Zertifikate mit Auto Deploy.

Erforderliche Berechtigungen für die ESXi-Zertifikatsverwaltung

Das Recht **Zertifikate.Zertifikate verwalten** ist erforderlich, damit Benutzer Ihre ESXi-Hostzertifikate verwalten können.

Änderungen des ESXi-Hostnamens und der -IP-Adresse

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

Tabelle 3-4. Notwendigkeit eines manuellen Eingriffs bei Hostnamen- oder IP-Adressänderung

ESXi-Host zu vCenter Server hinzugefügt mithilfe ...	Änderungen des ESXi-Hostnamens	Änderungen der ESXi-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-Host-Upgrades und Zertifikate

Wenn Sie ein Upgrade eines ESXi-Hosts auf ESXi 6.7 oder höher durchführen, werden beim Upgrade-Prozess die selbstsignierten (Fingerabdruck-)Zertifikate durch VMCA-signierte Zertifikate ersetzt. Wenn der ESXi-Host benutzerdefinierte Zertifikate verwendet, werden diese Zertifikate beim Upgrade-Prozess beibehalten, selbst wenn diese Zertifikate abgelaufen oder ungültig sind.

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

Host mit bereitgestellten Fingerabdruckzertifikaten

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

Hinweis Sie können keine VMCA-Zertifikate auf Legacy-Hosts bereitstellen. Für diese Hosts müssen Sie ein Upgrade auf ESXi 6.7 oder höher durchführen.

Host mit bereitgestellten benutzerdefinierten Zertifikaten

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

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

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

Hosts, die mit Auto Deploy bereitgestellt werden

Hosts, die mit Auto Deploy bereitgestellt werden, werden immer neue Zertifikate zugewiesen, wenn sie zum ersten Mal mit ESXi 6.7 oder höher gestartet werden. Wenn Sie ein Upgrade für einen Host mit Bereitstellung durch Auto Deploy durchführen, generiert der Auto Deploy-Server eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) für den Host und sendet diese an VMCA. VMCA speichert das signierte Zertifikat für den Host. Wenn der Auto Deploy-Server Bereitstellungen für den Host durchführt, ruft er das Zertifikat von VMCA ab und schließt es als Bestandteil des Bereitstellungsprozesses ein.

Sie können Auto Deploy mit benutzerdefinierten Zertifikaten verwenden.

Informationen dazu finden Sie unter Festlegen von Auto Deploy als untergeordnete Zertifizierungsstelle und Verwenden benutzerdefinierter Zertifikate mit Auto Deploy.

Moduswechsel-Workflows für Zertifikate in ESXi

Standardmäßig stellt VMware Certificate Authority (VMCA) ESXi mit Zertifikaten bereit. Verwenden Sie den benutzerdefinierten Modus, wenn Sie VMCA-Zertifikate durch benutzerdefinierte Zertifikate ersetzen. Verwenden Sie den alten Fingerabdruckmodus für das Debugging. Wenn Sie einen Moduswechsel benötigen, sollten Sie die möglichen Auswirkungen vor Beginn prüfen.

Eine Erläuterung der Zertifikatmodi finden Sie unter Zertifikate und Zertifikatmodi.

Verwenden von benutzerdefinierten ESXi-Zertifikaten

Hinweis Wenn Sie von der Verwendung von VMCA-Zertifikaten zu benutzerdefinierten Zertifikaten wechseln, planen Sie beim Generieren von Zertifikaten Zeit für die Genehmigungs- und Erfüllungsprozesse der Organisation ein. Planen Sie außerdem so, dass das aktuelle Zertifikat während des Wechsels nicht abläuft.

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

1. Wechseln Sie in den **benutzerdefinierten** Modus. Weitere Informationen hierzu finden Sie unter Ändern des ESXi-Zertifikatmodus.

   Wenn Sie den Modus wechseln, kann vSphere Client das Dropdown-Menü **Verwaltung mit externer Zertifizierungsstelle** aktivieren, sodass Sie die Zertifikatssignieranforderung generieren können.

2. Fügen Sie das Stammzertifikat der benutzerdefinierten Zertifizierungsstelle zu VMware Endpoint Certificate Store (VECS) hinzu.

3. Generieren Sie die Zertifikatssignieranforderung und rufen Sie die Zertifikate ab, die Sie verwenden möchten.

   Möglicherweise müssen Sie einige Zeit warten, bis die CSR zurückgesendet wird.

4 Importieren Sie das benutzerdefinierte CA-Zertifikat in den vCenter Server-Host.

   Warten Sie einige Zeit, bis vCenter Server das benutzerdefinierte CA-Zertifikat an die ESXi-Hosts verteilt hat.

Wechseln vom benutzerdefinierten Zertifizierungsstellen-Modus zum VMCA-Modus

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

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

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

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

Wechseln vom Fingerabdruckmodus in den VMCA-Modus

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

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

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

3 Fügen Sie die ESXi-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 ESXi-Zertifikatmodus folgen. Nach dem Moduswechsel prüft das vCenter Server-System nur das Format des Zertifikats, aber nicht mehr die Gültigkeit des Zertifikats selbst.

Wechseln vom Fingerabdruckmodus in den benutzerdefinierten Zertifizierungsstellen-Modus

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

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

2 Fügen Sie das Root-Zertifikat der benutzerdefinierten Zertifizierungsstelle dem TRUSTED_ROOTS-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 ESXi-Zertifikatmodus.

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

Standardeinstellungen für ESXi-Zertifikate

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

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

Tabelle 3-5. CSR-Einstellungen für ESXi

Parameter	Standardwert	Erweiterte Option
Schlüssellänge	2048	Nicht zutreffend
Schlüsselalgorithmus	RSA	Nicht zutreffend

Tabelle 3-5. CSR-Einstellungen für ESXi (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	US	vpxd.certmgmt.certs.cn.country
E-Mail-Adresse	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
Ort	Palo Alto	vpxd.certmgmt.certs.cn.localityName
Name der Organisationseinheit	VMware Engineering	vpxd.certmgmt.certs.cn.organizationalUnitName
Organisationsname	VMware	vpxd.certmgmt.certs.cn.organizationName
Bundesland/Kanton	Kalifornien	vpxd.certmgmt.certs.cn.state
Anzahl der Tage, die das Zertifikat gültig ist.	1825	vpxd.certmgmt.certs.daysValid
Fester Schwellenwert für den Ablauf des Zertifikats. vCenter Server löst einen roten Alarm aus, wenn dieser Schwellenwert erreicht wird.	30 Tage	vpxd.certmgmt.certs.hardThreshold
Abfrageintervall für Überprüfungen der Gültigkeit des vCenter Server-Zertifikats.	5 Tage	vpxd.certmgmt.certs.pollIntervalDays
Soft-Schwellenwert für den Ablauf des Zertifikats. vCenter Server löst ein Ereignis aus, wenn dieser Schwellenwert erreicht wird.	240 Tage	vpxd.certmgmt.certs.softThreshold
Modus, den vCenter Server verwendet, um zu ermitteln, ob vorhandene Zertifikate ersetzt werden. Ändern Sie diesen Modus, um benutzerdefinierte Zertifikate beim Upgrade beizubehalten. Weitere Informationen hierzu finden Sie unter ESXi-Host-Upgrades und Zertifikate.	vmca Sie können auch „Fingerabdruck“ oder „benutzerdefiniert“ festlegen. Weitere Informationen hierzu finden Sie unter Ändern des ESXi-Zertifikatmodus.	vpxd.certmgmt.mode

Ändern der Standardeinstellungen für ESXi-Zertifikate

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

Eine Liste der Standardeinstellungen finden Sie in der vorherigen Tabelle. Einige der Standardwerte können nicht geändert werden.

Verfahren

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

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

Nächste Schritte

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

Anzeigen von Informationen zum Ablauf von Zertifikaten für ESXi-Hosts

Für ESXi-Hosts im VMCA-Modus oder im benutzerdefinierten Modus können Sie Zertifikatsdetails über den vSphere Client anzeigen. Anhand der Zertifikatsinformationen können Sie feststellen, ob eines Ihrer Zertifikate bald abläuft. Sie können diese Informationen auch zum Debuggen von Zertifikatproblemen verwenden.

Sie können keine Zertifikatsstatusinformationen für ESXi-Hosts im Fingerabdruckmodus anzeigen. Sie können Informationen für mehrere ESXi-Hosts oder für einen einzelnen ESXi-Host anzeigen. In der Ansicht mit mehreren Hosts werden nur die Informationen zu dem bis zu einem bestimmten Datum gültigen Zertifikat angezeigt.

Verfahren

1. Melden Sie sich beim vCenter Server mit dem vSphere Client an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.

3 Rufen Sie die Zertifikatsinformationen ab.

Einzelner Host oder mehrere Hosts	Schritte
Single	a Navigieren Sie zum ESXi-Host. b Klicken Sie auf **Konfigurieren**. c Klicken Sie unter **System** auf **Zertifikat**.
Mehrere	a Wählen Sie **Hosts und Cluster > Hosts** aus. Standardmäßig wird der Zertifikatsstatus in der Anzeige der Hosts nicht eingeblendet. b Um Spalten ein- oder auszublenden, klicken Sie auf **Spalten verwalten**. c Aktivieren Sie das Kontrollkästchen **Zertifikat gültig bis** und führen Sie gegebenenfalls einen Bildlauf nach rechts durch, um die hinzugefügte Spalte anzuzeigen. Bei den Zertifikatsinformationen wird das Ablaufdatum des Zertifikats angezeigt. d (Optional) Heben Sie die Auswahl von anderen Spalten auf, damit die relevanten Informationen leichter zu sehen sind.

4 Überprüfen Sie die Zertifikatsinformationen.

Die folgenden Informationen sind nur in der Einzelhostansicht verfügbar.

Bereich	Beschreibung
Betreff	Der während der Zertifikatgenerierung verwendete Betreff.
Aussteller	Der Aussteller des Zertifikats.
Gültig von	Das Datum, an dem das Zertifikat generiert wurde.

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

Hinweis 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.

Nächste Schritte

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

Verlängern oder Aktualisieren von ESXi-Zertifikaten

Wenn Sie die VMware-Zertifizierungsstelle (VMCA) zum Zuweisen von Zertifikaten zu Ihren Hosts verwenden, können Sie diese Zertifikate über den vSphere Client verlängern. Wenn Sie entweder VMCA-Zertifikate oder benutzerdefinierte Zertifikate verwenden, können Sie alle Zertifikate aus dem TRUSTED_ROOTS-Speicher aktualisieren, der mit vCenter Server verknüpft ist.

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

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

Sie können ein ESXi-Zertifikat mit einem Ablaufdatum, das nach dem Ablaufdatum des vertrauenswürdigen Rootzertifikats liegt, nicht verlängern. Beispiel: Wenn die erweiterte Option ESXi `vpxd.certmgmt.certs.daysValid` auf fünf Jahre festgelegt ist und Ihr vertrauenswürdiges Rootzertifikat in zwei Jahren abläuft, ist das Ablaufdatum des ESXi-Zertifikats auf zwei Jahre beschränkt.

Sie können den vSphere Client verwenden, um alle Zertifikate, die sich derzeit im TRUSTED_ROOTS-Speicher des vCenter Server VECS-Speichers befinden, an den ESXi-Host zu übertragen. Verwenden Sie diese Funktion, wenn Sie die vertrauenswürdigen Roots auf einem ESXi-Host aktualisieren müssen. Diese Funktion ist sowohl für VMCA als auch für benutzerdefinierte Zertifikate vorhanden.

Voraussetzungen

Überprüfen Sie Folgendes:

- Bei Verwendung von VMCA-Zertifikaten ist der Zertifikatmodus auf **vmca** festgelegt.
- Wenn Sie benutzerdefinierte Zertifikate verwenden, ist der Zertifikatmodus auf **Benutzerdefiniert** festgelegt.
- Die ESXi-Hosts sind mit dem vCenter Server-System verbunden.
- Zwischen dem vCenter Server-System und den ESXi-Hosts findet eine ordnungsgemäße Uhrzeitsynchronisierung statt.
- DNS-Auflösung funktioniert zwischen dem vCenter Server-System und den ESXi-Hosts.
- Die Zertifikate MACHINE_SSL_CERT und Trusted_Root des vCenter Server-Systems sind gültig und nicht abgelaufen. Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/2111411.
- Die ESXi-Hosts befinden sich nicht im Wartungsmodus.

Hinweis Wenn Sie benutzerdefinierte Zertifikate verwenden und sie verlängern müssen, importieren Sie die Zertifikate erneut.

Verfahren

1 Navigieren Sie zum Host im Navigator von vSphere Client.

2 Klicken Sie auf **Konfigurieren**.

3 Klicken Sie unter **System** auf **Zertifikat**.

Sie können die Details zum Zertifikat des ausgewählten Hosts anzeigen.

4 Wählen Sie die entsprechende Option basierend auf dem verwendeten Zertifikatstyp aus.

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

Ändern des ESXi-Zertifikatmodus

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

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

Verfahren

1 Wählen Sie im vSphere Client das vCenter Server-System aus, das die Hosts verwaltet.

2 Klicken Sie auf **Konfigurieren** und unter „Einstellungen“ auf **Erweiterte Einstellungen**.

3 Klicken Sie auf **Einstellungen bearbeiten**.

4 Klicken Sie auf das Symbol **Filter** in der Spalte „Name“ und geben Sie im Feld „Filter“ den Wert **`vpxd.certmgmt`** ein, um ausschließlich Parameter der Zertifikatsverwaltung anzuzeigen.

Hinweis Die verfügbaren Optionen sind **VMCA**, **Benutzerdefiniert** und **Fingerabdruck**.

5 Ändern Sie den Wert von `vpxd.certmgmt.mode` in **Benutzerdefiniert**, wenn Sie eigene Zertifikate verwalten möchten, oder zu **Fingerabdruck**, wenn Sie vorübergehend in den Fingerabdruckmodus wechseln möchten. Klicken Sie anschließend auf **Speichern**.

Ersetzen des ESXi-Standardzertifikats durch ein benutzerdefiniertes Zertifikat

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

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

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

Sie können die Standardzertifikate mithilfe des vSphere Client oder der CLI durch benutzerdefinierte Zertifikate 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.

Vor 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.

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

Anforderungen für ESXi-Zertifikatsignieranforderungen für benutzerdefinierte Zertifikate

Verwenden Sie eine Zertifikatssignieranforderung mit den folgenden Eigenschaften:

- Schlüsselgröße: 2048 Bit (Minimum) bis 8192 (Maximum) (PEM-codiert)
- PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
- x509 Version 3
- Für Stammzertifikate muss die Zertifizierungsstellenerweiterung auf „true“ festgelegt sein, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.
- „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten.
- CRT-Format
- Enthält die folgenden Schlüsselverwendungen: digitale Signatur, Schlüsselverschlüsselung

- Startzeit von einem Tag vor dem aktuellen Zeitpunkt.
- CN (und SubjectAltName) auf den Hostnamen (oder die IP-Adresse) festgelegt, den/die der ESXi-Host in der vCenter Server-Bestandsliste hat.

Hinweis Das FIPS-Zertifikat von vSphere validiert nur die RSA-Schlüsselgrößen 2048 und 3072. Weitere Informationen hierzu finden Sie unter Überlegungen bei der Verwendung von FIPS.

Die folgenden Zertifikate werden von vSphere nicht unterstützt.

- Zertifikate mit Platzhalterzeichen.
- Die Algorithmen md2WithRSAEncryption, md5WithRSAEncryption, RSASSA-PSS, dsaWithSHA1, ecdsa_with_SHA1 und sha1WithRSAEncryption werden nicht unterstützt.

Weitere Informationen zum Generieren der CSR mit dem vSphere Client finden Sie unter Generieren einer Zertifikatssignieranforderung für ein benutzerdefiniertes Zertifikat mithilfe von vSphere Client.

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

Weitere Themen zum Lesen

- Generieren einer Zertifikatssignieranforderung für ein benutzerdefiniertes Zertifikat mithilfe von vSphere Client

  Ab vSphere 8.0 Update 3 können Sie den vSphere Client verwenden, um eine Zertifikatssignieranforderung für das ESXi-SSL-Zertifikat zu generieren und das Zertifikat zu ersetzen, sobald es bereit ist.
- Ersetzen des Standardzertifikats durch ein benutzerdefiniertes Zertifikat mithilfe des vSphere Client

  Sie können die standardmäßigen VMCA-signierten ESXi-Zertifikate über den vSphere Client durch benutzerdefinierte Zertifikate ersetzen.
- 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 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.

Generieren einer Zertifikatssignieranforderung für ein benutzerdefiniertes Zertifikat mithilfe von vSphere Client

Ab vSphere 8.0 Update 3 können Sie den vSphere Client verwenden, um eine Zertifikatssignieranforderung für das ESXi-SSL-Zertifikat zu generieren und das Zertifikat zu ersetzen, sobald es bereit ist.

Voraussetzungen

Ändern des Zertifikatsmodus in **Benutzerdefiniert**. Weitere Informationen hierzu finden Sie unter Ändern des ESXi-Zertifikatmodus. Wenn Sie den Modus wechseln, kann vSphere Client das Dropdown-Menü **Verwaltung mit externer Zertifizierungsstelle** aktivieren, sodass Sie die Zertifikatssignieranforderung generieren können.

Warnung Beim Generieren einer Zertifikatssignieranforderung wird ein neuer privater Schlüssel erstellt. Generieren Sie während des Ersetzens von Zertifikaten keine weitere Zertifikatssignieranforderung. Wenn Sie dies tun, sind die zuvor generierte CSR und das daraus folgende Zertifikat nicht mehr gültig.

Verfahren

1. Navigieren Sie im vSphere Client-Bestand zum Host.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter **System** auf **Zertifikat**.
4. Wählen Sie im Dropdown-Menü **Mit externer Zertifizierungsstelle verwalten** entweder **CSR mit IP generieren** oder **CSR mit FQDN generieren** aus.

   vCenter Server erkennt die Option, die zuvor zum Generieren des Zertifikats auf dem ESXi-Host verwendet wurde.
5. Wählen Sie entweder **In Zwischenablage kopieren** oder **Download** aus, je nachdem, wie Sie die Zertifikatssignieranforderung generieren möchten.

Nächste Schritte

Sie können die CSR jetzt an die Zertifizierungsstelle senden oder sie verwenden, um das Zertifikat intern zu generieren.

Ersetzen des Standardzertifikats durch ein benutzerdefiniertes Zertifikat mithilfe des vSphere Client

Sie können die standardmäßigen VMCA-signierten ESXi-Zertifikate über den vSphere Client durch benutzerdefinierte Zertifikate ersetzen.

Stellen Sie beim Importieren des benutzerdefinierten Zertifikats Folgendes sicher:

- Fügen Sie Ihre gesamte CA-Zertifikatskette hinzu, bevor Sie mit der Ersetzung fortfahren.
- Stellen Sie sicher, dass Sie das richtige CA-Zertifikat für Ihre Umgebung bereitstellen. Beim Importieren und Ersetzen wird das von Ihnen verwendete Zertifikat nicht überprüft.

- Stellen Sie sicher, dass keine SHA1-Hashes in der Zertifikatskette vorhanden sind. SHA1 wird nicht unterstützt.
- Fügen Sie die Root-Zertifizierungsstelle zu VECS hinzu, bevor Sie fortfahren. Falls nicht, wird der Host sofort nach der Zertifikatsersetzung getrennt.

Voraussetzungen

- Generieren Sie die Zertifikatsignieranforderung und senden Sie sie an die Zertifizierungsstelle. Weitere Informationen hierzu finden Sie unter Generieren einer Zertifikatssignieranforderung für ein benutzerdefiniertes Zertifikat mithilfe von vSphere Client.
- Wenn die Zertifizierungsstelle das Zertifikat zurückgibt, speichern Sie es auf den ESXi-Hosts.
- Stellen Sie sicher, dass der ESXi-Zertifikatmodus auf **benutzerdefiniert** festgelegt ist. Weitere Informationen hierzu finden Sie unter Ändern des ESXi-Zertifikatmodus.
- Aktualisieren Sie den vertrauenswürdigen Root-Speicher. Weitere Informationen hierzu finden Sie unter Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS (Benutzerdefinierte Zertifikate).

Verfahren

1. Navigieren Sie im vSphere Client-Bestand zum Host.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter **System** auf **Zertifikat**.
4. Wählen Sie im Dropdown-Menü **Mit externer CA verwalten** die Option **Importieren und ersetzen** aus.
5. Wählen Sie die Ersetzungsoption aus.

Option	Beschreibung
Durch externes CA-Zertifikat ersetzen, wenn CSR von ESXi erzeugt wird (eingebetteter privater Schlüssel)	Verwenden Sie diese Option, wenn Sie die CSR in ESXi generiert haben. In diesem Fall wird der private Schlüssel in ESXi gespeichert.
Durch externes CA-Zertifikat ersetzen, wobei CSR von einer Zertifizierungsstelle erzeugt wird (privater Schlüssel erforderlich)	Verwenden Sie diese Option, wenn Sie die CSR an eine Drittanbieter-Zertifizierungsstelle gesendet und das Zertifikat und den privaten Schlüssel zurückerhalten haben.

6. Klicken Sie auf **Weiter**.
7. Suchen Sie nach dem Zertifikat bzw. dem Zertifikat und dem privaten Schlüssel.
8. Überprüfen Sie die Informationen und klicken Sie dann auf **Importieren und ersetzen**.

Ergebnisse

Das benutzerdefinierte Zertifikat ersetzt das vorhandene Zertifikat.

Ersetzen des Standardzertifikats und -schlüssels über die ESXi Shell

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

Voraussetzungen

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

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

Verfahren

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

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

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

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

Ersetzen eines Standardzertifikats mit HTTPS PUT

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

Voraussetzungen

- Wenn Sie CA-signierte Zertifikate von Drittanbietern verwenden, generieren Sie die Zertifikatsanforderung, senden Sie sie an die Zertifizierungsstelle und speichern Sie die Zertifikate auf jedem ESXi-Host.

- Aktivieren Sie ggf. ESXi Shell oder SSH-Datenverkehr vom vSphere Client.
- Alle Dateiübertragungen und andere Kommunikationsvorgänge erfolgen über eine sichere HTTPS-Sitzung. Der zum Authentifizieren der Sitzung verwendete Benutzer muss über das Recht **Host.Config.AdvancedConfig** auf dem Host verfügen.

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

Verfahren

1 Sichern Sie die vorhandenen Zertifikate.

2 Richten Sie Standardzugriffsauthentifizierung ein und stellen Sie einen Base64-codierten Benutzernamen und ein Kennwort getrennt durch einen Doppelpunkt (:) bereit. Weitere Informationen finden Sie unter https://en.wikipedia.org/wiki/Basic_access_authentication.

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

   a Öffnen Sie die Datei.

   b Veröffentlichen Sie die Datei an einem der folgenden Speicherorte.

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

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

4 Starten Sie den Host neu.

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

Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS (Benutzerdefinierte Zertifikate)

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

Voraussetzungen

Ersetzen Sie die Zertifikate auf jedem Host durch benutzerdefinierte Zertifikate.

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

Verfahren

1. Informationen zum Aktualisieren des vCenter Server TRUSTED_ROOTS-Speichers mit vSphere Client finden Sie unter Hinzufügen eines vertrauenswürdigen Stammzertifikats zum Zertifikatsspeicher mithilfe des vSphere Client.
2. Um den vCenter Server TRUSTED_ROOTS-Speicher über die Befehlszeilenschnittstelle zu aktualisieren, melden Sie sich bei der vCenter Server-Shell des vCenter Server-Systems an, das die ESXi-Hosts verwaltet.
3. Um die neuen Zertifikate zum Speicher `TRUSTED_ROOTS` hinzuzufügen, führen Sie `dir-cli` aus. Beispiel:

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

4. Geben Sie bei Aufforderung die Single Sign-On-Administrator-Anmeldedaten ein.
5. Wenn Ihre benutzerdefinierten Zertifikate von einer Zwischenzertifizierungsstelle ausgestellt werden, müssen Sie auch die Zwischenzertifizierungsstelle zum Speicher `TRUSTED_ROOTS` auf dem vCenter Server hinzufügen. z. B.:

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

Nächste Schritte

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

Festlegen von Auto Deploy als untergeordnete Zertifizierungsstelle

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

Voraussetzungen

- Fordern Sie ein Zertifikat von Ihrer Zertifizierungsstelle an. Die Zertifikatsdatei muss die folgenden Anforderungen erfüllen.
  - Schlüsselgröße: 2048 Bit (Minimum) bis 8192 (Maximum) (PEM-codiert)
  - PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
  - x509 Version 3
  - Für Stammzertifikate muss die Zertifizierungsstellenerweiterung auf „true“ festgelegt sein, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.
  - „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten.
  - CRT-Format
  - Enthält die folgenden Schlüsselverwendungen: digitale Signatur, Schlüsselverschlüsselung
  - Startzeit von einem Tag vor dem aktuellen Zeitpunkt.
  - CN (und SubjectAltName) auf den Hostnamen (oder die IP-Adresse) festgelegt, den/die der ESXi-Host in der vCenter Server-Bestandsliste hat.

  Hinweis Das FIPS-Zertifikat von vSphere validiert nur die RSA-Schlüsselgrößen 2048 und 3072. Weitere Informationen hierzu finden Sie unter Überlegungen bei der Verwendung von FIPS.

- Benennen Sie die Zertifikatdatei als `rbd-ca.crt` und die Schlüsseldatei als `rbd-ca.key`.

Verfahren

1 Sichern Sie die standardmäßigen ESXi-Zertifikate.

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

2 Halten Sie den vSphere Authentication Proxy-Dienst an.

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

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

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

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

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

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

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

Weitere Informationen hierzu finden Sie unter Ändern des ESXi-Zertifikatmodus.

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

Ergebnisse

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

Hinweis Wenn Sie Probleme mit Auto Deploy nach der Zertifikatsersetzung haben, lesen Sie sich den VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/2000988 durch.

Verwenden benutzerdefinierter Zertifikate mit Auto Deploy

Ab vSphere 8.0 können Sie den Auto Deploy-Server so einrichten, dass ESXi-Hosts mit benutzerdefinierten Zertifikaten bereitgestellt werden, die von einer Drittanbieter-Zertifizierungsstelle (CA) oder Ihrer eigenen internen Zertifizierungsstelle signiert wurden. Standardmäßig stattet der Auto Deploy-Server ESXi-Host mit Zertifikaten aus, die von der VMware Certificate Authority (VMCA) signiert wurden.

Vor vSphere 8.0 haben Sie folgende Optionen für die Verwaltung von Zertifikaten mit Auto Deploy:

- Verwenden von vCenter Server und der integrierten VMware Certificate Authority (Standardeinstellung).
- Auto Deploy wird zu einer untergeordneten Zertifizierungsstelle einer Drittanbieter-Zertifizierungsstelle. In diesem Fall signiert der Auto Deploy-SSL-Schlüssel die Zertifikate.

Ab vSphere 8.0 können Sie benutzerdefinierte Zertifikate auf Auto Deploy hochladen, die entweder von einer Drittanbieter-Zertifizierungsstelle oder Ihrer eigenen internen Zertifizierungsstelle signiert wurden. Auto Deploy ordnet das benutzerdefinierte Zertifikat entweder der MAC-Adresse oder der BIOS-UUID des ESXi-Hosts zu. Bei jedem Start eines Auto Deploy-Hosts prüft Auto Deploy, ob ein benutzerdefiniertes Zertifikat vorhanden ist. Wenn Auto Deploy ein benutzerdefiniertes Zertifikat findet, verwendet es dieses Zertifikat, anstatt es über die VMCA zu generieren.

Zu den allgemeinen Schritten für diese Aufgabe gehören:

1 Generieren der benutzerdefinierten Zertifikatanforderung für eine Drittanbieter-Zertifizierungsstelle oder für Ihre eigene interne Zertifizierungsstelle.

2 Das signierte benutzerdefinierte Zertifikat (Schlüssel und Zertifikat) wird abgerufen und lokal gespeichert.

3 Wenn Sie eine Zertifizierungsstelle eines Drittanbieters verwenden und dies zuvor nicht geschehen ist, stellen Sie sicher, dass das Stammzertifikat Ihrer Zertifizierungsstelle in den TRUSTED_ROOTS-Speicher auf dem vCenter Server hochgeladen wird.

4 Hochladen des benutzerdefinierten Zertifikats auf Auto Deploy und Zuordnen des Zertifikats mit der MAC-Adresse oder der BIOS-UUID eines ESXi-Hosts.

5 Starten des ESXi-Hosts.

Wenn Sie einem ESXi-Host ein benutzerdefiniertes Zertifikat zuweisen, überträgt Auto Deploy das Zertifikat beim nächsten Start von Auto Deploy an den Host.

Beachten Sie bei der Verwendung von benutzerdefinierten Zertifikaten und Auto Deploy Folgendes.

- Sie müssen die PowerCLI-Cmdlets `Add-CustomCertificate`, `Remove-CustomCertificate` und `List-CustomCertificate` verwenden, um mit Auto Deploy verwendete benutzerdefinierte Zertifikate zu verwalten. Die Funktion zum Verwalten von benutzerdefinierten Zertifikaten ist im vSphere Client nicht verfügbar.
- Um ein benutzerdefiniertes Zertifikat zu aktualisieren, das für Auto Deploy verwendet wird, müssen Sie das `Add-CustomCertificate`-Cmdlet erneut ausführen.
- Prüfen Sie Ihr benutzerdefiniertes Zertifikat unbedingt auf potenzielle Fehler. Auto Deploy überprüft nur, ob das benutzerdefinierte Zertifikat den X.509-Zertifikatstandards entspricht und dass der Schwellenwert für den Ablauf des Zertifikats auf mindestens 240 Tage festgelegt ist. Auto Deploy führt keine andere Zertifikatvalidierung oder -überprüfung durch. Um den Schwellenwert des Zertifikats zu ändern, können Sie das `Set-DeployOption -Key certificate-refresh-threshold`-Cmdlet ausführen.
- Wenn Sie später ein benutzerdefiniertes Zertifikat mithilfe des `Remove-CustomCertificate`-Cmdlet von einem ESXi-Host entfernen, müssen Sie den Host neu starten, damit die Änderung wirksam wird.

Weitere Informationen zu benutzerdefinierten Zertifikaten und Auto Deploy finden Sie in der *Installation und Einrichtung von VMware ESXi*-Dokumentation.

Voraussetzungen

Vergewissern Sie sich, dass Sie über Folgendes verfügen:

- Fordern Sie ein Zertifikat von Ihrer Zertifizierungsstelle an. Die Zertifikatsdatei muss die folgenden Anforderungen erfüllen.
  - Schlüsselgröße: 2048 Bit (Minimum) bis 8192 (Maximum) (PEM-codiert)
  - PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
  - x509 Version 3
  - CRT-Format
  - Die CA-Erweiterung auf „true“ festgelegt
  - Schlüsselverwendung der Zertifikatsignierung
  - Startzeit von einem Tag vor dem aktuellen Zeitpunkt

  Hinweis Das FIPS-Zertifikat von vSphere validiert nur die RSA-Schlüsselgrößen 2048 und 3072. Weitere Informationen hierzu finden Sie unter Überlegungen bei der Verwendung von FIPS.
- MAC-Adresse oder BIOS-UUID des ESXi-Hosts. Bewerten Sie, welcher Ansatz für Ihre Umgebung am sinnvollsten ist. Die BIOS-UUID ist stabiler und kann weniger geändert werden als die MAC-Adresse. Wenn Sie Netzwerkadapter in einem ESXi-Host ändern, ändert sich die MAC-Adresse. Die MAC-Adresse ist jedoch möglicherweise vertrauter und lässt sich leichter abrufen als die BIOS-UUID.
- Mindestens PowerCLI Version 12.6.0. Weitere Informationen zu Auto Deploy PowerCLI-Cmdlets finden Sie im Thema „Auto Deploy PowerCLI-Cmdlet – Überblick“ in der *Installation und Einrichtung von VMware ESXi*-Dokumentation.

Stellen Sie sicher, dass Sie über die folgenden Berechtigungen verfügen:

- Benutzerdefiniertes Zertifikat hinzufügen: **Autodeploy.Regel.Erstellen**
- Benutzerdefinierte Zertifikatinformationen abrufen: **System.Lesen**

Verfahren

1 Generieren Sie die Zertifikatanforderung.

   a Erstellen Sie mithilfe der zuvor für die Zertifikatanforderung aufgeführten Anforderungen eine Konfigurationsdatei (.cfg).

   b Um eine CSR-Datei und eine Schlüsseldatei zu generieren, führen Sie den Befehl `openssl req` aus und übergeben Sie die Konfigurationsdatei (.cfg).

   Beispiel:

```
openssl req -new -config custom_cert.cfg -days 4200 -sha256 -keyout rui.key -out
rui.csr
```

   In diesem Befehl findet Folgendes statt:

   - `-new` generiert eine neue Zertifikatanforderung.
   - `-config custom_cert.cfg` gibt Ihre benutzerdefinierte.cfg-Datei an.
   - `-days 4200` gibt 4200 Tage an, für die das Zertifikat zertifiziert werden soll.
   - `-sha256` gibt den Meldungs-Digest zum Signieren der Anforderung mit an.
   - `-keyout rui.key` gibt die Datei an, in die der neu erstellte private Schlüssel geschrieben werden soll.
   - `-out rui.csr` gibt die Ausgabedatei an, in die geschrieben werden soll.

2 Senden Sie die Zertifikatanforderung entweder an Ihre Drittanbieter-Zertifizierungsstelle oder führen Sie, wenn Sie Ihre eigenen Zertifikate signieren, den Befehl `openssl x509 -req` aus, um Ihr benutzerdefiniertes Zertifikat aus der Datei `rui.csr` zu generieren.

   Beispiel:

```
openssl x509 -req -in rui.csr -CA "/etc/vmware-rbd/ssl/rbd-ca.crt" -CAkey \
"/etc/vmware-rbd/ssl/rbd-ca.key" -extfile \
openssl.cfg -extensions x509 -CAserial "/etc/vmware-rbd/ssl/rbd-ca.srl" -days \
4200 -sha256 -out signed_rui.crt
```

   In diesem Befehl findet Folgendes statt:

   - `-in rui.csr` gibt die Eingabedatei an.
   - `-CA "/etc/vmware-rbd/ssl/rbd-ca.crt"` gibt das Verzeichnis an, das für die Verifizierung des Serverzertifikats verwendet werden soll.
   - `-CAkey "/etc/vmware-rbd/ssl/rbd-ca.key"` legt den privaten Schlüssel der Zertifizierungsstelle fest, um ein Zertifikat mit zu signieren.
   - `-extfile openssl.cfg` gibt eine zusätzliche, optionale Konfigurationsdatei zum Lesen von Zertifikaterweiterungen an.
   - `-extensions x509` gibt die Verwendung von x509-Zertifikaterweiterungen an.

- `-CAserial "/etc/vmware-rbd/ssl/rbd-ca.srl"` verwendet die Seriennummer in `rbd-ca.srl`, um ein Zertifikat zu signieren.
- `-days 4200` gibt 4200 Tage an, für die das Zertifikat zertifiziert werden soll.
- `-sha256` gibt den Meldungs-Digest zum Signieren der Anforderung mit an.
- `-out signed_rui.crt` gibt die Ausgabedatei an, in die geschrieben werden soll.

3 (Optional) Wenn Sie das Zertifikat Ihrer signaturgebenden Zertifizierungsstelle noch nicht in den TRUSTED_ROOTS-Speicher im VMware Endpoint Certificate Store (VECS) hochgeladen haben, führen Sie die folgenden Schritte auf dem vCenter Server aus, auf dem der Auto Deploy-Dienst ausgeführt wird.

   a Kopieren Sie das Zertifikat mithilfe eines Tools wie WinSCP in den vCenter Server.

   b Melden Sie sich bei vCenter Server mithilfe von SSH an und führen Sie folgenden Befehl aus.

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

4 Rufen Sie entweder die MAC-Adresse oder die BIOS-UUID des ESXi-Hosts ab.

5 Führen Sie die folgenden Schritte aus, um das benutzerdefinierte Zertifikat zu Auto Deploy hinzuzufügen.

   a Um eine Verbindung mit dem vCenter Server herzustellen, führen Sie das `Connect-VIServer`-Cmdlet aus.

   ```
   Connect-VIServer -server VC_ip_address -User administrator_user -Password 'password'
   ```

   b (Optional) Um vorhandene benutzerdefinierte Zertifikate anzuzeigen, führen Sie das `Get-CustomCertificates`-Cmdlet aus.

   Beim ersten Hinzufügen von benutzerdefinierten Zertifikaten werden keine von diesem Cmdlet zurückgegebenen Zertifikate angezeigt.

c Um das benutzerdefinierte Zertifikat mit dem ESXi-Host zu verknüpfen, führen Sie das `Add-CustomCertificate`-Cmdlet aus.

```
Add-CustomCertificate -HostID [MAC_Address | BIOS_UUID] -Certificate
"path_to_custom_cert" -Key "path_to_custom_cert_key"
```

Sie können entweder die MAC-Adresse oder die BIOS-UUID des Hosts angeben. Auto Deploy lädt das benutzerdefinierte Zertifikat auf den Host hoch.

d Um zu überprüfen, ob das Zertifikat hochgeladen wurde, führen Sie das `Get-CustomCertificates`-Cmdlet aus.

Sie erhalten eine Ausgabe ähnlich der Folgenden:

```
Name:     CustomHostCert-1
CertificateId:      1
HostId:             02:08:b0:8e:18:a2
ExpirationTime: 1   2/28/2033 10:45:50 AM
TimeCreated:        9/29/2022 7:40:28 AM
LastModified:       9/29/2022 7:40:28 AM
AssociatedHostName:
```

`AssociatedHostName` ist vorerst leer. Nachdem Sie den Host gestartet haben, spiegelt die Ausgabe den Namen des ESXi-Hosts wider, der dem benutzerdefinierten Zertifikat zugeordnet ist.

6 Starten Sie den ESXi-Host.

7 Um zu überprüfen, ob das benutzerdefinierte Zertifikat mit dem vCenter Server verknüpft ist, führen Sie das `Get-CustomCertificates`-Cmdlet erneut aus.

Die Ausgabe wird wie folgt angezeigt.

```
Name:     CustomHostCert-1
CertificateId:      1
HostId:             02:08:b0:8e:18:a2
ExpirationTime: 1   2/28/2033 10:45:50 AM
TimeCreated:        9/29/2022 7:40:28 AM
LastModified:       9/29/2022 7:40:28 AM
AssociatedHostName: host1.example.com
```

Jetzt enthält `AssociatedHostName` den Namen des ESXi-Hosts.

Wiederherstellen der ESXi-Zertifikats- und -Schlüsseldateien, wenn die Zertifikatsersetzung fehlschlägt

Wenn das Ersetzen eines Zertifikats auf einem ESXi-Host fehlschlägt, erstellt das System `.bak`-Zertifikatsdateien, mit denen Sie den vorherigen Zustand wiederherstellen können.

Das Hostzertifikat und der Schlüssel befinden sich am Speicherort `/etc/vmware/ssl/rui.crt` bzw. `/etc/vmware/ssl/rui.key`. Wenn Sie ein Hostzertifikat entweder mithilfe des vSphere Client oder des von vSphere Web Services SDK verwalteten Objekts `vim.CertificateManager` ersetzen und die Ersetzung fehlschlägt, erstellt das System `.bak`-Dateien für die vorherigen Schlüssel- und Zertifikatsdateien.

Wenn die Zertifikatsersetzung fehlschlägt, können Sie vorherige Zertifikate wiederherstellen, indem Sie die `.bak`-Dateien in das aktuelle Zertifikat und die Schlüsseldateien kopieren.

Anpassen der ESXi-Hostsicherheit

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

Konfigurieren der ESXi Firewall

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. Sie verwalten die Firewall mithilfe von vSphere Client, der CLI und der API.

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

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

Sie können ESXi-Firewallports wie folgt verwalten:

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

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

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

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

Verwalten von ESXi-Firewalleinstellungen

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

In dieser Aufgabe wird die Verwendung des vSphere Client zum Konfigurieren von ESXi-Firewalleinstellungen beschrieben. Sie können die ESXi Shell oder ESXCLI-Befehle verwenden, um ESXi an der Befehlszeile zu konfigurieren und die Firewallkonfiguration zu automatisieren. Unter Verwenden von ESXCLI-Firewall-Befehlen zum Konfigurieren des ESXi-Verhaltens finden Sie Beispiele zur Verwendung der ESXCLI zum Ändern von Firewalls und Firewallregeln.

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

Verfahren

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

   Sie können zwischen eingehenden und ausgehenden Verbindungen wechseln, indem Sie auf **Eingehend** und **Ausgehend** klicken.
4. Klicken Sie im Abschnitt „Firewall“ auf **Bearbeiten**.
5. Wählen Sie aus einer der Dienstgruppen **Nicht gruppiert**, **Secure Shell** und **Simple Network Management Protocol** aus.
6. Wählen Sie die zu aktivierenden Regelsätze aus oder heben Sie die Auswahl der zu deaktivierenden Regelsätze auf.

7 Für bestimmte Dienste können Sie auch Dienstdetails verwalten, indem Sie zu **Konfigurieren > System > Dienste** navigieren.

   Weitere Informationen zum Starten, Stoppen und Neustarten von Diensten finden Sie unter Aktivieren oder Deaktivieren eines ESXi-Diensts.

8 Bei einigen Diensten können Sie ausdrücklich IP-Adressen angeben, von denen aus Verbindungen zulässig sind.

   Weitere Informationen hierzu finden Sie unter Hinzufügen von zulässigen IP-Adressen für einen ESXi-Host.

9 Klicken Sie auf **OK**.

Hinzufügen von zulässigen IP-Adressen für einen ESXi-Host

Standardmäßig lässt die Firewall für jeden Dienst den Zugriff auf alle IP-Adressen zu. Um den Datenverkehr einzuschränken, ändern Sie jeden Dienst so, dass nur Datenverkehr aus Ihrem Verwaltungssubnetz zugelassen wird. Sie können auch einige Dienste deaktivieren, wenn diese in Ihrer Umgebung nicht verwendet werden.

Um die Liste zulässiger IP-Adressen für einen Dienst zu aktualisieren, können Sie den vSphere Client, ESXCLI oder PowerCLI verwenden. Diese Aufgabe beschreibt, wie Sie vSphere Client verwenden. Anweisungen zur Verwendung der ESXCLI finden Sie im Thema „Verwalten der ESXi Firewall“ in der Dokumentation *ESXCLI-Konzepte und -Beispiele*.

Verfahren

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

2 Navigieren Sie zum ESXi-Host.

3 Klicken Sie auf **Konfigurieren** und dann unter **System** auf **Firewall**.

   Sie können zwischen eingehenden und ausgehenden Verbindungen wechseln, indem Sie auf **Eingehend** und **Ausgehend** klicken.

4 Klicken Sie im Abschnitt „Firewall“ auf **Bearbeiten**.

5 Wählen Sie aus einer der drei Dienstgruppen **Nicht gruppiert**, **Secure Shell** und **Simple Network Management Protocol** aus.

6 Um den Abschnitt „Zulässige IP-Adressen“ anzuzeigen, erweitern Sie einen Dienst.

7 Deaktivieren Sie im Abschnitt „Zulässige IP-Adressen“ die Option **Verbindungen von jeder beliebigen IP-Adresse zulassen** und geben Sie die IP-Adressen der Netzwerke ein, die eine Verbindung zum Host herstellen dürfen.

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

   - 192.168.0.0/24
   - 192.168.1.2, 2001::1/64

- fd3e:29a6:0a81:e478::/64

8 Stellen Sie sicher, dass der Dienst selbst ausgewählt ist.

9 Klicken Sie auf **OK**.

10 Überprüfen Sie Ihre Änderung in der Spalte **Zulässige IP-Adressen** für den Dienst.

Ein- und ausgehende Firewall-Ports für ESXi-Hosts

Öffnen und schließen Sie die Firewall-Ports für jeden Dienst, indem Sie entweder den vSphere Client oder den VMware Host Client verwenden.

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

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

NFS-Client-Firewallverhalten

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

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

Firewallverhalten in NFS v3

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

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

- Wenn `nfsClient` aktiviert ist, bleiben der Status des Regelsatzes und die Richtlinien der zugelassenen IP-Adressen unverändert. Die IP-Adresse des NFS-Servers wird der zugelassenen Liste für ausgehende IP-Adressen hinzugefügt.

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

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

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

Firewallverhalten in NFS v4.1

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

Verwenden von ESXCLI-Firewall-Befehlen zum Konfigurieren des ESXi-Verhaltens

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

Firewall-Befehlsreferenz

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

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

Tabelle 3-6. Firewall-Befehle

Befehl	Beschreibung
`esxcli network firewall get`	Geben Sie den Status der Firewall zurück und listen Sie die Standardaktionen auf.
`esxcli network firewall set --default-action`	Legen Sie „true“ fest, um die Standardaktion auszuführen. Legen Sie „false“ fest, um die Standardaktion nicht auszuführen.
`esxcli network firewall set --enabled`	Aktivieren oder deaktivieren Sie die ESXi-Firewall.
`esxcli network firewall load`	Lädt das Firewallmodul und die Konfigurationsdateien des Regelsatzes.
`esxcli network firewall refresh`	Aktualisiert die Firewall-Konfiguration durch das Einlesen der Regelsatzdateien, wenn das Firewallmodul geladen ist.
`esxcli network firewall unload`	Löscht Filter und entlädt das Firewallmodul.
`esxcli network firewall ruleset list`	Listet Informationen zu Regelsätzen auf.
`esxcli network firewall ruleset set --allowed-all`	Legen Sie „true“ fest, um den Zugriff auf alle IP-Adressen zu erlauben. Legen Sie „false“ fest, um eine Liste mit zulässigen IP-Adressen zu verwenden.
`esxcli network firewall ruleset set --enabled --ruleset-id=<string>`	Setzen Sie „Aktiviert“ auf „true“, um den angegebenen Regelsatz zu aktivieren. Setzen Sie „Aktiviert“ auf „false“, um den angegebenen Regelsatz zu deaktivieren.
`esxcli network firewall ruleset allowedip list`	Listet die zulässigen IP-Adressen des angegebenen Regelsatzes auf.
`esxcli network firewall ruleset allowedip add`	Ermöglicht den Zugriff auf den Regelsatz von der angegebenen IP-Adresse oder einem Bereich von IP-Adressen aus.
`esxcli network firewall ruleset allowedip remove`	Deaktiviert den Zugriff auf den Regelsatz von der angegebenen IP-Adresse oder einem Bereich von IP-Adressen aus.
`esxcli network firewall ruleset rule list`	Listet die Regeln jedes Regelsatzes in der Firewall auf.

Aktivieren oder Deaktivieren eines ESXi-Diensts

Sie können ESXi-Dienste über den vSphere Client aktivieren oder deaktivieren.

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

Hinweis Die Aktivierung von Diensten wirkt sich auf die Sicherheit Ihres Hosts aus. Aktivieren Sie einen Dienst also nur, wenn es absolut notwendig ist.

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

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

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

Tabelle 3-7. 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 auf dem Host, der Remoteverbindungen über die Secure Shell zulässt.
bestätigt	Gestoppt	vSphere Trust Authority-Bestätigungsdienst.
dpd	Gestoppt	Data Protection-Daemon.
Auslastungsbasierter Gruppierungs-Daemon	Wird ausgeführt	Auslastungsbasierte Gruppierung
kmxd	Gestoppt	vSphere Trust Authority-Schlüsselanbieterdienst.
Active Directory-Dienst	Gestoppt	Wenn Sie ESXi für Active Directory konfigurieren, wird dieser Dienst gestartet.
NTP-Daemon	Gestoppt	Network Time Protocol-Daemon
PC/SC Smartcard-Daemon	Gestoppt	Wenn Sie den Host für die Smartcard-Authentifizierung aktivieren, wird dieser Dienst gestartet. Weitere Informationen hierzu finden Sie unter Konfigurieren und Verwalten der Smartcard-Authentifizierung für ESXi.
CIM-Server	Wird ausgeführt	Ein Dienst, der von CIM-Anwendungen (Common Information Model) genutzt werden kann

Tabelle 3-7. ESXi-Dienste im Sicherheitsprofil (Fortsetzung)

Dienst	Standard	Beschreibung
slpd	Gestoppt	Dienstspeicherortprotokoll-Daemon.
SNMP-Server	Gestoppt	SNMP-Daemon. Informationen zur Konfiguration von SNMP v1, v2 und v3 finden Sie in der *vSphere-Überwachung und -Leistung*-Dokumentation.
VTDC-Dienst	Wird ausgeführt	vSphere Distributed Tracing Collector-Dienst.
vltd	Gestoppt	VCDR LWD-Transport-Daemon.
Syslog-Server	Gestoppt	Syslog-Daemon. Syslog kann in den erweiterten Systemeinstellungen in vSphere Client aktiviert werden. Informationen finden Sie in der Dokumentation *Installation und Einrichtung von vCenter Server*.
VMware vCenter Agent	Wird ausgeführt	vCenter Server-Agent. Ermöglicht die Verbindung zwischen vCenter Server und ESXi-Host. vpxa ist der Kommunikationskanal zum Hostdaemon, der wiederum mit dem ESXi-Kernel kommuniziert.
X.Org-Server	Gestoppt	X.Org-Server. Dieses optionale Feature wird intern für 3D-Grafiken in virtuellen Maschinen genutzt.

Voraussetzungen

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

Verfahren

1. Navigieren Sie zu einem ESXi-Host in der Bestandsliste.
2. Klicken Sie auf **Konfigurieren** und dann unter **System** auf **Dienste**.
3. Wählen Sie den Dienst, den Sie ändern möchten.
   a. Wählen Sie für eine einmalige Änderung des Hoststatus **Neustart**, **Starten** oder **Beenden**.
   b. Um den Status des Hosts für mehrere Neustarts zu ändern, klicken Sie auf **Startrichtlinie bearbeiten** und wählen Sie eine Richtlinie aus.
   - **Mit dem Host starten und beenden**: Der Dienst wird unmittelbar nach dem Host gestartet und unmittelbar vor dem Herunterfahren des Hosts beendet. Ähnlich wie bei der Option **Mit Port-Verwendung starten und beenden** besagt diese Option, dass der Dienst regelmäßig versucht, seine Aufgaben abzuschließen, wie z. B. das Herstellen einer Verbindung zum angegebenen NTP-Server. Wenn der Port geschlossen war, später jedoch geöffnet wird, beginnt der Client unmittelbar mit der Erledigung seiner Aufgaben.
   - **Manuell starten und beenden**: Der Host übernimmt unabhängig davon, welche Ports offen oder geschlossen sind, die vom Benutzer festgelegten Diensteinstellungen. Wenn

ein Benutzer den NTP-Dienst startet, wird dieser Dienst so lange ausgeführt, bis der Host ausgeschaltet wird. Wenn der Dienst gestartet und der Host ausgeschaltet wird, wird der Dienst beim Herunterfahren angehalten. Wenn der Host eingeschaltet ist, wird der Dienst erneut gestartet, wobei der vom Benutzer festgelegte Status beibehalten wird.

- **Mit Port-Verwendung starten und beenden**: Die Standardeinstellung für diese Dienste. Falls ein beliebiger Port geöffnet ist, versucht der Client, die Netzwerkressourcen für den Dienst zu kontaktieren. Wenn einige Ports geöffnet sind, der Port für einen bestimmten Dienst aber geschlossen ist, schlägt der Versuch fehl. Wird der zugehörige ausgehende Port geöffnet, beginnt der Dienst mit dem Abschluss des Startvorgangs.

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

4 Klicken Sie auf **OK**.

Konfigurieren und Verwalten des Sperrmodus auf ESXi-Hosts

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

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

Verhalten im Sperrmodus

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

Sperrmodus-Dienste für unterschiedliche Benutzer verfügbar

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

- Im strengen und normalen Sperrmodus haben berechtigte Benutzer über vCenter Server Zugriff auf den Host, und zwar über den vSphere Client oder mit dem vSphere Web Services SDK.
- Das Verhalten der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) ist für den strengen Sperrmodus und den normalen Sperrmodus unterschiedlich.
  - Im strengen Sperrmodus ist der DCUI-Dienst deaktiviert.

  - Im normalen Sperrmodus können Konten in der Liste der ausgenommenen Benutzer auf die DCUI zugreifen, wenn sie über Administratorrechte verfügen. Darüber hinaus können alle Benutzer, die in der erweiterten Systemeinstellung `DCUI.Access` angegeben sind, auf die DCUI zugreifen.
- Falls die ESXi Shell oder SSH aktiviert ist und der Host in den normalen Sperrmodus wechselt, können diese Dienste von Konten in der Liste der ausgenommenen Benutzer mit Administratorrechten verwendet werden. Für alle anderen Benutzer ist ESXi Shell oder SSH deaktiviert. ESXi- oder SSH-Sitzungen werden für Benutzer ohne Administratorrechte geschlossen.

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

Tabelle 3-8. 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	Ausgenommene vCenter (vpxuser)-Benutzer, basierend auf Berechtigungen vCloud Director (vslauser, soweit verfügbar)	Ausgenommene vCenter (vpxuser)-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 Systemeinstellung „`DCUI.Access`“	In der erweiterten Systemeinstellung „`DCUI.Access`“ definierte Benutzer Ausgenommene Benutzer mit Administratorrechten auf dem Host	DCUI-Dienst wird angehalten.
ESXi Shell (falls aktiviert) und SSH (falls aktiviert)	Benutzer mit Administratorrechten auf dem Host	In der erweiterten Option `DCUI.Access` definierte Benutzer Ausgenommene Benutzer mit Administratorrechten auf dem Host	In der erweiterten Systemeinstellung „`DCUI.Access`“ definierte Benutzer Ausgenommene Benutzer mit Administratorrechten auf dem Host

Sperrmodusverhalten für Benutzer, die bei der ESXi Shell angemeldet sind, wenn der Sperrmodus aktiviert ist

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

Vorgehensweise zum Deaktivieren des Sperrmodus

Sie können den Sperrmodus folgendermaßen deaktivieren.

Über den vSphere Client

Benutzer können sowohl den normalen Sperrmodus als auch den strengen Sperrmodus über den vSphere Client deaktivieren. Weitere Informationen finden Sie unter Deaktivieren des Sperrmodus über den vSphere Client.

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. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren des normalen Sperrmodus über die Benutzerschnittstelle der direkten Konsole.

Aktivieren des Sperrmodus über den vSphere Client

Wählen Sie den Sperrmodus aus, damit alle Konfigurationsänderungen vCenter Server durchlaufen müssen. vSphere unterstützt den normalen Sperrmodus und den strengen Sperrmodus.

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

Verfahren

1. Navigieren Sie zum Host im Navigator des vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Sicherheitsprofil**.
4. Klicken Sie im Bereich „Sperrmodus“ auf **Bearbeiten**.

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

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

6 Klicken Sie auf **OK**.

Deaktivieren des Sperrmodus über den vSphere 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.

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

Verfahren

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

2 Klicken Sie auf **Konfigurieren**.

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

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

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

6 Klicken Sie auf **OK**.

Ergebnisse

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

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

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

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

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

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

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

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

Verfahren

1. Drücken Sie F2 an der Benutzerschnittstelle der direkten Konsole des Hosts und melden Sie sich an.
2. Führen Sie einen Bildlauf nach unten zur Einstellung **Sperrmodus konfigurieren** aus und drücken Sie die Eingabetaste, um die aktuelle Einstellung umzuschalten.
3. Drücken Sie die Esc-Taste wiederholt, bis Sie zurück zum Hauptmenü der Benutzerschnittstelle der direkten Konsole gelangt sind.

Angeben von Konten mit Zugriffsrechten im Sperrmodus

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

Funktionsweise von Konten bei aktiviertem Sperrmodus in vSphere

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

- In vSphere 5.0 und früheren Versionen kann sich nur der Root-Benutzer bei der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) auf einem ESXi-Host anmelden, der sich im Sperrmodus befindet.

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

  Ausgenommene Benutzer geben Sie über den vSphere Client an.

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

Hinzufügen von Benutzern zur erweiterten Systemeinstellung „DCUI.Access“

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

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

1. Navigieren Sie zum Host im Navigator von vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen** und dann auf **Bearbeiten**.
4. Filtern Sie nach „DCUI“.
5. Geben Sie im Textfeld **DCUI.Access** die lokalen ESXi-Benutzernamen durch Komma getrennt ein.

   Hinweis Sie können keine Active Directory Benutzer eingeben. Es werden nur lokale ESXi-Benutzer unterstützt.

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

6 Klicken Sie auf **OK**.

Angeben der Benutzerausnahmen für den Sperrmodus

Sie können Benutzer über den vSphere Client zur Liste „Ausgenommene Benutzer“ hinzufügen. Diese Benutzer verlieren ihre Berechtigungen nicht, wenn der Host in den Sperrmodus wechselt.

Bei diesen Benutzern handelt es sich gewöhnlich um Konten, die Drittanbieterlösungen und externe Anwendungen darstellen, die auch im Sperrmodus weiterhin funktionieren müssen. Beispielsweise ist es sinnvoll, Dienstkonten wie beispielsweise einen Backup-Agenten zur Liste „Ausnahme für Benutzer“ hinzuzufügen.

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

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

1 Navigieren Sie zum Host im Navigator von vSphere Client.

2 Klicken Sie auf **Konfigurieren**.

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

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

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

6 Klicken Sie auf **OK**.

Durchführen sicherer Updates mithilfe von vSphere-Installationspaketen

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

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

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

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

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

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

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

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

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

Verwalten der Akzeptanzebenen von ESXi-Hosts und vSphere-Installationspaketen

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

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

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

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

Folgende Akzeptanzebenen werden unterstützt:

VMwareCertified

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

VMwareAccepted

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

PartnerSupported

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

CommunitySupported

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

Verfahren

1. Stellen Sie mithilfe von SSH eine Verbindung mit jedem ESXi-Host her.
2. Stellen Sie sicher, dass die Akzeptanzebene auf „VMwareCertified“, „VMwareAccepted“ oder „PartnerSupported“ gesetzt ist, indem Sie den folgenden Befehl ausführen.

   ```
   esxcli software acceptance get
   ```

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

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

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

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

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

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

Ergebnisse

Die neue Akzeptanzebene ist wirksam.

Hinweis ESXi führt Integritätsprüfungen von VIBs durch, die von der Akzeptanzebene gesteuert werden. Mithilfe der Einstellung `VMkernel.Boot.execInstalledOnly` können Sie ESXi anweisen, nur Binärdateien auszuführen, die aus einem gültigen auf dem Host installierten VIB stammen. Gemeinsam mit Secure Boot stellt diese Einstellung sicher, dass jeder einzelne jemals auf einem ESXi-Host ausgeführte Prozess signiert, zugelassen und erwartet wird. Standardmäßig ist die Einstellung `VMkernel.Boot.execInstalledOnly` für Partnerkompatibilität in vSphere 7.0 und höher aktiviert. Die Aktivierung dieser Einstellung (soweit möglich) verbessert die Sicherheit. Weitere Informationen zum Konfigurieren erweiterter Optionen für ESXi finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/1038578.

Zuweisen von Rechten für ESXi-Hosts

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

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

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

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

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

Zuweisen von Berechtigungen für eigenständige ESXi-Hosts

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

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

Die folgenden Rollen sind vordefiniert.

Nur Lesen

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

Administrator

Administratorrolle.

Kein Zugriff

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

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

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

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

Vordefinierte ESXi-Benutzer und -Rechte

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

Root-Benutzer

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

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

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

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

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

vpxuser-Benutzer

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

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

Sie können den vpxuser-Benutzer nicht mithilfe von Active Directory verwalten.

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

dcui-Benutzer

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

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

Deaktivieren des Shell-Zugriffs für Nicht-Root-ESXi-Benutzer

In vSphere 8.0 und höher können Sie den Shell-Zugriff für Nicht-Root-ESXi-Benutzer deaktivieren, z. B. für die vordefinierten Benutzer „vpxuser“ und „dcui“. Durch Deaktivieren des Shell-Zugriffs können Sie die Sicherheit erhöhen, indem Sie für diese Benutzer „nur API“ erzwingen.

Um den Shell-Zugriff zu deaktivieren, können Sie den Befehl `esxcli system account set --id` *user* `--shell-access false` verwenden. Die entsprechende API lautet `LocalAccountManager.updateUser`. Sie können auch den VMware Host Client verwenden, um das Flag „Shell-Zugriff aktivieren“ von lokalen ESXi-Benutzern zu ändern.

Hinweis Wenn Sie den Shell-Zugriff für einen Benutzer mit Administratorzugriff deaktivieren, kann dieser Benutzer anderen Benutzern weder Shell-Zugriff gewähren noch die Kennwörter von Benutzern mit Shell-Zugriff ändern, da ihm der Shell-Zugriff verweigert wird. Mit anderen Berechtigungen, z. B. Hostprofilen, können Benutzer wie „vpxuser“ und „dcui“ weiterhin Kennwörter anderer Benutzer ändern.

Wenn Sie solche Änderungen vornehmen, stellen Sie sicher, dass diese vorhandene Workflows von Drittanbietern nicht beeinträchtigen.

Verwenden von Active Directory zum Verwalten von ESXi-Benutzern

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

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

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

Konfigurieren eines ESXi-Hosts für die Verwendung von Active Directory

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

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

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

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

Voraussetzungen

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

  vollqualifizierter Domänenname = Hostname.Domänenname

Verfahren

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

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

2 Stellen Sie sicher, dass die DNS-Server, die Sie für den Host konfiguriert haben, die Hostnamen für die Active Directory-Controller auflösen können.

   a Navigieren Sie zum Host im Navigator von vSphere Client.

   b Klicken Sie auf **Konfigurieren**.

   c Klicken Sie unter Netzwerk auf **TCP/IP-Konfiguration**.

   d Klicken Sie unter TCP/IP Stack: Standard auf **DNS** und stellen Sie sicher, dass der Hostname und die DNS-Server-Informationen für den Host richtig sind.

Nächste Schritte

Fügen Sie den Host zu einer Verzeichnisdienstdomäne hinzu. Weitere Informationen hierzu finden Sie unter Hinzufügen eines ESXi-Hosts zu einer Verzeichnisdienst-Domäne. Für Hosts, die mit Auto Deploy bereitgestellt wurden, müssen Sie vSphere Authentication Proxy einrichten. Weitere Informationen hierzu finden Sie unter Verwenden des vSphere Authentication Proxy. Sie können Berechtigungen konfigurieren, damit Benutzer und Gruppen aus der hinzugefügten Active Directory-Domäne auf die vCenter Server-Komponenten zugreifen können. Informationen zum Verwalten von Berechtigungen finden Sie unter Hinzufügen einer Berechtigung zu einem Bestandslistenobjekt .

Hinzufügen eines ESXi-Hosts zu einer Verzeichnisdienst-Domäne

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

Sie können den Domänennamen auf zwei Arten eingeben:

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

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

Verfahren

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

2 Klicken Sie auf **Konfigurieren**.

3 Wählen Sie unter „System“ die Option **Authentifizierungsdienste**.

4 Klicken Sie auf **Domäne beitreten**.

5 Geben Sie eine Domäne ein.

   Verwenden Sie das Fomular **`name.tld`** oder **`name.tld/container/path`**.

6 Geben Sie den Benutzernamen und das Kennwort eines Verzeichnisdienstbenutzers ein, der über die Berechtigung verfügt, den Host mit der Domäne zu verbinden, und klicken Sie auf **OK**.

7 (Optional) Wenn Sie einen Authentifizierungs-Proxy verwenden möchten, geben Sie die IP-Adresse des Proxy-Servers ein.

8 Klicken Sie auf **OK** um das Dialogfeld für die Verzeichnisdienstkonfiguration zu schließen.

Nächste Schritte

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

Anzeigen der Verzeichnisdiensteinstellungen für einen ESXi-Host

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

Verfahren

1 Navigieren Sie zum Host im Navigator des vSphere Client.

2 Klicken Sie auf **Konfigurieren**.

3 Wählen Sie unter „System“ die Option **Authentifizierungsdienste**.

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

Nächste Schritte

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

Verwenden des vSphere Authentication Proxy

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

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

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

Auto Deploy

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

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

Weitere Informationen hierzu finden Sie unter Festlegen von Auto Deploy als untergeordnete Zertifizierungsstelle.

Andere ESXi-Hosts

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

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

Hinweis IPv6 wird auf vSphere durchgehend unterstützt. Auf vSphere with Tanzu wird IPv6 nicht unterstützt.

Starten des vSphere Authentication Proxy-Diensts

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

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

Voraussetzungen

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

Verfahren

1 Starten Sie den VMware vSphere Authentication Proxy-Dienst.

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

2 Bestätigen Sie, dass der Dienst erfolgreich gestartet wurde.

Ergebnisse

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

Hinzufügen einer Domäne zu vSphere Authentication Proxy mit dem vSphere Client

Sie können mit dem vSphere Client eine Domäne zu vSphere Authentication Proxy hinzufügen.

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

Verfahren

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

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

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

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

5 Klicken Sie auf **Speichern**.

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

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

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

Verfahren

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

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

```
shell
```

3 Wechseln Sie zum Verzeichnis `/usr/lib/vmware-vmcam/bin/`, in dem sich das Skript **camconfig** befindet.

4 Um die Active Directory-Anmeldedaten für Domäne und Benutzer der Authentication Proxy-Konfiguration hinzuzufügen, führen Sie den folgenden Befehl aus.

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

Sie werden zur Eingabe eines Kennworts aufgefordert.

vSphere Authentication Proxy speichert diesen Benutzernamen und das Kennwort. Sie können den Benutzer nach Bedarf entfernen und neu erstellen. Die Domäne muss über DNS erreichbar sein. Es muss sich aber nicht um eine vCenter Single Sign-On-Identitätsquelle handeln.

vSphere Authentication Proxy verwendet den vom *Benutzer* angegebenen Benutzernamen, um die Konten für ESXi-Hosts in Active Directory zu erstellen. Der Benutzer muss über Berechtigungen zum Erstellen von Konten in der Active Directory-Domäne verfügen, zu der Sie die Hosts hinzufügen. Zum Zeitpunkt der Zusammenstellung dieser Informationen enthielt der Microsoft Knowledge Base-Artikel 932455 Hintergrundinformationen zu den Kontoerstellungsberechtigungen.

5 Wenn Sie später die Domäne und die Benutzerinformationen aus vSphere Authentication Proxy entfernen möchten, führen Sie folgenden Befehl aus.

```
camconfig remove-domain -d domain
```

Verwenden des vSphere Authentication Proxy zum Hinzufügen eines Hosts zu einer Domäne

Der Auto Deploy-Server fügt alle Hosts hinzu, die er für vSphere Authentication Proxy bereitstellt, und vSphere Authentication Proxy fügt diese Hosts zur Domäne hinzu. Wenn Sie mithilfe von vSphere Authentication Proxy weitere Hosts zu einer Domäne hinzufügen möchten, können Sie diese Hosts explizit zu vSphere Authentication Proxy hinzufügen. Danach fügt der vSphere Authentication Proxy-Server diese Hosts zur Domäne hinzu. Folglich müssen vom Benutzer angegebene Anmeldeinformationen nicht mehr an das vCenter Server-System übermittelt werden.

Sie können den Domänennamen auf zwei Arten eingeben:

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

Voraussetzungen

- Wenn der ESXi-Host ein VMCA-signiertes Zertifikat verwendet, stellen Sie sicher, dass der Host zum vCenter Server hinzugefügt wurde. Anderenfalls kann der Authentication Proxy-Dienst dem ESXi-Host nicht vertrauen.
- Wenn der ESXi-Host ein von einer Stammzertifizierungsstelle signiertes Zertifikat verwendet, stellen Sie sicher, dass das entsprechende von einer Stammzertifizierungsstelle signierte Zertifikat zum vCenter Server-System hinzugefügt wurde. Weitere Informationen hierzu finden Sie unter Verwalten von Zertifikaten für ESXi-Hosts.

Verfahren

1 Navigieren Sie zum Host im Navigator von vSphere Client.

2 Klicken Sie auf **Konfigurieren**.

3 Wählen Sie unter **System** die Option **Authentifizierungsdienste**.

4 Klicken Sie auf **Domäne beitreten**.

5 Geben Sie eine Domäne ein.

Verwenden Sie das Format **name.tld** (Beispiel: **meinedomaene.com**) oder **name.tld/container/pfad** (Beispiel: **meinedomaene.com/organisationseinheit1/organisationseinheit2**).

6 Wählen Sie **Proxy-Server verwenden** aus.

7 Geben Sie die IP-Adresse des Authentication Proxy-Servers ein. Diese Adresse ist mit der IP-Adresse des vCenter Server-Systems identisch.

8 Klicken Sie auf **OK**.

Aktivieren von Clientauthentifizierung für vSphere Authentication Proxy

Standardmäßig fügt vSphere Authentication Proxy einen beliebigen Host hinzu, wenn die IP-Adresse dieses Hosts in seiner Zugriffssteuerungsliste vorhanden ist. Zur zusätzlichen Sicherheit können Sie die Clientauthentifizierung aktivieren. Wenn die Clientauthentifizierung aktiviert ist, überprüft vSphere Authentication Proxy auch das Zertifikat des Hosts.

Voraussetzungen

- Stellen Sie sicher, dass das vCenter Server-System dem Host vertraut. Wenn Sie einen Host zu vCenter Server hinzufügen, wird dem Host standardmäßig ein Zertifikat zugewiesen, das von einer vCenter Server vertrauenswürdigen Stammzertifizierungsstelle signiert ist. vSphere Authentication Proxy vertraut vCenter Server vertrauenswürdiger Stammzertifizierungsstelle.
- Wenn Sie vorhaben, ESXi-Zertifikate in Ihrer Umgebung zu ersetzen, nehmen Sie die Ersetzung vor, bevor Sie den vSphere Authentication Proxy aktivieren. Die Zertifikate auf dem ESXi-Host müssen mit denen der Host-Registrierung übereinstimmen.

Verfahren

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

2 Um Zugriff auf die Bash-Shell zu aktivieren, führen Sie den Befehl `shell` aus.

3 Wechseln Sie zum Verzeichnis `/usr/lib/vmware-vmcam/bin/`, in dem sich das Skript **camconfig** befindet.

4 Führen Sie zum Aktivieren der Clientauthentifizierung den folgenden Befehl aus.

```
camconfig ssl-cliAuth -e
```

Ab diesem Zeitpunkt prüft vSphere Authentication Proxy das Zertifikat von jedem Host, der hinzugefügt wird.

5 Wenn Sie die Clientauthentifizierung später erneut deaktivieren möchten, führen Sie den folgenden Befehl aus.

```
camconfig ssl-cliAuth -n
```

Importieren des vSphere Authentication Proxy-Zertifikats in den ESXi-Host

Standardmäßig erfordern ESXi-Hosts eine explizite Verifizierung des vSphere Authentication Proxy-Zertifikats. Wenn Sie vSphere Auto Deploy verwenden, übernimmt der Auto Deploy-Dienst das Hinzufügen des Zertifikats zu den Hosts, die er bereitstellt. Bei anderen Hosts müssen Sie das Zertifikat explizit hinzufügen.

Voraussetzungen

- Laden Sie das vSphere Authentication Proxy-Zertifikat auf einen Datenspeicher, auf den der ESXi-Host zugreifen kann. Mit einer SFTP-Anwendung wie WinSCP können Sie das Zertifikat vom vCenter Server-Host am folgenden Speicherort herunterladen.

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

- Stellen Sie sicher, dass die fortgeschrittene Einstellung für `UserVars.ActiveDirectoryVerifyCAMCertificate` ESXi auf 1 festgelegt ist (Standardwert).

Verfahren

1. Wählen Sie den ESXi-Host aus und klicken Sie auf **Konfigurieren**.
2. Wählen Sie unter **System** die Option **Authentifizierungsdienste**.
3. Klicken Sie auf **Zertifikat importieren**.
4. Geben Sie den Pfad zur Zertifikatsdatei im Format `[`*`Datenspeicher`*`]/`*`Pfad/Zertifikatsname`*`.crt` ein.
5. Geben Sie die IP-Adresse des vSphere Authentication Proxy-Servers ein.
6. Klicken Sie auf **OK**.

Erstellen eines neuen Zertifikats für vSphere Authentication Proxy

Sie können ein neues von VMware Certificate Authority (VMCA) bereitgestelltes Zertifikat oder ein neues Zertifikat erstellen, das VMCA als untergeordnetes Zertifikat enthält.

Wenn Sie ein benutzerdefiniertes Zertifikat verwenden möchten, das von der Zertifizierungsstelle eines Drittanbieters oder Unternehmens signiert wurde, finden Sie weitere Informationen unter Einrichten von vSphere Authentication Proxy für die Verwendung von benutzerdefinierten Zertifikaten.

Voraussetzungen

Sie müssen über Root- oder Administratorrechte auf dem System verfügen, auf dem der vSphere Authentication Proxy ausgeführt wird.

Verfahren

1 Erstellen Sie eine Kopie der Datei `certool.cfg`.

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

2 Fügen Sie in die Kopie Informationen über Ihre Organisation ein, wie im folgenden Beispiel beschrieben.

```
Country = IE
Name = vmcam
Organization = VMware
OrgUnit = vTSU
State = Cork
Locality = Cork
Hostname = test-cam-1.test1.vmware.com
```

3 Erzeugen Sie den neuen privaten Schlüssel in `/var/lib/vmware/vmcam/ssl/`.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=/var/lib/vmware/vmcam/ssl/rui.key --
pubkey=/tmp/vmcam.pub --server=localhost
```

Geben Sie unter *localhost* den FQDN des vCenter Servers an.

4 Erzeugen Sie das neue Zertifikat in `/var/lib/vmware/vmcam/ssl/` unter Verwendung des Schlüssels und der Datei `vmcam.cfg`, die Sie in Schritt 1 und Schritt 2 erstellt haben.

```
/usr/lib/vmware-vmca/bin/certool --server=localhost --gencert --privkey=/var/lib/
vmware/vmcam/ssl/rui.key --cert=/var/lib/vmware/vmcam/ssl/rui.crt --config=/var/lib/vmware/
vmcam/ssl/vmcam.cfg
```

Geben Sie unter *localhost* den FQDN des vCenter Servers an.

Einrichten von vSphere Authentication Proxy für die Verwendung von benutzerdefinierten Zertifikaten

Für das Verwenden von benutzerdefinierten Zertifikaten mit vSphere Authentication Proxy sind mehrere Schritte erforderlich. Als Erstes generieren Sie einen CSR und leiten diesen zum Signieren an Ihre Zertifizierungsstelle weiter. Dann speichern Sie das signierte Zertifikat und die Schlüsseldatei an einem Speicherort, auf den vSphere Authentication Proxy zugreifen kann.

Standardmäßig generiert vSphere Authentication Proxy einen CSR während des anfänglichen Startvorgangs und fordert VMCA auf, diesen CSR zu signieren. vSphere Authentication Proxy verwendet dieses Zertifikat, um sich bei vCenter Server zu registrieren. Sie können benutzerdefinierte Zertifikate in Ihrer Umgebung verwenden, wenn Sie diese Zertifikate zu vCenter Server hinzufügen.

Verfahren

1 Generieren Sie einen CSR für vSphere Authentication Proxy.

a Erstellen Sie die Konfigurationsdatei `/var/lib/vmware/vmcam/ssl/vmcam.cfg` nach dem nachfolgenden Beispiel.

```
[ req ]
distinguished_name = req_distinguished_name
encrypt_key = no
prompt = no
string_mask = nombstr
req_extensions = v3_req
[ v3_req ]
basicConstraints = CA:false
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = DNS:vcenter1.example.com
[ req_distinguished_name ]
countryName = US
stateOrProvinceName = NY
localityName = New York
0.organizationName = Example Inc.
organizationalUnitName = IT Org
commonName = vcenter1.example.com
```

Beachten Sie Folgendes:

- subjectAltName: Verwenden Sie das Format **DNS:***FQDN_der_vCenter_Appliance_zum_Verwenden_des_CA-signierten_Zertifikats*.
- commonName: Verwenden Sie denselben FQDN der vCenter Appliance, die in subjectAltName verwendet wird.

b Führen Sie unter Angabe der Konfigurationsdatei `openssl` aus, um eine CSR- und eine Schlüsseldatei zu generieren.

```
openssl req -new -nodes -out vmcam.csr -newkey rsa:2048 -keyout /var/lib/vmware/
vmcam/ssl/rui.key -config /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

2 Sichern Sie die Zertifikatsdateien `rui.crt` und `rui.key`, welche sich im folgenden Speicherort befinden.

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

3 Heben Sie die Registrierung von vSphere Authentication Proxy auf.

   a Navigieren Sie zum Verzeichnis `/usr/lib/vmware-vmcam/bin`, in dem sich das Skript `camregister` befindet.

   b Führen Sie den folgenden Befehl aus.

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

   Benutzer muss ein vCenter Single Sign-On-Benutzer mit Administratorberechtigungen für vCenter Server sein.

4 Halten Sie den vSphere Authentication Proxy-Dienst an.

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

5 Ersetzen Sie die bestehenden Zertifikatsdateien `rui.crt` und `rui.key` durch die Dateien, die Sie von Ihrer Zertifizierungsstelle erhalten haben.

6 Starten Sie den vSphere Authentication Proxy-Dienst neu.

7 Registrieren Sie vSphere Authentication Proxy mithilfe des neuen Zertifikats und des neuen Schlüssels explizit bei vCenter Server neu.

```
camregister --register -a VC_address -u user -c full_path_to_rui.crt -k
full_path_to_rui.key
```

Konfigurieren und Verwalten der Smartcard-Authentifizierung für ESXi

Sie können sich mit der Smartcard-Authentifizierung bei der ESXi-Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) anmelden, indem Sie eine persönliche Identitätsprüfung (Personal Identity Verification, PIV), eine allgemeine Zugriffskarte (Common Access Card, CAC) oder eine SC650-Smartcard anstelle der Eingabe eines Benutzernamens und eines Kennworts verwenden.

Eine Smartcard (Chipkarte) ist eine kleine Plastikkarte mit einem integrierten Schaltkreis (Chip). Viele staatliche Behörden und große Unternehmen verwenden eine auf Smartcards basierende Zwei-Faktor-Authentifizierung, um die Sicherheit ihrer Systeme zu erhöhen und bestehende Sicherheitsbestimmungen zu erfüllen.

Wenn die Smartcard-Authentifizierung auf einem ESXi-Host aktiviert ist, werden Sie von der DCUI zur Eingabe einer Smartcard und einer PIN-Kombination anstelle des standardmäßigen Benutzernamens und Kennworts aufgefordert.

1 Wenn Sie die Smartcard in den Kartenleser stecken, liest der ESXi-Host die darauf gespeicherten Anmeldedaten.

2 Die ESXi-DCUI zeigt Ihre Anmeldekennung an und fordert Sie zur Eingabe Ihrer PIN auf.

3 Nach der Eingabe Ihrer PIN vergleicht der ESXi-Host sie mit der auf der Smartcard gespeicherten PIN und überprüft das Zertifikat auf der Smartcard mit Active Directory.

4 Nach erfolgreicher Prüfung des Smartcard-Zertifikats schließt ESXi die Anmeldung bei der DCUI ab.

Sie können durch Drücken von F3 zur Benutzernamen- und Kennwort-Authentifizierung über die DCUI wechseln.

Nach einigen aufeinanderfolgenden falschen PIN-Eingaben (gewöhnlich drei) wird die Smartcard gesperrt. Eine gesperrte Smartcard kann nur von ausgewähltem Personal entsperrt werden.

Aktivieren der Smartcard-Authentifizierung

Aktivieren Sie die Smartcard-Authentifizierung, um eine Chipkarte und eine PIN-Kombination zum Anmelden bei der ESXi-DCUI zu verlangen.

Voraussetzungen

- Richten Sie die Infrastruktur zur Smartcard-Authentifizierung ein, wie beispielsweise Konten in der Active Directory-Domäne, Smartcard-Lesegeräte und Smartcards.
- Konfigurieren Sie ESXi für den Beitritt zu einer Active Directory-Domäne, die die Smartcard-Authentifizierung unterstützt. Weitere Informationen finden Sie unter Verwenden von Active Directory zum Verwalten von ESXi-Benutzern .
- Verwenden Sie den vSphere Client zum Hinzufügen von Stammzertifikaten. Weitere Informationen hierzu finden Sie unter Verwalten von Zertifikaten für ESXi-Hosts.

Verfahren

1 Navigieren Sie zum Host im Navigator des vSphere Client.

2 Klicken Sie auf **Konfigurieren**.

3 Wählen Sie unter „System“ die Option **Authentifizierungsdienste**.

Der aktuelle Status der Smartcard-Authentifizierung und eine Liste mit importierten Zertifikaten werden angezeigt.

4 Klicken Sie im Fensterbereich „Smartcard-Authentifizierung“ auf **Bearbeiten**.

5 Wählen Sie im Dialogfeld zum Bearbeiten der Smartcard-Authentifizierung die Seite für Zertifikate aus.

6 Fügen Sie vertrauenswürdige CA-Zertifikate hinzu, zum Beispiel Zertifikate von Root- und zwischengeschalteten Zertifizierungsstellen (CA).

   Zertifikate müssen im PEM-Format sein.

7 Öffnen Sie die Seite „Smartcard-Authentifizierung“, aktivieren Sie das Kontrollkästchen **Smartcard-Authentifizierung aktivieren** und klicken Sie auf **OK**.

Deaktivieren der Smartcard-Authentifizierung

Deaktivieren Sie die Smartcard-Authentifizierung, um zur standardmäßigen Authentifizierung mit Benutzernamen und Kennwort bei der ESXi-DCUI-Anmeldung zurückzukehren.

Verfahren

1 Navigieren Sie zum Host im Navigator des vSphere Client.

2 Klicken Sie auf **Konfigurieren**.

3 Wählen Sie unter „System“ die Option **Authentifizierungsdienste**.

   Der aktuelle Status der Smartcard-Authentifizierung und eine Liste mit importierten Zertifikaten werden angezeigt.

4 Klicken Sie im Fensterbereich „Smartcard-Authentifizierung“ auf **Bearbeiten**.

5 Deaktivieren Sie auf der Seite „Smartcard-Authentifizierung“ das Kontrollkästchen **Smartcard-Authentifizierung aktivieren** und klicken Sie auf **OK**.

Authentifizieren mit Benutzernamen und Kennwort bei Verbindungsproblemen

Sollte der Active Directory-(AD-)Domänenserver nicht erreichbar sein, können Sie sich bei der ESXi-DCUI mit Benutzername-und-Kennwort-Authentifizierung anmelden und Notfallmaßnahmen auf dem Host ergreifen.

In Ausnahmefällen kann es vorkommen, dass der AD-Domänenserver aufgrund von Verbindungsproblemen, Netzwerkausfällen oder Naturkatastrophen nicht erreichbar ist und die Benutzeranmeldedaten auf der Smartcard nicht authentifiziert werden können. In diesem Fall können Sie sich bei der ESXi-DCUI mit den Anmeldeinformationen eines lokalen ESXi-Administratorbenutzers anmelden. Nach der Anmeldung können Sie Diagnosen oder andere Notfallmaßnahmen durchführen. Der Fallback auf die Anmeldung mit Benutzernamen und Kennwort wird im Protokoll vermerkt. Sobald die Verbindung mit AD wieder hergestellt ist, ist auch die Smartcard-Authentifizierung wieder verfügbar.

Hinweis Der Verlust der Netzwerkverbindung zu vCenter Server hat keinen Einfluss auf die Smartcard-Authentifizierung, solange der Active Directory-Domänenserver verfügbar bleibt.

Verwenden der Smartcard-Authentifizierung im Sperrmodus

Wenn aktiviert, erhöht der Sperrmodus auf dem ESXi-Host die Sicherheit des Hosts und beschränkt den Zugriff auf die DCUI. Der Sperrmodus kann dazu führen, dass die Smartcard-Authentifizierung nicht mehr funktioniert.

Im normalen Sperrmodus haben nur Benutzer, die Administratorrechte besitzen und in der Liste der ausgenommenen Benutzer geführt werden, Zugriff auf die DCUI. Ausgenommene Benutzer sind lokale Hostbenutzer oder Active Directory-Benutzer mit lokal für den ESXi-Host definierten Rechten. Wenn Sie die Smartcard-Authentifizierung auch im normalen Sperrmodus nutzen möchten, müssen Sie Benutzer mithilfe des vSphere Client in die Liste der ausgenommenen Benutzer aufnehmen. Diese Benutzer behalten ihre Berechtigungen auch dann, wenn der Host in den normalen Sperrmodus versetzt wird, und können sich auch weiterhin bei der DCUI anmelden. Weitere Informationen finden Sie unter Angeben der Benutzerausnahmen für den Sperrmodus.

Im strengen Sperrmodus wird der DCUI-Dienst beendet. Daher ist auch kein Zugriff auf den Host über Smartcard-Authentifizierung möglich.

Verwenden der ESXi Shell

Die ESXi Shell stellt wichtige Wartungsbefehle bereit und 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.

Dies sind die Anwendungsdienste:

ESXi Shell

Aktivieren Sie diesen Dienst, um lokal auf die ESXi Shell zuzugreifen.

SSH

Aktivieren Sie diesen Dienst, um die ESXi Shell remote über SSH aufzurufen.

Der Root-Benutzer und Benutzer mit der Rolle „Administrator“ können auf die ESXi Shell zugreifen. Benutzern, die zur Active Directory-Gruppe „ESX Admins“ gehören, wird automatisch die Rolle „Administrator“ zugewiesen. Standardmäßig kann nur der Root-Benutzer Systembefehle (z. B. `vmware -v`) über die ESXi Shell ausführen.

Hinweis Aktivieren Sie die ESXi Shell nur, wenn dies wirklich erforderlich ist.

Weitere Themen zum Lesen

- Festlegen der Zeitüberschreitungswerts für Leerlauf für die ESXi Shell mithilfe des vSphere Client

  Wenn Sie die ESXi Shell auf einem Host aktivieren, sich aber nicht von der Sitzung abmelden, bleibt die Sitzung im Leerlauf für unbestimmte Zeit bestehen. Die offene Verbindung erhöht die Möglichkeit für einen privilegierten Zugriff auf den Host. Verhindern Sie dies, indem Sie eine Zeitüberschreitung für Sitzungen im Leerlauf festlegen.

- Festlegen eines Zeitüberschreitungswerts für Verfügbarkeit für die ESXi Shell mithilfe des vSphere Client

  Die ESXi Shell ist standardmäßig deaktiviert. Sie können einen Zeitüberschreitungswert für die Verfügbarkeit für die ESXi Shell festlegen, um die Sicherheit beim Aktivieren der Shell zu erhöhen.

- Festlegen von Zeitüberschreitungswerten für Verfügbarkeit oder Leerlauf für die ESXi Shell mithilfe der DCUI

  Die ESXi Shell ist standardmäßig deaktiviert. Zur Erhöhung der Sicherheit beim Aktivieren der Shell können Sie einen Zeitüberschreitungswert für Verfügbarkeit und/oder Leerlauf festlegen.

- Aktivieren des Zugriffs auf ESXi Shell mithilfe des vSphere Client

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

- Aktivieren des Zugriffs auf die ESXi Shell mithilfe der DCUI

  Mithilfe der Benutzerschnittstelle der direkten Konsole (DCUI) können Sie lokal unter Verwendung textbasierter Menüs mit dem Hosts interagieren. Wägen Sie ab, ob die Sicherheitsanforderungen Ihrer Umgebung die Direct Console User Interface unterstützen.

- Anmelden bei der ESXi Shell zur Fehlerbehebung

  Führen Sie ESXi-Konfigurationsaufgaben mit vSphere Client, ESXCLI oder VMware PowerCLI aus. Melden Sie sich bei der ESXi Shell (vormals Support-Modus oder TSM) nur zwecks Fehlerbehebung an.

Festlegen der Zeitüberschreitungswerts für Leerlauf für die ESXi Shell mithilfe des vSphere Client

Wenn Sie die ESXi Shell auf einem Host aktivieren, sich aber nicht von der Sitzung abmelden, bleibt die Sitzung im Leerlauf für unbestimmte Zeit bestehen. Die offene Verbindung erhöht die Möglichkeit für einen privilegierten Zugriff auf den Host. Verhindern Sie dies, indem Sie eine Zeitüberschreitung für Sitzungen im Leerlauf festlegen.

Der Zeitüberschreitungswert für die Leerlaufzeit gibt die Zeitspanne an, die verstreichen darf, bis ein Benutzer bei interaktiven Sitzungen, die sich im Leerlauf befinden, abgemeldet wird. Sie können die Zeit sowohl für lokale als auch Remote-Sitzungen (SSH) vom Direct Console Interface (DCUI) oder vom vSphere Client aus steuern.

Verfahren

1. Navigieren Sie zum Host im Navigator des vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
4. Klicken Sie auf **Bearbeiten**, wählen Sie `UserVars.ESXiShellInteractiveTimeOut` aus und geben Sie die Einstellung für die Zeitüberschreitung ein.

   Mit dem Wert NULL (0) wird die Leerlaufzeit deaktiviert.
5. Sie müssen den ESXi Shell-Dienst neu starten, damit die Einstellungen wirksam werden.
   a. Wechseln Sie zu **System > Dienste**.
   b. Wählen Sie nacheinander „ESXi Shell“ und „SSH“ aus und klicken Sie auf **Neustart**.

Ergebnisse

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

Festlegen eines Zeitüberschreitungswerts für Verfügbarkeit für die ESXi Shell mithilfe des vSphere Client

Die ESXi Shell ist standardmäßig deaktiviert. Sie können einen Zeitüberschreitungswert für die Verfügbarkeit für die ESXi Shell festlegen, um die Sicherheit beim Aktivieren der Shell zu erhöhen.

Der Zeitüberschreitungswert für die Verfügbarkeit gibt die Zeitspanne an, während der Sie sich nach der Aktivierung der ESXi Shell anmelden müssen. Nach Ablauf dieser Zeitspanne wird der Dienst deaktiviert und die Benutzer können sich nicht mehr anmelden.

Verfahren

1. Navigieren Sie zum Host im Navigator des vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.

4 Klicken Sie auf **Bearbeiten** und wählen Sie `UserVars.ESXiShellTimeOut` aus.

5 Geben Sie den Zeitüberschreitungswert für den Leerlauf ein.

6 Klicken Sie auf **OK**.

7 Sie müssen den ESXi Shell-Dienst neu starten, damit die Einstellungen wirksam werden.

   a Wechseln Sie zu **System > Dienste**.

   b Wählen Sie nacheinander „ESXi Shell“ und „SSH“ aus und klicken Sie auf **Neustart**.

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.

Festlegen von Zeitüberschreitungswerten für Verfügbarkeit oder Leerlauf für die ESXi Shell mithilfe der DCUI

Die ESXi Shell ist standardmäßig deaktiviert. Zur Erhöhung der Sicherheit beim Aktivieren der Shell können Sie einen Zeitüberschreitungswert für Verfügbarkeit und/oder Leerlauf festlegen.

Die beiden Zeitüberschreitungstypen treten in verschiedenen Situationen auf.

ESXi Shell-Leerlauf-Zeitüberschreitung

Wenn ein Benutzer die ESXi Shell auf einem Host aktiviert, aber vergisst, sich von der Sitzung abzumelden, bleibt die Sitzung im Leerlauf für unbestimmte Zeit bestehen. Die offene Verbindung kann die Möglichkeit für einen privilegierten Zugriff auf den Host erhöhen. Diese Situation können Sie verhindern, indem Sie eine Zeitüberschreitung für Sitzungen im Leerlauf festlegen.

ESXi Shell-Verfügbarkeits-Zeitüberschreitung

Der Zeitüberschreitungswert für Verfügbarkeit bestimmt, wie viel Zeit bis zur Anmeldung nach der anfänglichen Aktivierung der Shell vergehen kann. Wenn Sie länger warten, wird der Dienst deaktiviert und eine Anmeldung bei der ESXi Shell ist nicht möglich.

Voraussetzungen

Aktivieren Sie ESXi Shell. Weitere Informationen hierzu finden Sie unter Aktivieren des Zugriffs auf die ESXi Shell mithilfe der DCUI.

Verfahren

1 Melden Sie sich beim ESXi Shell an.

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

3 Geben Sie den Zeitüberschreitungswert für Leerlauf (in Sekunden) oder den Zeitüberschreitungswert für Verfügbarkeit ein.

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

5 Klicken Sie auf **OK**.

6 Sie müssen den ESXi Shell-Dienst neu starten, damit die Einstellungen wirksam werden.

   a Wählen Sie im vSphere Client den Host aus und navigieren Sie zu **Konfigurieren > System > Dienste**.

   b Wählen Sie nacheinander „ESXi Shell“ und „SSH“ aus und klicken Sie auf **Neustart**.

Ergebnisse

- Bei festgelegtem Zeitüberschreitungswert für Leerlauf werden Benutzer abgemeldet, wenn sich die Sitzung während des angegebenen Zeitraums im Leerlauf befindet.
- Wenn Sie den Zeitüberschreitungswert für Verfügbarkeit festlegen und sich nicht vor Ablauf dieses Zeitüberschreitungswerts anmelden, werden die Anmeldungen erneut deaktiviert.

Aktivieren des Zugriffs auf ESXi Shell mithilfe des vSphere Client

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

Hinweis Greifen Sie auf den Host zu, indem Sie den vSphere Client, Remote-Befehlszeilentools (ESXCLI und PowerCLI) und veröffentlichte APIs verwenden. Aktivieren Sie den Remotezugriff auf den Host nicht mit SSH, es sei denn, bestimmte Umstände erfordern eine Aktivierung.

Voraussetzungen

Wenn Sie einen autorisierten SSH-Schlüssel verwenden möchten, können Sie ihn hochladen. Weitere Informationen finden Sie unter ESXi-SSH-Schlüssel.

Verfahren

1 Navigieren Sie zum Host in der Bestandsliste.

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

3 Verwalten Sie ESXi-, SSH- oder Dienste der Benutzerschnittstelle der direkten Konsole.

   a Wählen Sie im Fenster „Dienste“ den Dienst aus.

   b Klicken Sie auf **Startrichtlinie bearbeiten** und wählen Sie die Startrichtlinie **Manuell starten und stoppen** aus.

   c Klicken Sie zum Aktivieren des Diensts auf **Starten**.

   Wenn Sie **Manuell starten und beenden** wählen, wird der Dienst nicht gestartet, wenn Sie den Host neu starten. Wenn Sie den Dienst beim Neustart des Hosts starten möchten, wählen Sie **Mit dem Host starten und beenden**.

Nächste Schritte

Legen Sie die Zeitüberschreitungswerte für die Verfügbarkeits- und Leerlaufzeiten der ESXi Shell fest. Weitere Informationen hierzu finden Sie unter Festlegen eines Zeitüberschreitungswerts für Verfügbarkeit für die ESXi Shell mithilfe des vSphere Client und Festlegen der Zeitüberschreitungswerts für Leerlauf für die ESXi Shell mithilfe des vSphere Client.

Aktivieren des Zugriffs auf die ESXi Shell mithilfe der DCUI

Mithilfe der Benutzerschnittstelle der direkten Konsole (DCUI) können Sie lokal unter Verwendung textbasierter Menüs mit dem Hosts interagieren. Wägen Sie ab, ob die Sicherheitsanforderungen Ihrer Umgebung die Direct Console User Interface unterstützen.

Sie können die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) verwenden, um lokalen und Remotezugriff auf die ESXi Shell zu ermöglichen. Sie greifen über die mit dem Host verbundene physische Konsole auf die Benutzerschnittstelle der direkten Konsole zu. Nachdem der Host neu gestartet und ESXi geladen wurde, drücken Sie F2 zum Anmelden bei der DCUI. Geben Sie die Anmeldedaten ein, die Sie bei der Installation von ESXi erstellt haben.

Hinweis Änderungen am Host, die mit der Benutzerschnittstelle der direkten Konsole, dem vSphere Client, ESXCLI oder anderen Verwaltungs-Tools vorgenommen wurden, werden stündlich oder beim ordnungsgemäßen Herunterfahren des Systems dauerhaft gespeichert. Wenn der Host ausfällt, bevor die Änderungen vorgenommen wurden, gehen sie möglicherweise verloren.

Verfahren

1. Drücken Sie in Direct Console User Interface die Taste F2, um das Menü für die Systemanpassung aufzurufen.
2. Wählen Sie **Fehlerbehebungsoptionen** und drücken Sie die Eingabetaste.
3. Wählen Sie im Menü „Optionen für den Fehlerbehebungsmodus“ einen Dienst aus, der aktiviert werden soll.
   - Aktivieren von ESXi Shell
   - Aktivieren von SSH
4. Drücken Sie die Eingabetaste, um den Dienst zu aktivieren.
5. Drücken Sie die Esc-Taste wiederholt, bis Sie zurück zum Hauptmenü der Benutzerschnittstelle der direkten Konsole gelangt sind.

Nächste Schritte

Legen Sie die Zeitüberschreitungswerte für die Verfügbarkeits- und Leerlaufzeiten der ESXi Shell fest. Weitere Informationen hierzu finden Sie unter Festlegen von Zeitüberschreitungswerten für Verfügbarkeit oder Leerlauf für die ESXi Shell mithilfe der DCUI.

Anmelden bei der ESXi Shell zur Fehlerbehebung

Führen Sie ESXi-Konfigurationsaufgaben mit vSphere Client, ESXCLI oder VMware PowerCLI aus. Melden Sie sich bei der ESXi Shell (vormals Support-Modus oder TSM) nur zwecks Fehlerbehebung an.

Verfahren

1. Melden Sie sich an der ESXi Shell mit einer der folgenden Methoden an:
   - Wenn Sie direkten Zugriff auf den Host haben, drücken Sie Alt+F1, um den Anmeldebildschirm auf der physischen Konsole der Maschine aufzurufen.
   - Wenn Sie eine Verbindung mit dem Host remote herstellen, verwenden Sie SSH oder eine andere Remote-Konsolenverbindung, um eine Sitzung auf dem Host zu starten.
2. Geben Sie einen Benutzernamen und ein Kennwort ein, die vom Host erkannt werden.

UEFI Secure Boot für ESXi-Hosts

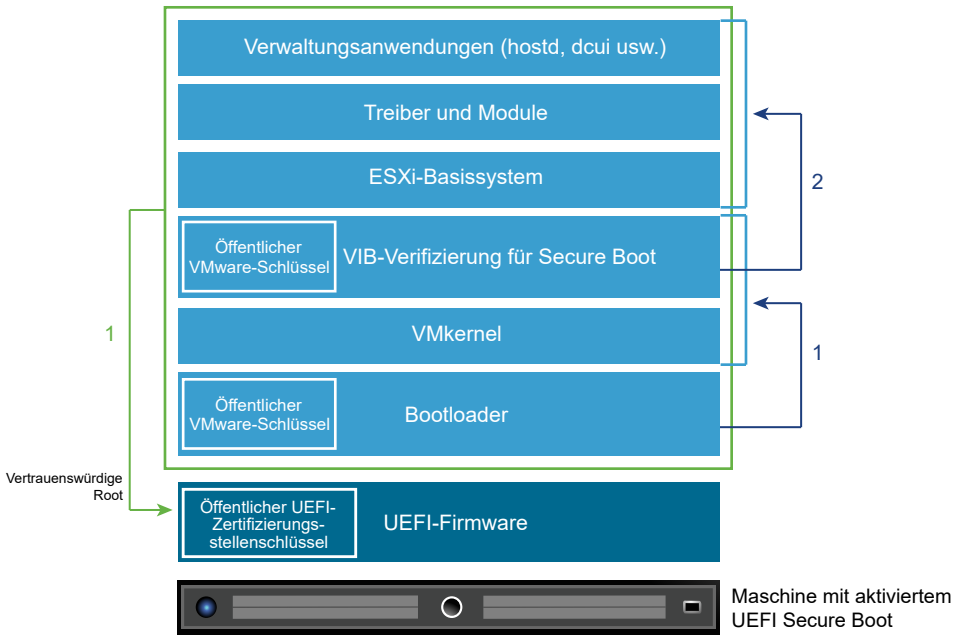
Secure Boot (sicherer Start) ist Bestandteil des UEFI-Firmwarestandards. Bei verwendetem Secure Boot lädt eine Maschine UEFI-Treiber oder -Apps nur, wenn der Bootloader des Betriebssystems kryptografisch signiert ist. In vSphere 6.5 und höher unterstützt ESXi den sicheren Start, falls die entsprechende Option in der Hardware aktiviert ist.

Verwendung von UEFI Secure Boot durch ESXi

ESXi Version 6.5 und höher unterstützt UEFI Secure Boot auf jeder Ebene des Boot-Stacks.

Hinweis Vor der Verwendung von UEFI Secure Boot auf einem aktualisierten Host überprüfen Sie die Kompatibilität anhand der Anweisungen unter Ausführen des Secure Boot-Validierungsskripts nach dem ESXi-Upgrade.

Abbildung 3-1. UEFI Secure Boot



Bei verwendetem Secure Boot sieht die Startsequenz wie folgt aus.

1 In vSphere 6.5 und höher enthält der ESXi-Bootloader einen öffentlichen VMware-Schlüssel. Der Bootloader überprüft mithilfe dieses Schlüssels die Signatur des Kernels und einen kleinen Teil des Systems, das eine VIB-Verifizierung für Secure Boot beinhaltet.

2 Die VIB-Verifizierung überprüft jedes im System installierte VIB-Paket.

Zu diesem Zeitpunkt wird das gesamte System gestartet, mit der vertrauenswürdigen Root in Zertifikaten, die Bestandteil der UEFI-Firmware sind.

Hinweis Wenn Sie vSphere 7.0 Update 2 oder höher installieren oder ein Upgrade auf diese Version durchführen und ein ESXi-Host über ein TPM verfügt, versiegelt das TPM die vertraulichen Informationen mithilfe einer TPM-Richtlinie. Diese basiert auf PCR-Werten für UEFI Secure Boot. Dieser Wert wird bei nachfolgenden Neustarts geladen, wenn die Richtlinie als wahr erfüllt ist. Informationen zum Deaktivieren oder Aktivieren von UEFI Secure Boot in vSphere 7.0 Update 2 oder höher finden Sie unter Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration.

Fehlerbehebung bei UEFI Secure Boot

Wenn Secure Boot auf keiner Ebene der Startsequenz erfolgreich ist, wird ein Fehler gemeldet.

Die Fehlermeldung ist abhängig vom Hardwareanbieter und von der Ebene, auf der die Verifizierung fehlgeschlagen ist.

- Wenn Sie versuchen, mit einem nicht signierten oder manipulierten Bootloader zu starten, wird während der Startsequenz ein Fehler gemeldet. Die genaue Fehlermeldung ist abhängig vom Hardwareanbieter. Die Fehlermeldung kann so oder ähnlich wie die folgende Fehlermeldung lauten.

  ```
  UEFI0073: Unable to boot PXE Device...because of the Secure Boot policy
  ```

- Wenn der Kernel manipuliert wurde, wird eine Fehlermeldung ähnlich der folgenden angezeigt:

  ```
  Fatal error: 39 (Secure Boot Failed)
  ```

- Wenn ein Paket (VIB oder Treiber) manipuliert wurde, wird ein lilafarbener Bildschirm mit der folgenden Fehlermeldung angezeigt:

  ```
  UEFI Secure Boot failed:
  Failed to verify signatures of the following vibs (XX)
  ```

Führen Sie die folgenden Schritte aus, um Probleme mit Secure Boot zu beheben:

1 Führen Sie einen Neustart des Hosts mit deaktivierter Funktion für Secure Boot durch.

2 Führen Sie das Skript für die Prüfung des sicheren Starts aus (siehe Ausführen des Secure Boot-Validierungsskripts nach dem ESXi-Upgrade).

3 Analysieren Sie die Informationen in der Datei `/var/log/esxupdate.log`.

Ausführen des Secure Boot-Validierungsskripts nach dem ESXi-Upgrade

Nach dem Upgrade eines ESXi-Hosts von einer Version, die UEFI Secure Boot nicht unterstützt, müssen Sie überprüfen, ob Sie den sicheren Start aktivieren können.

Für eine erfolgreiche Durchführung des sicheren Starts müssen die Signaturen aller installierten VIBs auf dem System vorhanden sein. In älteren ESXi-Versionen werden die Signaturen beim Installieren von VIBs nicht gespeichert.

- Wenn Sie das Upgrade mithilfe von ESXCLI-Befehlen durchführen, führt die alte Version von ESXi die Installation der neuen VIBs durch, sodass ihre Signaturen nicht gespeichert werden und ein sicherer Start (Secure Boot) nicht möglich ist.
- Wenn Sie das Upgrade mithilfe des ISO-Images durchführen, werden die Signaturen der neuen VIBs gespeichert. Dies gilt auch für vSphere Lifecycle Manager-Upgrades, die das ISO-Image verwenden.

- Wenn alte VIBs auf dem System verbleiben, stehen die Signaturen dieser VIBs nicht zur Verfügung und ein sicherer Start ist nicht möglich.
  - Wenn das System einen Drittanbietertreiber verwendet und das VMware-Upgrade keine neue Version des Treiber-VIB enthält, verbleibt das alte VIB nach dem Upgrade auf dem System.
  - In seltenen Fällen stellt VMware die fortlaufende Entwicklung eines bestimmten VIB ein, ohne ein neues VIB bereitzustellen, das das alte ersetzt oder überflüssig macht. In diesem Fall verbleibt das alte VIB nach dem Upgrade auf dem System.

Hinweis Für den sicheren Start über UEFI ist außerdem ein aktueller Bootloader erforderlich. Mit diesem Skript wird nicht geprüft, ob ein aktueller Bootloader vorhanden ist.

Voraussetzungen

Nach dem Upgrade eines ESXi-Hosts von einer früheren ESXi-Version, die UEFI Secure Boot nicht unterstützte, können Sie möglicherweise den sicheren Start aktivieren. Ob Sie den sicheren Start aktivieren können, richtet sich danach, wie Sie das Upgrade durchgeführt haben und ob beim Upgrade alle vorhandenen VIBs ersetzt oder bestimmte VIBs unverändert belassen wurden. Sie können nach der Durchführung des Upgrades ein Validierungsskript ausführen, um festzustellen, ob der sichere Start von der aktualisierten Installation unterstützt wird.

- Stellen Sie sicher, dass die Hardware den sicheren Start über UEFI unterstützt.
- Stellen Sie sicher, dass alle VIBs mindestens mit der Akzeptanzebene „PartnerSupported“ signiert sind. Wenn Sie VIBs auf der Ebene „CommunitySupported“ einbeziehen, können Sie den sicheren Start nicht verwenden.

Verfahren

1 Führen Sie ein Upgrade für ESXi durch und führen Sie den folgenden Befehl aus.

```
/usr/lib/vmware/secureboot/bin/secureBoot.py -c
```

2 Prüfen Sie die Ausgabe.

Die Ausgabe enthält entweder `Secure boot can be enabled` oder `Secure boot CANNOT be enabled`.

Sichern von ESXi-Hosts mit Trusted Platform Module

ESXi-Hosts können die Funktionalität von TPM-Chips (Trusted Platform Modules) nutzen. Hierbei handelt es sich um sichere Kryptoprozessoren, die die Hostsicherheit erhöhen, indem sie eine Zusicherung der Vertrauenswürdigkeit ermöglichen, die in Hardware und nicht in Software verankert ist.

 (Demonstration der ESXi- und Trusted Platform Module 2.0-Funktionen)

Was ist ein TPM?

TPM ist ein branchenweiter Standard für sichere Kryptoprozessoren. TPM-Chips sind in den meisten Computern zu finden. Dies gilt gleichermaßen für Laptops, Desktop-Computer und sogar Server. vSphere 6.7 und höher unterstützt TPM Version 2.0.

Ein TPM 2.0-Chip bestätigt die ESXi-Identität eines Hosts. Ein Host-Integritätsnachweis ist der Prozess der Authentifizierung und Bescheinigung des Zustands der Software eines Hosts zu einem bestimmten Zeitpunkt. Die Implementierung des UEFI Secure Boot-Mechanismus, der sicherstellt, dass beim Starten nur signierte Software geladen wird, ist eine Voraussetzung für einen erfolgreichen Integritätsnachweis. Der TPM 2.0-Chip zeichnet die Messungen der im System gestarteten Softwaremodule auf und speichert sie sicher ab, was extern von vCenter Server überprüft wird.

Der Fernbescheinigungsprozess umfasst die folgenden allgemeinen Schritte:

1 Stellen Sie die Vertrauenswürdigkeit des Remote-TPMs fest und erstellen Sie darauf basierend einen Integritätsnachweisschlüssel (Attestation Key, AK).

   Wenn ein ESXi-Host zu vCenter Server hinzugefügt, von dort aus neu gestartet oder erneut mit vCenter Server verbunden wird, fordert vCenter Server einen AK vom Host an. Ein Teil des AK-Erstellungsprozesses beinhaltet auch die Überprüfung der TPM-Hardware selbst, um sicherzustellen, dass sie von einem bekannten (und vertrauenswürdigen) Anbieter produziert wurde.

2 Rufen Sie den Integritätsnachweisbericht (Attestation Report) vom Host ab.

   vCenter Server verlangt, dass der Host einen Integritätsnachweisbericht sendet, der einen vom TPM signierten Auszug der Werte in den Platform Configuration Registers (PCRs) sowie andere signierte binäre Metadaten des Hosts enthält. Durch Überprüfung, ob die Informationen mit einer Konfiguration übereinstimmen, die er für vertrauenswürdig hält, identifiziert ein vCenter Server die Plattform auf einem zuvor nicht vertrauenswürdigen Host.

3 Überprüfen Sie die Authentizität des Hosts.

   vCenter Server prüft die Echtheit des signierten Datenauszugs, leitet die Softwareversionen ab und bestimmt deren Vertrauenswürdigkeit. Wenn vCenter Server feststellt, dass der signierte Auszug ungültig ist, schlägt die Fernbescheinigung fehl, und der Host gilt als nicht vertrauenswürdig.

Was sind die vSphere-Anforderungen für die Verwendung eines TPM?

Um einen TPM 2.0-Chip verwenden zu können, muss Ihre Umgebung vCenter Server die folgenden Anforderungen erfüllen:

- vCenter Server 6.7 oder höher
- ESXi 6.7-Host oder höher mit installiertem und in UEFI aktivierten TPM 2.0-Chip
- UEFI Secure Boot ist aktiviert

Stellen Sie sicher, dass das TPM im BIOS des ESXi-Hosts so konfiguriert ist, dass es den SHA-256-Hashing-Algorithmus und die TIS/FIFO-Schnittstelle (First-In, First-Out) verwendet und nicht CRB (Command Response Buffer). Informationen zum Einstellen dieser erforderlichen BIOS-Optionen finden Sie in der Dokumentation des Herstellers.

Überprüfen Sie die von VMware zertifizierten TPM 2.0-Chips unter

https://www.vmware.com/resources/compatibility/search.php

Was passiert, wenn Sie einen Host mit einem TPM starten?

Wenn Sie einen ESXi-Host mit installiertem TPM 2.0-Chip starten, überwacht vCenter Server den Nachweisstatus des Hosts. Um den Status der Hardwarevertrauensstellung anzuzeigen, wählen Sie im vSphere Client die Registerkarte vCenter Server und dann die Registerkarte **Übersicht** unter **Überwachen** aus. Status der Hardwarevertrauensstellung wird wie folgt angegeben:

- Grün: Normaler Status, zeigt uneingeschränkte Vertrauenswürdigkeit an.
- Rot: Integritätsnachweis ist fehlgeschlagen.

Hinweis Wenn Sie einen TPM 2.0-Chip zu einem ESXi-Host hinzufügen, der von vCenter Server bereits verwaltet wird, müssen Sie zuerst den Host trennen und dann erneut verbinden. Informationen zum Trennen und Wiederverbinden von Hosts finden Sie in der *vCenter Server und Hostverwaltung*-Dokumentation.

Mit vSphere 7.0 und höher verwendet VMware® vSphere Trust Authority™ Remotenachweisfunktionen für ESXi-Hosts. Weitere Informationen finden Sie unter Was ist der vSphere Trust Authority-Nachweisdienst?.

Überprüfen des Integritätsnachweis-Status eines ESXi-Hosts

Wenn einem ESXi-Host ein Trusted Platform Module 2.0-kompatibler Chip hinzugefügt wurde, bescheinigt dieser die Integrität der Plattform. Sie können den Integritätsnachweis-Status des Hosts im vSphere Client anzeigen. Sie können auch den Intel TXT-Status (Trusted Execution Technology) anzeigen.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Navigieren Sie zu einem Datencenter und klicken Sie auf die Registerkarte **Überwachen**.
3. Klicken Sie auf **Sicherheit**.
4. Überprüfen Sie den Host-Status in der Spalte „Integritätsnachweis“ und lesen Sie die begleitende Nachricht in der Spalte **Nachricht**.
5. Wenn es sich bei diesem Host um einen vertrauenswürdigen Host handelt, finden Sie weitere Informationen unter Anzeigen des Nachweisstatus des vertrauenswürdigen Clusters.

Nächste Schritte

Informationen zur Fehlerbehandlung bei einem Integritätsnachweis-Status „Fehlgeschlagen“ oder „Warnung“ finden Sie unter Beheben von Problemen beim ESXi-Hostnachweis. Weitere Informationen zu vertrauenswürdigen Hosts finden Sie unter Beheben von Problemen beim Nachweis des vertrauenswürdigen Hosts.

Beheben von Problemen beim ESXi-Hostnachweis

Wenn Sie ein Trusted Platform Module (TPM)-Gerät auf einem ESXi-Host installieren, kann der Host möglicherweise keinen Nachweis erbringen. Sie können die möglichen Ursachen für dieses Problem beheben.

Verfahren

1. Sehen Sie sich den Alarmstatus des ESXi-Hosts und die begleitende Fehlermeldung an. Weitere Informationen hierzu finden Sie unter Überprüfen des Integritätsnachweis-Status eines ESXi-Hosts.
2. Wenn die Fehlermeldung `Sicherer Start des Hosts wurde deaktiviert` lautet, müssen Sie den sicheren Start erneut aktivieren, um das Problem zu beheben.
3. Wenn der Beglaubigungsstatus des Hosts fehlgeschlagen ist, überprüfen Sie die vCenter Server-Datei `vpxd.log` auf folgende Meldung:

   ```
   Kein gecachter Identitätsschlüssel, Laden von der DB
   ```

   Diese Meldung zeigt an, dass Sie einen TPM 2.0-Chip zu einem ESXi-Host hinzufügen, der von vCenter Server bereits verwaltet wird. Sie müssen zuerst die Verbindung zum Host trennen und dann erneut verbinden. Informationen zum Trennen und Wiederverbinden von Hosts finden Sie in der *vCenter Server und Hostverwaltung*-Dokumentation.

   Weitere Informationen zu vCenter Server-Protokolldateien, einschließlich Speicherort und Protokollrotation, finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/1021804.
4. Wenden Sie sich bei allen anderen Fehlermeldungen an den Kunden-Support.

ESXi-Protokolldateien

Protokolldateien sind eine wichtige Komponente bei der Fehlersuche nach Angriffen und für die Suche nach Informationen über Sicherheitsverletzungen. Alle ESXi-Hosts führen einen Syslog-Dienst aus. Dieser protokolliert Meldungen vom VMkernel und anderen Systemkomponenten in lokalen Dateien oder auf einem Remotehost.

Treffen Sie folgende Maßnahmen, um die Sicherheit des Hosts zu erhöhen.

- Konfigurieren Sie die dauerhafte Protokollierung in einem Datenspeicher. Standardmäßig werden die Protokolldateien auf ESXi-Hosts im speicherresidenten Dateisystem gespeichert. Sie gehen daher verloren, wenn Sie den Host neu starten, und Protokolldaten werden nur für 24 Stunden gespeichert. Wenn Sie die dauerhafte Protokollierung aktivieren, verfügen Sie über eine dedizierte Aufzeichnung der Aktivitäten für den Host.
- Mithilfe der Remoteprotokollierung auf einem zentralen Host können Sie Protokolldateien auf einem zentralen Host speichern. Über diesen Host können Sie alle Hosts mit einem einzigen Tool überwachen, zusammenfassende Analysen durchführen und Protokolldaten durchsuchen. Diese Vorgehensweise vereinfacht die Überwachung und macht Informationen zu koordinierten Angriffen auf mehreren Hosts verfügbar.
- Konfigurieren Sie das Remotesicherheits-Syslog auf ESXi-Hosts mithilfe von ESXCLI oder PowerCLI oder mithilfe eines API-Clients.
- Führen Sie eine Abfrage der Syslog-Konfiguration durch, um sicherzustellen, dass der Syslog-Server und der Port gültig sind.

In der Dokumentation *vSphere-Überwachung und -Leistung* finden Sie Informationen zum Syslog-Setup sowie zusätzliche Informationen zu ESXi-Protokolldateien.

Konfiguration von Syslog auf ESXi-Hosts

Sie können den vSphere Client, den VMware Host Client oder den Befehl `esxcli system syslog` zum Konfigurieren des Syslog-Diensts verwenden.

Informationen zur Verwendung des `esxcli system syslog`-Befehls und anderen ESXCLI-Befehlen finden Sie unter *Erste Schritte mit ESXCLI*. Weitere Informationen zum Öffnen der ESXi-Firewall für den in jeder Remotehostspezifikation angegebenen Port finden Sie unter Konfigurieren der ESXi Firewall.

Verfahren

1. Navigieren Sie zum Host im Navigator von vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
4. Klicken Sie auf **Bearbeiten**.
5. Filter für **`syslog`**.
6. Informationen zum globalen Einrichten der Protokollierung und zur Konfiguration verschiedener erweiterter Einstellungen finden Sie unter ESXi-Syslog-Optionen.
7. (Optional) So überschreiben Sie die Standardprotokollgröße und die Rotationsangaben für ein Protokoll:
   a. Klicken Sie auf den Namen des Protokolls, das Sie anpassen möchten.
   b. Geben Sie die Anzahl der Rotationen und die gewünschte Protokollgröße ein.

8 Klicken Sie auf **OK**.

Ergebnisse

Änderungen an den syslog-Optionen werden sofort wirksam.

Hinweis Mithilfe des vSphere Client oder VMware Host Client definierte Einstellungen für Syslog-Parameter werden sofort wirksam. Die meisten mithilfe von ESXCLI definierten Einstellungen benötigen jedoch einen zusätzlichen Befehl, um wirksam zu werden. Weitere Informationen finden Sie unter ESXi-Syslog-Optionen.

ESXi-Syslog-Optionen

Sie können das Verhalten von ESXi-Syslog-Dateien und -Übertragungen mithilfe mehrerer Syslog-Optionen definieren.

Neben den Basiseinstellungen, wie z. B. `Syslog.global.logHost`, steht ab ESXi 7.0 Update 1 eine Liste mit erweiterten Optionen für Anpassungen und NIAP-Konformität zur Verfügung.

Hinweis Konfigurieren Sie dauerhaften Speicher immer, bevor Sie Überwachungsdatensatzparameter oder den `Syslog.global.logDir`-Parameter festlegen.

Hinweis Alle Einstellungen für Überwachungsdatensätze, die mit `Syslog.global.auditRecord` beginnen, werden sofort wirksam. Für andere Einstellungen, die Sie mithilfe von ESXCLI definieren, müssen Sie zum Aktivieren der Änderungen jedoch den Befehl `esxcli system syslog reload` ausführen.

Tabelle 3-9. Legacy-Syslog-Optionen

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.logHost`	`esxcli system syslog config set --loghost=<str>`	Definiert eine kommagetrennte Liste mit Remotehosts und Spezifikationen für Meldungsübertragungen. Wenn das Feld `loghost=<str>` leer ist, werden keine Protokolle weitergeleitet. Obwohl es keinen festen Grenzwert für die Anzahl der Remotehosts gibt, die Syslog-Meldungen empfangen, wird dennoch empfohlen, die Anzahl der Remotehosts auf fünf oder weniger zu begrenzen. Das Format einer Remotehostspezifikation lautet: `protocol://hostname|ipv4|'['ipv6']'[:port]`. Als Protokoll muss TCP, UDP oder SSL verwendet werden. Der Wert eines Ports kann eine beliebige Zahl zwischen 1 und 65535 sein. Wenn kein Port angegeben wird, wird 1514 von SSL und TCP verwendet. UDP verwendet 514. Beispiel: `ssl://hostName1:1514`.
`Syslog.global.defaultRotate`	`esxcli system syslog config set --default-rotate=<long>`	Maximale Anzahl alter beizubehaltender Protokolldateien Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen (siehe `Syslog.global.defaultSize`).
`Syslog.global.defaultSize`	`esxcli system syslog config set --default-size=<long>`	Standardgröße der Protokolldateien in KiB. Nachdem eine Datei die Standardgröße erreicht hat, erstellt der Syslog-Dienst eine neue Datei. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.

Tabelle 3-9. Legacy-Syslog-Optionen (Fortsetzung)

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.logDir`	`esxcli system syslog config set --logdir=<str>`	Verzeichnis, in dem sich Protokolle befinden. Das Verzeichnis kann sich auf gemounteten NFS- oder VMFS-Volumes befinden. Nur das Verzeichnis `/scratch` auf dem lokalen Dateisystem bleibt nach einem Neustart konsistent. Geben Sie das Verzeichnis im Format [*Datenspeichername*] *Pfad_zur_Datei* an, wobei sich der Pfad auf das Stammverzeichnis des Volumes bezieht, in dem sich das Backing für den Datenspeicher befindet. Beispielsweise ist der Pfad `[storage1] /systemlogs` dem Pfad `/vmfs/volumes/storage1/systemlogs` zuzuordnen.
`Syslog.global.logDirUnique`	`esxcli system syslog config set --logdir-unique=<bool>`	Gibt den Namen des ESXi-Hosts an, der mit dem Wert von `Syslog.global.logDir` verknüpft werden soll. Diese Einstellung muss aktiviert werden, wenn sich mehrere ESXi-Hosts bei einem gemeinsam genutzten Dateisystem anmelden. 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.certificate.checkSSLCerts`	`esxcli system syslog config set --check-ssl-certs=<bool>`	Erzwingt die Überprüfung von SSL-Zertifikaten bei der Übertragung von Nachrichten an Remotehosts.

Tabelle 3-10. Verfügbare Syslog-Optionen ab ESXi 7.0 Update 1

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.auditRecord.storageCapacity`	`esxcli system auditrecords local set --size=<long>`	Gibt die Kapazität des Verzeichnisses zum Speichern von Überwachungsdatensätzen auf dem ESXi-Host in MiB an. Sie können die Kapazität des Überwachungsdatensatzspeichers nicht verringern. Sie können die Kapazität vor oder nach der Aktivierung des Überwachungsdatensatzspeichers erhöhen (siehe `Syslog.global.auditRecord.storageEnable`).
`Syslog.global.auditRecord.remoteEnable`	`esxcli system auditrecords remote enable`	Ermöglicht das Senden von Überwachungsdatensätzen an Remotehosts. Remotehosts werden mithilfe des Parameters `Syslog.global.logHost` angegeben.
`Syslog.global.auditRecord.storageDirectory`	`esxcli system auditrecords local set --directory=<dir>`	Erstellt ein Verzeichnis zum Speichern von Überwachungsdatensätzen und legt `/scratch/auditLog` als Standardspeicherort fest. Sie dürfen kein Verzeichnis zur Speicherung von Überwachungsdatensätzen manuell erstellen, und das Verzeichnis für den Überwachungsdatensatzspeicher kann nicht geändert werden, solange der Überwachungsdatensatzspeicher aktiviert ist (siehe `Syslog.global.auditRecord.storageEnable`).
`Syslog.global.auditRecord.storageEnable`	`esxcli system auditrecords local enable`	Aktiviert die Speicherung von Überwachungsdatensätzen auf einem ESXi-Host. Wenn das Verzeichnis zum Speichern von Überwachungsdatensätzen nicht vorhanden ist, wird es mit der von `Syslog.global.auditRecord.storageCapacity` angegebenen Kapazität erstellt.

Tabelle 3-10. Verfügbare Syslog-Optionen ab ESXi 7.0 Update 1 (Fortsetzung)

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.certificate.checkCRL`	`esxcli system syslog config set --crl-check=<bool>`	Ermöglicht die Überprüfung des Widerrufstatus aller Zertifikate in einer SSL-Zertifikatskette. Ermöglicht die Überprüfung von X.509-CRLs, die in Übereinstimmung mit den Branchenkonventionen nicht standardmäßig überprüft werden. Eine mit NIAP validierte Konfiguration benötigt CRL-Prüfungen. Wenn CRL-Prüfungen aktiviert sind, müssen alle Zertifikate in einer Zertifikatskette aufgrund von Implementierungseinschränkungen einen CRL-Link bereitstellen. Aktivieren Sie die Option `crl-check` nicht für Installationen ohne Bezug zur Zertifizierung, da sich die ordnungsgemäße Konfiguration einer Umgebung, die CRL-Prüfungen verwendet, als schwierig erweist.
`Syslog.global.certificate.strictX509Compliance`	`esxcli system syslog config set --x509-strict=<bool>`	Aktiviert strikte Übereinstimmung mit X.509. Führt während der Überprüfung zusätzliche Gültigkeitsprüfungen für CA-Stammzertifikate durch. Diese Prüfungen werden in der Regel nicht durchgeführt, da CA-Roots inhärent vertrauenswürdig sind und Inkompatibilitäten mit vorhandenen, falsch konfigurierten CA-Roots verursachen können. Eine mit NIAP validierte Konfiguration benötigt CA-Roots sogar, um Validierungen erfolgreich zu durchlaufen. Aktivieren Sie die Option `x509-strict` nicht für Installationen ohne Bezug zur Zertifizierung, da sich die ordnungsgemäße Konfiguration einer Umgebung, die CRL-Prüfungen verwendet, als schwierig erweist.
`Syslog.global.droppedMsgs.fileRotate`	`esxcli system syslog config set --drop-log-rotate=<long>`	Gibt die Anzahl der beizubehaltenden Protokolldateien mit alten gelöschten Meldungen an.
`Syslog.global.droppedMsgs.fileSize`	`esxcli system syslog config set --drop-log-size=<long>`	Gibt die Größer aller Protokolldateien mit gelöschten Meldungen vor dem Wechsel zu einer neuen Datei in KiB an.

Tabelle 3-10. Verfügbare Syslog-Optionen ab ESXi 7.0 Update 1 (Fortsetzung)

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.logCheckSSLCerts`	`esxcli system syslog config set --check-ssl-certs=<bool>`	Erzwingt die Überprüfung von SSL-Zertifikaten bei der Übertragung von Nachrichten an Remotehosts. **Hinweis** Veraltet. Verwenden Sie `Syslog.global.certificate.checkSSLCerts` in ESXi 7.0 Update 1 und höher.
`Syslog.global.logFilters`	`esxcli system syslog config logfilter [add | remove | set] ...`	Gibt eine oder mehrere Spezifikationen für die Protokollfilterung an. Alle Protokollfilter müssen durch einen doppelten vertikalen Balken (||) getrennt werden. Das Format eines Protokollfilters lautet: `numLogs | ident | logRegexp`. `numLogs` legt die maximale Anzahl von Protokolleinträgen für die angegebenen Protokollmeldungen fest. Nach Erreichen dieses Werts werden die angegebenen Protokollmeldungen gefiltert und ignoriert. `ident` gibt eine oder mehrere Systemkomponenten an, um den Filter auf die Protokollmeldungen anzuwenden, die von diesen Komponenten erzeugt werden. `logRegexp` gibt eine Zeichenfolge unter Beachtung der Groß-/Kleinschreibung mit Python-Syntax für reguläre Ausdrücke an, um die Protokollmeldungen anhand ihres Inhalts zu filtern.
`Syslog.global.logFiltersEnable`		Aktiviert die Verwendung von Protokollfiltern.
`Syslog.global.logLevel`	`esxcli system syslog config set --log-level=<str>`	Gibt die Ebene der Protokollfilterung an. Sie müssen diesen Parameter nur bei der Behebung eines Problems mit dem Syslog-Daemon ändern. Sie können den Wert `debug` für die Ebene mit den meisten Details, den Wert `info` für die Ebene mit Standarddetails, den Wert `warning` für Warnungen bzw. Fehler oder den Wert `error` für Fehler verwenden.
`Syslog.global.msgQueueDropMark`	`esxcli system syslog config --queue-drop-mark=<long>)`	Gibt den Prozentsatz der Kapazität der Meldungswarteschlange an, ab dem Meldungen verworfen werden.

Tabelle 3-10. Verfügbare Syslog-Optionen ab ESXi 7.0 Update 1 (Fortsetzung)

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.remoteHost.connectRetryDelay`	`esxcli system syslog config set --default-timeout=<long>`	Gibt die Verzögerung in Sekunden vor dem erneuten Versuch einer Verbindungsherstellung mit einem Remotehost an, nachdem ein Verbindungsversuch fehlgeschlagen ist.
`Syslog.global.remoteHost.maxMsgLen`	`esxcli system syslog config set --remote-host-max-msg-len=<long>`	Für die TCP- und SSL-Protokolle gibt dieser Parameter die maximale Länge einer Syslog-Übertragung vor dem Auftreten von Kürzungen in Byte an. Die maximale Standardlänge für Meldungen von Remotehosts beträgt 1 KiB. Sie können die maximale Nachrichtenlänge auf bis zu 16 KiB erhöhen. Bei einer Erhöhung dieses Werts auf über 1 KiB ist es jedoch möglich, dass lange Übertragungen gekürzt bei einem Syslog-Collector ankommen. Beispiel: Die Syslog-Infrastruktur, die eine Meldung ausgibt, befindet sich außerhalb von ESXi. Diese Einstellung hat keinen Einfluss auf das UDP-Protokoll. RFC 5426 legt die maximale Nachrichtenübertragungslänge für das UDP-Protokoll auf 480 Byte für IPV4 und 1180 Byte für IPV6 fest. Aufgrund dieser Einschränkung und da UDP-Pakete von der Netzwerkinfrastruktur willkürlich verworfen werden können, wird die Verwendung von UDP für die Übertragung kritischer Syslog-Nachrichten nicht empfohlen.
`Syslog.global.vsanBacking`	`esxcli system syslog config set --vsan-backing=<bool>`	Ermöglicht das Platzieren von Protokolldateien sowie des Verzeichnisses zum Speichern von Überwachungsdatensätzen in einem vSAN-Cluster. Die Aktivierung dieses Parameters kann jedoch dazu führen, dass der ESXi-Host nicht mehr reagiert.

Speicherorte der ESXi-Protokolldateien

ESXi zeichnet die Hostaktivität in Protokolldateien mithilfe eines syslog-Hilfsprogramms auf.

Tabelle 3-11. Speicherorte der ESXi-Protokolldateien

Komponente	Speicherort	Zweck
Authentifizierung	`/var/log/auth.log`	Enthält alle Ereignisse, die sich auf die Authentifizierung für das lokale System beziehen.
ESXi-Hostagenten-Protokoll	`/var/log/hostd.log`	Enthält Informationen zum Agenten, mit dem der ESXi-Host und seine virtuellen Maschinen verwaltet und konfiguriert werden.
Shell-Protokoll	`/var/log/shell.log`	Enthält einen Datensatz mit allen Befehlen, die in die ESXi-Shell eingegeben wurden, und Shell-Ereignisse (z. B. Zeitpunkt der Aktivierung der Shell).
Systemmeldungen	`/var/log/syslog.log`	Enthält alle allgemeinen Protokollmeldungen und kann zur Fehlerbehebung verwendet werden. Diese Informationen befanden sich vorher in der Protokolldatei „messages“.
Protokoll des vCenter Server-Agenten	`/var/log/vpxa.log`	Enthält Informationen zu dem Agenten, der mit vCenter Server kommuniziert (wenn der Host von vCenter Server verwaltet wird).
virtuelle Maschinen	Dasselbe Verzeichnis wie für die Konfigurationsdateien der jeweiligen virtuellen Maschine mit der Bezeichnung `vmware.log` und `vmware*.log`. Beispiel: `/vmfs/volumes/datastore/virtual machine/vmware.log`	Enthält Ereignisse der virtuellen Maschine, Informationen zum Systemausfall, den Status und die Aktivitäten von Tools, die Uhrzeitsynchronisierung, Änderungen an der virtuellen Hardware, vMotion-Migrationen, Maschinen-Klonvorgänge usw.
VMkernel	`/var/log/vmkernel.log`	Zeichnet Aktivitäten in Verbindung mit virtuellen Maschinen und ESXi auf.
VMkernel-Übersicht	`/var/log/vmksummary.log`	Wird verwendet, um die Betriebszeit und die Verfügbarkeitsstatistiken für ESXi (kommagetrennt) zu bestimmen.
VMkernel-Warnungen	`/var/log/vmkwarning.log`	Zeichnet Aktivitäten in Verbindung mit virtuellen Maschinen auf.
Quick Boot	`/var/log/loadESX.log`	Enthält alle Ereignisse bezüglich des Neustarts eines ESXi-Hosts mithilfe von Quick Boot.
Agent der vertrauenswürdigen Infrastruktur	`/var/run/log/kmxa.log`	Zeichnet Aktivitäten im Zusammenhang mit dem Client-Dienst auf dem vertrauenswürdigen ESXi-Host auf.

Tabelle 3-11. Speicherorte der ESXi-Protokolldateien (Fortsetzung)

Komponente	Speicherort	Zweck
Schlüsselanbieterdienst	`/var/run/log/kmxd.log`	Zeichnet Aktivitäten im Zusammenhang mit dem vSphere Trust Authority-Schlüsselanbieterdienst auf.
Bestätigungsdienst	`/var/run/log/attestd.log`	Zeichnet Aktivitäten im Zusammenhang mit dem vSphere Trust Authority-Bestätigungsdienst auf.
ESX-Token-Dienst	`/var/run/log/esxtokend.log`	Zeichnet Aktivitäten im Zusammenhang mit dem vSphere Trust Authority-ESX-Token-Dienst auf.
ESX-API-Weiterleitung	`/var/run/log/esxapiadapter.log`	Zeichnet Aktivitäten im Zusammenhang mit der vSphere Trust Authority-API-Weiterleitung auf.

Sichern des Fault Tolerance-Protokollierungsdatenverkehrs

VMware Fault Tolerance (FT) erfasst Eingaben und Ereignisse einer primären virtuellen Maschine und sendet sie an eine sekundäre virtuelle Maschine, die auf einem anderen Host ausgeführt wird.

Dieser Datenverkehr für die Protokollierung zwischen den primären und sekundären virtuelle Maschinen erfolgt unverschlüsselt und enthält Gastnetzwerk- und Storage I/O-Daten sowie die Speicherinhalte des Gastbetriebssystems. Dieser Datenverkehr enthält möglicherweise sensible Daten, wie z. B. Kennwörter in Klartext. Um zu verhindern, dass solche Daten preisgegeben werden, stellen Sie sicher, dass dieses Netzwerk gesichert ist, insbesondere gegen sogenannte „Man-in-the-middle“-Angriffe. Verwenden Sie z. B. ein privates Netzwerk für den Datenverkehr für die Fault Tolerance-Protokollierung. Sie können auch den Datenverkehr für die Fault Tolerance-Protokollierung verschlüsseln.

Aktivieren der Fault Tolerance-Verschlüsselung

Sie können den Fault Tolerance-Protokolldatenverkehr verschlüsseln.

vSphere Fault Tolerance führt häufige Prüfungen zwischen einer primären und einer sekundären VM durch, damit die sekundäre VM vom letzten erfolgreichen Prüfpunkt aus schnell fortgesetzt werden kann. Der Prüfpunkt enthält den VM-Status, der seit dem vorherigen Prüfpunkt geändert wurde. Sie können den Fault Tolerance-Protokolldatenverkehr verschlüsseln.

Wenn Sie Fault Tolerance aktivieren, ist die FT-Verschlüsselung standardmäßig auf **Opportunistisch** festgelegt. Dies bedeutet, dass die Verschlüsselung nur aktiviert wird, wenn sowohl der primäre als auch der sekundäre Host verschlüsselt werden können. Befolgen Sie dieses Verfahren, wenn Sie den FT-Verschlüsselungsmodus manuell ändern müssen.

Hinweis Fault Tolerance unterstützt vSphere Virtual Machine Encryption mit vSphere 7.0 Update 2 und höher. Gastinterne und Array-basierte Verschlüsselung sind nicht von der VM-Verschlüsselung abhängig und stören sie nicht. Bei Verwendung mehrerer Verschlüsselungsschichten werden zusätzliche Computing-Ressourcen verwendet, was sich auf die Leistung der virtuellen Maschine auswirken kann. Die Auswirkung variiert je nach Hardware sowie der Menge und dem Typ der E/A, aber die Auswirkungen auf die Gesamtleistung sind für die meisten Arbeitslasten vernachlässigbar. Die Effektivität und Kompatibilität von Back-End-Speicherfunktionen wie Deduplizierung, Komprimierung und Replizierung kann auch von der VM-Verschlüsselung betroffen sein.

Voraussetzungen

Die FT-Verschlüsselung erfordert SMP-FT. Eine Verschlüsselung auf Legacy FT (Record-Replay FT) wird nicht unterstützt.

Verfahren

1 Wählen Sie die VM und dann **Einstellungen bearbeiten** aus.

2 Wählen Sie unter **VM-Optionen** das Dropdown-Menü **Verschlüsselte FT** aus.

3 Wählen Sie eine der folgenden Optionen aus:

Option	Beschreibung
Deaktiviert	Schalten Sie die verschlüsselte Fault Tolerance-Protokollierung nicht ein.
Opportunistisch	Aktivieren Sie die Verschlüsselung nur, wenn beide Seiten dazu in der Lage sind. Eine Fault Tolerance-VM kann auf einen ESXi-Host verschoben werden, der keine verschlüsselte Fault Tolerance-Protokollierung unterstützt.
Erforderlich	Wählen Sie Hosts für die primäre und sekundäre Fault Tolerance aus, die beide die verschlüsselte FT-Protokollierung unterstützen.

Hinweis Während die VM-Verschlüsselung aktiviert ist, ist der FT-Verschlüsselungsmodus standardmäßig auf **Erforderlich** festgelegt und kann nicht geändert werden.

Wenn der FT-Verschlüsselungsmodus auf **Erforderlich** festgelegt ist:

- Wenn Sie FT aktivieren, werden nur Hosts für die Platzierung der sekundären FT-Verschlüsselung aufgelistet, welche die FT-Verschlüsselung unterstützen.
- FT-Failover kann nur auf den von der FT-Verschlüsselung unterstützten Hosts erfolgen.

4 Klicken Sie auf **OK**.

Verwalten von ESXi-Überwachungsdatensätzen

Überwachungsdatensätze entsprechen RFC 5424 und enthalten Informationen zu Ereignissen in Bezug auf Elemente wie Zeit, Status, Beschreibung und Benutzerinformationen, die für Ereignisse protokolliert wurden, die bei Aktionen auf ESXi-Hosts aufgetreten sind. Sowohl lokale als auch Remote-Überwachungsdatensätze sind verfügbar. Die Aufbewahrung von Überwachungsdatensätzen ist standardmäßig deaktiviert. Sie müssen den lokalen und den Remoteüberwachungsmodus manuell aktivieren.

Das lokale ESXi-Überwachungsprotokoll fungiert als Puffer mit fester Größe für kürzlich ausgegebene Überwachungsmeldungen. Wenn der Puffer mit Meldungen gefüllt ist, werden die ältesten Datensätze von neuen Datensätzen überschrieben. Das Remote-Überwachungsprotokoll leitet denselben Stream von Überwachungsdatensätzen entweder unverschlüsselt oder verschlüsselt (RFC 5425) in einem Syslog-Standardformat (RFC 3164) an einen Remoteserver weiter. Überwachungsmeldungen entsprechen RFC 5424, allgemeine Syslog-Meldungen entsprechen jedoch nur RFC 3164. Das System sendet eine generierte Überwachungsmeldung gleichzeitig an den lokalen Speicher und den Remotespeicher.

Während des Verlusts der Verbindung zwischen dem Host und dem Remotespeicher löscht der Remotespeicher alle generierten Überwachungsmeldungen. Bei einer erneuten Verbindung generiert das System eine Überwachungsmeldung, die auf einen potenziellen Verlust von Meldungen hinweist.

Konfigurieren von Überwachungsdatensätzen

Sie konfigurieren die lokale Aufbewahrung von Überwachungsdatensätzen mithilfe von ESXCLI. Weitere Informationen finden Sie unter *ESXCLI – Konzepte und Beispiele*.

Anzeigen von Überwachungsdatensätzen

Sie können die Überwachungsdatensätze wie folgt anzeigen.

- Lokal: Verwenden Sie die ESXi-Anwendung `/bin/viewAudit`.
- Remote: Konfigurieren Sie mithilfe von ESXCLI einen Remote-Überwachungsserver. Weitere Informationen finden Sie unter Aktivieren der Übertragung von Überwachungsdatensätzen an einen Remotehost mit ESXCLI.

Sie können auch die FetchAuditRecords-API (im verwalteten DiagnosticsManager-Objekt) verwenden, um Überwachungsdatensätze anzuzeigen.

Sichern der ESXi-Konfiguration

In vSphere 7.0 Update 2 und höher ist die ESXi-Konfiguration durch Verschlüsselung geschützt.

Was ist eine sichere ESXi-Konfiguration

Viele ESXi-Dienste speichern geheime Schlüssel in ihren Konfigurationsdateien. Diese Konfigurationen werden in einer Startbank des ESXi-Hosts als archivierte Datei beibehalten. Vor vSphere 7.0 Update 2 ist die archivierte ESXi-Konfigurationsdatei nicht verschlüsselt. In vSphere 7.0 Update 2 und höher ist die archivierte Konfigurationsdatei verschlüsselt. Dies führt dazu, dass Angreifer diese Datei nicht direkt lesen oder ändern können, selbst wenn sie physischen Zugriff auf den Speicher des ESXi-Hosts haben.

Zusätzlich zur Verhinderung des Zugriffs eines Angreifers auf geheime Schlüssel kann eine sichere ESXi-Konfiguration bei Verwendung eines TPM die Verschlüsselungsschlüssel der virtuellen Maschine über Neustarts hinweg speichern. Wenn der ESXi-Host mit einem TPM konfiguriert ist, wird das TPM zum „Versiegeln“ der Konfiguration für den Host verwendet, was eine starke Sicherheitsgarantie bietet. Daher können verschlüsselte Arbeitslasten weiterhin funktionieren, wenn ein Schlüsselserver nicht verfügbar oder nicht erreichbar ist. Weitere Informationen hierzu finden Sie unter vSphere-Schlüsselpersistenz auf ESXi-Hosts.

Sie müssen die Verschlüsselung der ESXi-Konfiguration nicht manuell aktivieren. Wenn Sie vSphere 7.0 Update 2 oder höher installieren oder aktualisieren, ist die archivierte ESXi-Konfigurationsdatei verschlüsselt.

Informationen zu Aufgaben im Zusammenhang mit einer sicheren ESXi-Konfiguration finden Sie unter Verwalten einer sicheren ESXi-Konfiguration.

ESXi-Konfigurationsdateien vor vSphere 7.0 Update 2

Die Konfiguration eines ESXi-Hosts besteht aus Konfigurationsdateien für jeden Dienst, der auf dem Host ausgeführt wird. Die Konfigurationsdateien befinden sich in der Regel im Verzeichnis `/etc/`, aber sie können sich auch in anderen Namespaces befinden. Die Konfigurationsdateien enthalten Laufzeitinformationen über den Status der Dienste. Im Laufe der Zeit können sich die Standardwerte in den Konfigurationsdateien ändern, z. B. wenn Sie Einstellungen auf dem ESXi-Host ändern. Ein Cron-Auftrag sichert die ESXi-Konfigurationsdateien regelmäßig, oder wenn ESXi ordnungsgemäß heruntergefahren wird, oder bei Bedarf, und erstellt eine archivierte Konfigurationsdatei in der Startbank. Wenn ESXi neu startet, wird die archivierte Konfigurationsdatei gelesen und der Zustand wird wiederhergestellt, in dem sich ESXi befand, als die Sicherung erstellt wurde. Vor vSphere 7.0 Update 2 ist die archivierte Konfigurationsdatei unverschlüsselt. Dies führt dazu, dass ein Angreifer, der Zugriff auf den physischen ESXi-Speicher hat, diese Datei lesen und ändern kann, während das System offline ist.

Vorgehensweise zur Implementierung der sicheren ESXi-Konfiguration

Beim ersten Start nach der Installation oder dem Upgrade des ESXi-Hosts auf vSphere 7.0 Update 2 oder höher tritt Folgendes auf:

- Wenn der ESXi-Host über ein TPM verfügt und in der Firmware aktiviert ist, wird die archivierte Konfigurationsdatei mit einem im TPM gespeicherten Verschlüsselungsschlüssel verschlüsselt. Ab diesem Zeitpunkt wird die Konfiguration des Hosts durch das TPM versiegelt.
- Wenn der ESXi-Host nicht über ein TPM verfügt, verwendet ESXi eine Schlüsselableitungsfunktion (Key Derivation Function, KDF), um einen sicheren Verschlüsselungsschlüssel für die Konfiguration der archivierten Konfigurationsdatei zu generieren. Die Eingaben für KDF werden auf der Festplatte in der Datei `encryption.info` gespeichert.

Hinweis Wenn ein ESXi-Host über ein aktiviertes TPM-Gerät verfügt, erhalten Sie zusätzlichen Schutz.

Wenn der ESXi-Host nach dem ersten Start neu gestartet wird, tritt Folgendes auf:

- Wenn der ESXi-Host über ein TPM verfügt, muss der Host den Verschlüsselungsschlüssel vom TPM für diesen spezifischen Host abrufen. Wenn die TPM-Messungen der Versiegelungsrichtlinie entsprechen, die beim Erstellen des Verschlüsselungsschlüssels verwendet wurde, erhält der Host den Verschlüsselungsschlüssel vom TPM.
- Wenn der ESXi-Host nicht über ein TPM verfügt, liest ESXi Informationen aus der Datei `encryption.info` um die sichere Konfiguration zu entsperren.

Anforderungen für die sichere ESXi-Konfiguration

- ESXi 7.0 Update 2 oder höher
- TPM 2.0 für Konfigurationsverschlüsselung und die Möglichkeit, eine Versiegelungsrichtlinie zu verwenden

Wiederherstellungsschlüssel für die sichere ESXi-Konfiguration

Eine sichere ESXi-Konfiguration beinhaltet einen Wiederherstellungsschlüssel. Wenn Sie die sichere ESXi-Konfiguration wiederherstellen müssen, verwenden Sie einen Wiederherstellungsschlüssel, dessen Inhalt Sie als Befehlszeilen-Startoption eingeben. Sie können den Wiederherstellungsschlüssel auflisten, um eine Sicherung des Wiederherstellungsschlüssels zu erstellen. Sie können den Wiederherstellungsschlüssel auch im Rahmen Ihrer Sicherheitsanforderungen rotieren.

Die Sicherung des Wiederherstellungsschlüssels ist ein wichtiger Bestandteil der Verwaltung Ihrer sicheren ESXi-Konfiguration. vCenter Server generiert einen Alarm, um Sie daran zu erinnern, den Wiederherstellungsschlüssel zu sichern.

Alarm für Wiederherstellungsschlüssel in der sicheren ESXi-Konfiguration

Die Sicherung des Wiederherstellungsschlüssels ist ein wichtiger Bestandteil der Verwaltung Ihrer sicheren ESXi-Konfiguration. Wenn ein ESXi-Host im TPM-Modus mit dem vCenter Server verbunden oder erneut verbunden wird, generiert vCenter Server einen Alarm, um Sie daran zu erinnern, den Wiederherstellungsschlüssel zu sichern. Wenn Sie den Alarm zurücksetzen, wird er nicht erneut ausgelöst, es sei denn, die Bedingungen ändern sich.

Empfohlene Vorgehensweisen für die sichere ESXi-Konfiguration

Befolgen Sie diese empfohlenen Vorgehensweisen für den sicheren ESXi-Wiederherstellungsschlüssel:

- Wenn Sie einen Wiederherstellungsschlüssel auflisten, wird er vorübergehend in einer nicht vertrauenswürdigen Umgebung angezeigt und befindet sich im Arbeitsspeicher. Entfernen Sie Ablaufverfolgungen des Schlüssels.
  - Durch den Neustart des Hosts wird der verbleibende Schlüssel im Arbeitsspeicher entfernt.
  - Für erweiterten Schutz können Sie den Verschlüsselungsmodus auf dem Host aktivieren. Weitere Informationen hierzu finden Sie unter Explizites Aktivieren des Hostverschlüsselungsmodus.
- Vorgehensweise beim Durchführen einer Wiederherstellung:
  - Um Ablaufverfolgungen des Wiederherstellungsschlüssels in einer nicht vertrauenswürdigen Umgebung zu eliminieren, starten Sie den Host neu.
  - Um die Sicherheit zu verbessern, rotieren Sie den Wiederherstellungsschlüssel, um einen neuen Schlüssel zu verwenden, nachdem Sie den Schlüssel einmal wiederhergestellt haben.

Was sind TPM-Versiegelungsrichtlinien?

Ein TPM kann mithilfe von PCR-Messungen (Platform Configuration Register) Richtlinien implementieren, die den nicht autorisierten Zugriff auf vertrauliche Daten beschränken. Wenn Sie einen ESXi-Host mit einem TPM installieren oder ein Upgrade auf vSphere 7.0 Update 2 und höher durchführen, versiegelt das TPM die vertraulichen Informationen mithilfe einer Richtlinie, die die Einstellung für den sicheren Start enthält. Diese Richtlinie überprüft, dass, wenn der sichere Start aktiviert war, als Daten zum ersten Mal mit dem TPM versiegelt wurden, der sichere Start immer noch aktiviert sein muss, wenn versucht wird, die Daten bei einem nachfolgenden Start zu entsiegeln.

Secure Boot (sicherer Start) ist Bestandteil des UEFI-Firmwarestandards. Bei aktiviertem UEFI Secure Boot lädt ein Host einen UEFI-Treiber oder -Apps nur, wenn der Bootloader des Betriebssystems über ein gültige digitale Signatur verfügt.

Sie können die UEFI Secure Boot-Erzwingung deaktivieren oder aktivieren. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration.

Hinweis Wenn Sie bei der Installation von oder beim Upgrade auf vSphere 7.0 Update 2 oder höher kein TPM aktivieren, ist dies zu einem späteren Zeitpunkt mithilfe des folgenden Befehls möglich.

```
esxcli system settings encryption set --mode=TPM
```

Nach Aktivierung des TPM können Sie die Einstellung nicht mehr rückgängig machen.

Der Befehl `esxcli system settings encryption set` schlägt auf manchen TPMs selbst dann fehl, wenn das jeweilige TPM für den Host aktiviert ist.

- In vSphere 7.0 Update 2: TPMs von NationZ (NTZ), Infineon Technologies (IFX) und bestimmte neue Modelle (wie NPCT75x) von Nuvoton Technologies Corporation (NTC)
- In vSphere 7.0 Update 3: TPMs von NationZ (NTZ)

Wenn eine Installation oder ein Upgrade von vSphere 7.0 Update 2 das TPM beim ersten Start nicht verwenden kann, wird die Installation oder das Upgrade fortgesetzt, und der Modus wird standardmäßig auf KEINE (d. h. `--mode=NONE`) festgelegt. Das resultierende Verhalten sieht so aus, als ob das TPM nicht aktiviert ist.

Das TPM kann auch die Einstellung für die Startoption „execInstalledOnly“ in der Versiegelungsrichtlinie erzwingen. Die Erzwingung „execInstalledOnly“ ist eine erweiterte ESXi-Startoption, mit der garantiert wird, dass der VMkernel nur Binärdateien ausführt, die ordnungsgemäß verpackt und als Teil eines VIB signiert wurden. Die Startoption „execInstalledOnly“ ist von der Option für den sicheren Start abhängig. Die Erzwingung des sicheren Starts muss aktiviert sein, bevor Sie die Startoption „execInstalledOnly“ in der Versiegelungsrichtlinie erzwingen können. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der execInstalledOnly-Erzwingung für eine sichere ESXi-Konfiguration.

Verwalten einer sicheren ESXi-Konfiguration

Sie können ESXCLI-Befehle verwenden, um den Wiederherstellungsschlüssel für die sichere ESXi-Konfiguration anzuzeigen, den Wiederherstellungsschlüssel zu rotieren und die TPM-Richtlinien zu ändern (z. B. Erzwingen von UEFI Secure Boot).

Auflisten der Inhalte des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration

Sie können ESXCLI verwenden, um den Inhalt des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration anzuzeigen.

Diese Aufgabe gilt nur für einen ESXi-Host, der über ein TPM verfügt. Im Allgemeinen listen Sie den Inhalt des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration auf, um eine Sicherung zu erstellen, oder als Teil der rotierenden Wiederherstellungsschlüssel.

Voraussetzungen

- Zugriff auf den ESXCLI-Befehlssatz. Sie können ESXCLI-Befehle remote oder in der ESXi-Shell ausführen.
- Notwendige Berechtigung zur Verwendung der eigenständigen ESXCLI-Version oder über PowerCLI: **Host.Config.Settings**

Verfahren

1 Führen Sie den folgenden Befehl auf dem ESXi-Host aus.

```
esxcli system settings encryption recovery list
```

2 Speichern Sie die Ausgabe an einem sicheren Remotespeicherort als Sicherung, falls Sie die sichere Konfiguration wiederherstellen müssen.

Ergebnisse

Die Wiederherstellungsschlüssel-ID und der Schlüssel werden angezeigt.

Beispiel: Auflisten des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration

```
[root@host1] esxcli system settings encryption recovery list

Recovery ID                              Key
---------------------------------------  ---
{2DDD5424-7F3F-406A-8DA8-D62630F6C8BC}
478269-039194-473926-430939-686855-231401-642208-184477-602511
-225586-551660-586542-338394-092578-687140-267425
```

Rotieren des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration

Sie können ESXCLI verwenden, um den Wiederherstellungsschlüssel für die sichere ESXi-Konfiguration zu rotieren.

Diese Aufgabe gilt nur für einen ESXi-Host, der über ein TPM verfügt. Sie können den Wiederherstellungsschlüssel für die sichere ESXi-Konfiguration im Rahmen der Best Practices für die Sicherheit rotieren.

Voraussetzungen

- Zugriff auf den ESXCLI-Befehlssatz. Sie können ESXCLI-Befehle remote oder in der ESXi-Shell ausführen.
- Notwendige Berechtigung zur Verwendung der eigenständigen ESXCLI-Version oder über PowerCLI: **Host.Config.Settings**

Verfahren

1 Listet den Wiederherstellungsschlüssel auf.

Weitere Informationen hierzu finden Sie unter Auflisten der Inhalte des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration.

2 Führen Sie den folgenden Befehl aus.

```
esxcli system settings encryption recovery rotate [-k keyID] -u uuid
```

In diesem Befehl ist die optionale *keyID* die Schlüssel-ID im VMkernel-Schlüssel-Cache und *uuid* die Wiederherstellungs-ID (erhalten über den Befehl `esxcli system settings encryption recovery list`). Wenn Sie die optionale Schlüssel-ID nicht angeben, ersetzt ESXi den alten Wiederherstellungsschlüssel durch einen neuen, der zufällig generiert wird.

Ergebnisse

Der Wiederherstellungsschlüssel ist jetzt auf den Inhalt des Schlüssels festgelegt, auf den die Schlüssel-ID verweist (sofern sie bereitgestellt wurde). Andernfalls stellt ESXi eine neue Schlüssel-ID bereit.

Fehlerbehebung und Wiederherstellung der sicheren ESXi-Konfiguration

Sie können Probleme beim Starten beheben und wiederherstellen, die bei einer sicheren ESXi-Konfiguration auftreten können.

Wenn Sie ein TPM löschen (d. h. die Seed-Werte im TPM zurückgesetzt werden), wenn ein TPM fehlschlägt oder wenn Sie das Motherboard oder das TPM-Gerät ersetzen oder aber beides, müssen Sie Schritte zum Wiederherstellen der sicheren ESXi-Konfiguration durchführen. Sie müssen über den Wiederherstellungsschlüssel verfügen, um die Konfiguration wiederherstellen zu können. Bis Sie die Konfiguration wiederherstellen, kann der ESXi-Host nicht gestartet werden. Weitere Informationen hierzu finden Sie unter Wiederherstellen der sicheren ESXi-Konfiguration.

Obwohl es eher ungewöhnlich ist, ist es möglich, dass ein ESXi-Host die sichere Konfiguration nicht wiederherstellen oder entschlüsseln kann, was dazu führen kann, dass der Host nicht gestartet wird. Mögliche Situationen:

- Zur Einstellung für sicheren Start (oder andere Richtlinie) wechseln
- Tatsächliche Manipulation
- Der Wiederherstellungsschlüssel ist nicht verfügbar

Weitere Informationen zur Fehlerbehebung bei diesen Bedingungen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/81446.

Wiederherstellen der sicheren ESXi-Konfiguration

Wenn ein TPM fehlschlägt oder wenn Sie ein TPM löschen, müssen Sie die sichere ESXi-Konfiguration wiederherstellen. Bis Sie die Konfiguration wiederherstellen, kann der ESXi-Host nicht gestartet werden.

Die Wiederherstellung der ESXi-Konfiguration bezieht sich auf die folgenden Situationen:

- Sie haben das TPM gelöscht (d. h., die Speicher im TPM wurden zurückgesetzt).
- Das TPM ist fehlgeschlagen.
- Sie haben die Hauptplatine oder das TPM-Gerät oder beides ersetzt.

Informationen zur Behebung anderer Probleme bei der sicheren ESXi-Konfiguration finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/81446.

Führen Sie eine manuelle Wiederherstellung aus. Führen Sie die Wiederherstellung nicht als Teil eines Installations- oder Upgrade-Skripts durch.

Voraussetzungen

Rufen Sie Ihren Wiederherstellungsschlüssel ab. Sie sollten zuvor den Wiederherstellungsschlüssel aufgelistet und gespeichert haben. Weitere Informationen hierzu finden Sie unter Auflisten der Inhalte des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration.

Verfahren

1. (Optional) Wenn das TPM fehlgeschlagen ist, verschieben Sie die Festplatte (mit der Startbank) auf einen anderen Host mit einem TPM.
2. Starten Sie den ESXi-Host.
3. Wenn das ESXi-Installationsprogramms angezeigt wird, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.
4. Um die Konfiguration wiederherzustellen, hängen Sie an der Eingabeaufforderung die folgende Startoption an alle vorhandenen Startoptionen an.

   ```
   encryptionRecoveryKey=recovery_key
   ```

   Die sichere ESXi-Konfiguration wird wiederhergestellt, und der ESXi-Host wird gestartet.
5. Geben Sie zum Beibehalten der Änderung den folgenden Befehl ein:

   ```
   /sbin/auto-backup.sh
   ```

Nächste Schritte

Wenn Sie den Wiederherstellungsschlüssel eingeben, wird er vorübergehend in einer nicht vertrauenswürdigen Umgebung angezeigt und befindet sich im Arbeitsspeicher. Damit der Schlüssel vollständig aus dem Arbeitsspeicher entfernt wird, empfiehlt es sich als Best Practice (nicht erforderlich), den Host neu zu starten. Sie können den Link auch rotieren. Weitere Informationen hierzu finden Sie unter Rotieren des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration.

Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration

Sie können UEFI Secure Boot-Erzwingung aktivieren oder eine zuvor aktivierte UEFI Secure Boot-Erzwingung deaktivieren. Sie müssen ESXCLI verwenden, um die Einstellung im TPM auf dem ESXi-Host zu ändern.

Diese Aufgabe gilt nur für ESXi-Hosts, die über ein TPM verfügen. Bei UEFI Secure Boot handelt es sich um eine Firmware-Einstellung, mit der sichergestellt wird, dass die von der Firmware gestartete Software vertrauenswürdig ist. Weitere Informationen finden Sie unter UEFI Secure Boot für ESXi-Hosts. Die Aktivierung von UEFI Secure Boot kann bei jedem Start mithilfe des TPM erzwungen werden.

Voraussetzungen

- Zugriff auf den ESXCLI-Befehlssatz. Sie können ESXCLI-Befehle remote oder in der ESXi-Shell ausführen.
- Notwendige Berechtigung zur Verwendung der eigenständigen ESXCLI-Version oder über PowerCLI: **Host.Config.Settings**

Verfahren

1 Listen Sie die aktuellen Einstellungen auf dem ESXi-Host auf.

```
esxcli system settings encryption get
   Mode: TPM
   Require Executables Only From Installed VIBs: false
   Require Secure Boot: true
```

Bei aktivierter Secure Boot-Erzwingung wird „True“ für „Secure Boot anfordern“ angezeigt. Bei deaktivierter Secure Boot-Erzwingung wird „False“ für „Secure Boot anfordern“ angezeigt.

Wenn als Modus KEINE angezeigt wird, müssen Sie das TPM in der Firmware des Hosts aktivieren und den Modus durch Ausführen des folgenden Befehls festlegen:

```
esxcli system settings encryption set --mode=TPM
```

2 Aktivieren oder deaktivieren Sie Secure Boot-Erzwingung.

Option	Beschreibung

Aktivieren	a Fahren Sie den Host ordnungsgemäß herunter.
	Beispiel: Klicken Sie mit der rechten Maustaste auf den ESXi-Host im vSphere Client und wählen Sie **Betrieb > Herunterfahren** aus.
	b Aktivieren Sie „Secure Boot“ in der Firmware des Hosts.
	Weitere Informationen finden Sie in der Hardwaredokumentation Ihres Anbieters.
	c Starten Sie den Host neu.
	d Führen Sie den folgenden ESXCLI-Befehl aus.
	`esxcli system settings encryption set --require-secure-boot=T`
	e Überprüfen Sie die Änderung.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Bestätigen Sie, dass „True“ für „Secure Boot anfordern“ angezeigt wird.
	f Führen Sie zum Speichern der Einstellung folgenden Befehl aus:
	`/bin/backup.sh 0`

Deaktivieren	a Führen Sie den folgenden ESXCLI-Befehl aus.
	`esxcli system settings encryption set --require-secure-boot=F`
	b Überprüfen Sie die Änderung.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: false`
	Bestätigen Sie, dass „False“ für „Secure Boot anfordern“ angezeigt wird.
	c Führen Sie zum Speichern der Einstellung folgenden Befehl aus:
	`/bin/backup.sh 0`
	Sie können „Secure Boot“ in der Firmware des Hosts deaktivieren. Zum gegenwärtigen Zeitpunkt besteht die Abhängigkeit zwischen der Firmware-Einstellung und der TPM-Erzwingung jedoch nicht mehr.

Ergebnisse

Der ESXi-Host wird je nach Benutzerauswahl mit aktivierter oder deaktivierter Secure Boot-Erzwingung ausgeführt.

Hinweis Wenn Sie bei der Installation von oder beim Upgrade auf vSphere 7.0 Update 2 oder höher kein TPM aktivieren, ist dies zu einem späteren Zeitpunkt mithilfe des folgenden Befehls möglich.

```
esxcli system settings encryption set --mode=TPM
```

Nach Aktivierung des TPM können Sie die Einstellung nicht mehr rückgängig machen.

Der Befehl `esxcli system settings encryption set` schlägt auf manchen TPMs selbst dann fehl, wenn das jeweilige TPM für den Host aktiviert ist.

- In vSphere 7.0 Update 2: TPMs von NationZ (NTZ), Infineon Technologies (IFX) und bestimmte neue Modelle (wie NPCT75x) von Nuvoton Technologies Corporation (NTC)
- In vSphere 7.0 Update 3: TPMs von NationZ (NTZ)

Wenn eine Installation oder ein Upgrade von vSphere 7.0 Update 2 das TPM beim ersten Start nicht verwenden kann, wird die Installation oder das Upgrade fortgesetzt, und der Modus wird standardmäßig auf KEINE (d. h. `--mode=NONE`) festgelegt. Das resultierende Verhalten sieht so aus, als ob das TPM nicht aktiviert ist.

Aktivieren oder Deaktivieren der execInstalledOnly-Erzwingung für eine sichere ESXi-Konfiguration

Sie können execInstalledOnly-Erzwingung aktivieren oder eine zuvor aktivierte execInstalledOnly-Erzwingung deaktivieren. Sie müssen ESXCLI verwenden, um die Einstellung im TPM auf dem ESXi-Host zu ändern. UEFI Secure Boot-Erzwingung muss aktiviert sein. Erst dann kann die execInstalledOnly-Erzwingung aktiviert werden.

Diese Aufgabe gilt nur für ESXi-Hosts, die über ein TPM verfügen. Unter der Voraussetzung, dass die erweiterte ESXi-Startoption „execInstalledOnly“ auf TRUE festgelegt ist, wird garantiert, dass der VMkernel nur diejenigen Binärdateien ausführt, die als Teil des VIB gepackt und signiert wurden. Die Aktivierung dieser Startoption kann bei jedem Start mithilfe des TPM erzwungen werden.

Voraussetzungen

- Zum Aktivieren der execInstalledOnly-Erzwingung müssen Sie zuerst die UEFI Secure Boot-Erzwingung aktivieren. Die execInstalledOnly-Erzwingung baut auf der UEFI Secure Boot-Erzwingung auf. Weitere Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration.
- Zugriff auf den ESXCLI-Befehlssatz. Sie können ESXCLI-Befehle remote oder in der ESXi-Shell ausführen.

- Notwendige Berechtigung zur Verwendung der eigenständigen ESXCLI-Version oder über PowerCLI: **Host.Config.Settings**

Verfahren

1 Listen Sie die aktuellen Einstellungen auf dem ESXi-Host auf.

```
esxcli system settings encryption get
   Mode: TPM
   Require Executables Only From Installed VIBs: false
   Require Secure Boot: true
```

Bei aktivierter execInstalledOnly-Erzwingung wird „True“ für „Ausführbare Dateien nur aus installierten VIBs anfordern“ angezeigt. Bei deaktivierter execInstalledOnly-Erzwingung wird „False“ für „Ausführbare Dateien nur aus installierten VIBs anfordern“ angezeigt. Zum Aktivieren der execInstalledOnly-Erzwingung muss die Secure Boot-Erzwingung aktiviert sein, und „Secure Boot anfordern“ ist in diesem Fall auf „True“ festgelegt.

Wenn als Modus KEINE angezeigt wird, müssen Sie das TPM in der Firmware des Hosts aktivieren und den Modus durch Ausführen des folgenden Befehls festlegen:

```
esxcli system settings encryption set --mode=TPM
```

Wenn „Secure Boot anfordern“ auf „False“ festgelegt ist, finden Sie unter Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration Informationen zum Aktivieren der Erzwingung.

2 Aktivieren oder deaktivieren Sie die execInstalledOnly-Erzwingung.

Option	Beschreibung

Aktivieren	a Stellen Sie sicher, dass die Secure Boot-Option aktiviert ist.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Bestätigen Sie, dass „True“ für „Secure Boot anfordern“ angezeigt wird. Falls nicht, finden Sie weitere Informationen unter Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration.
	b Um den Laufzeitwert der execInstalledOnly-Startoption auf TRUE zu setzen, führen Sie den folgenden ESXCLI-Befehl aus.
	`esxcli system settings kernel set -s execInstalledOnly -v TRUE`
	c Fahren Sie den Host ordnungsgemäß herunter.
	Beispiel: Klicken Sie mit der rechten Maustaste auf den ESXi-Host im vSphere Client und wählen Sie **Betrieb > Herunterfahren** aus.
	d Starten Sie den Host neu.
	e Führen Sie zum Festlegen der execInstalledOnly-Erzwingung den folgenden ESXCLI-Befehl aus.
	`esxcli system settings encryption set --require-exec-installed-only=T`
	f Überprüfen Sie die Änderung.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: true`
	`Require Secure Boot: true`
	Vergewissern Sie sich, dass „Ausführbare Dateien nur aus installierten VIBs anfordern“ auf „true“ festgelegt ist.
	g Führen Sie zum Speichern der Einstellung folgenden Befehl aus:
	`/bin/backup.sh 0`

Deaktivieren	a Führen Sie den folgenden ESXCLI-Befehl aus.
	`esxcli system settings encryption set --require-exec-installed-only=F`
	b Überprüfen Sie die Änderung.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Vergewissern Sie sich, dass „Ausführbare Dateien nur aus installierten VIBs anfordern“ auf „false“ festgelegt ist.

Option	Beschreibung
	c Führen Sie zum Speichern der Einstellung folgenden Befehl aus: `/bin/backup.sh 0` Das TPM erzwingt die execInstalledOnly-Startoption nicht mehr.

Ergebnisse

Der ESXi-Host wird je nach Benutzerauswahl mit aktivierter oder deaktivierter execInstalledOnly-Erzwingung ausgeführt.

Deaktivieren der internen Laufzeitoption „execInstalledOnly“

Wenn Sie ESXi 8.0 oder höher installieren oder ein Upgrade auf 8.0 durchführen, wird auf Hosts standardmäßig die interne Laufzeitoption „execInstalledOnly“ aktiviert. Mit dieser Option können Sie Ihre Hosts vor Ransomware-Angriffen schützen. Wenn auf Ihren Hosts mit ESXi 8.0 oder höher weiterhin Nicht-VIB-Binärdateien aus externen Quellen ausgeführt werden, können Sie die interne Laufzeitoption „execInstalledOnly“ deaktivieren.

Die Option „execInstalledOnly“ schützt Ihre Hosts vor Ransomware-Angriffen, indem sichergestellt wird, dass der VMkernel nur die Binärdateien auf einem Host ausführt, die ordnungsgemäß verpackt und als Teil eines gültigen VIB signiert wurden.

Die Option „execInstalledOnly“ ist sowohl eine Start- als auch eine interne Laufzeitoption. Die Startoption „execInstalledOnly“, auch Kernel-Option genannt, wurde in ESXi 5.5 eingeführt. Die Startoption „execInstalledOnly“ ist standardmäßig deaktiviert. In vSphere 7.0 Update 2 oder höher können Sie die Startoption „execInstalledOnly“ bei jedem Start mithilfe eines TPM erzwingen. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der execInstalledOnly-Erzwingung für eine sichere ESXi-Konfiguration.

Die in ESXi 8.0 hinzugefügte interne Laufzeitoption „execInstalledOnly“ ist auf Hosts standardmäßig aktiviert. Die Startoption „execInstalledOnly“ ist weiterhin standardmäßig deaktiviert, außer dass eine zuvor aktivierte Startoption „execInstalledOnly“ die interne Laufzeitoption überschreibt, wenn Sie beide festlegen.

Hinweis Die Option „execInstalledOnly“ ist unabhängig von Secure Boot. Secure Boot überprüft, ob alle installierten VIBs signiert sind. Weitere Informationen finden Sie unter UEFI Secure Boot für ESXi-Hosts.

Wenn Sie die interne Laufzeitoption „execInstalledOnly“ deaktivieren, werden vCenter Server-Warnungen für den Host angezeigt.

Voraussetzungen

Zum Deaktivieren der internen Laufzeitoption „execInstalledOnly“ benötigen Sie Root-Zugriff auf den ESXi-Host. Sie können ESXCLI, PowerCLI oder die API verwenden. Die folgende Aufgabe verwendet ESXCLI.

Vorsicht Durch das Deaktivieren der internen Laufzeitoption „execInstalledOnly“ sind Sie anfälliger für Angriffe.

Verfahren

1. Stellen Sie mithilfe von SSH eine Verbindung zum ESXi-Host her.
2. Um die interne Laufzeitoption „execInstalledOnly“ zu deaktivieren, geben Sie den folgenden ESXCLI-Befehl ein.

```
esxcli system settings advanced set -o /User/execInstalledOnly -i 0
```

Sichern von vCenter Server-Systemen

4

Für die vCenter Server-Sicherung muss gewährleistet werden, dass der Host gesichert wird, auf dem vCenter Server läuft, indem Best Practices für die Zuweisung von Berechtigungen und Rollen verwendet werden und die Integrität der Clients überprüft wird, die sich mit vCenter Server verbinden.

Lesen Sie als Nächstes die folgenden Themen:

- Best Practices für die vCenter Server-Zugriffssteuerung
- Begrenzen der vCenter Server-Netzwerkkonnektivität
- Empfohlene Vorgehensweisen für die Sicherheit von vCenter Server
- Kennwortanforderungen und Sperrverhalten für vCenter
- Überprüfen der Fingerabdrücke bei Legacy-ESXi-Hosts
- Erforderliche Ports für vCenter Server

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 für den Zugriff auf vCenter Server

- Gewähren Sie die Administratorrolle nur Administratoren, die diese Rolle benötigen. Sie können benutzerdefinierte Rollen erstellen oder die Rolle „Kein Kryptografie-Administrator“ für Administratoren mit eingeschränkteren Rechten verwenden. Wenden Sie diese Rolle nicht auf eine Gruppe an, deren Mitgliedschaft nicht streng kontrolliert wird.
- Vergewissern Sie sich, dass die Anwendungen eindeutige Dienstkonten verwenden, wenn sie eine Verbindung zu einem vCenter Server-System herstellen.

Überwachen der Rechte von vCenter Server-Administratorbenutzern

Nicht alle Administratorbenutzer benötigen die Administratorrolle. Stattdessen können Sie eine benutzerdefinierte Rolle mit den geeigneten Rechten erstellen und diese den anderen Administratoren zuweisen.

Benutzer mit der vCenter Server-Administratorrolle haben Rechte für alle Objekte in der Hierarchie. Standardmäßig ermöglicht z. B. die Administratorrolle Benutzern die Interaktion mit Dateien und Programmen innerhalb des Gastbetriebssystems einer virtuellen Maschine. Wenn diese Rolle zu vielen Benutzern zugewiesen wird, kann dies die Vertraulichkeit, Verfügbarkeit oder Integrität der Daten auf der virtuellen Maschine beeinträchtigen. Erstellen Sie eine Rolle, die den Administratoren die benötigten Rechte zuweist, aber entfernen Sie einige der Verwaltungsrechte für die virtuelle Maschine. Siehe auch Verwenden des Rechte-Recorders.

Minimieren des Zugriffs auf die vCenter Server Appliance

Sorgen Sie dafür, dass sich keine Benutzer direkt bei der vCenter Server Appliance anmelden können. Benutzer, die bei der vCenter Server Appliance angemeldet sind, können absichtlich oder unabsichtlich Schaden anrichten, indem sie Einstellungen und Prozesse ändern. Diese Benutzer haben auch potenziell Zugriff auf vCenter Server-Anmeldedaten wie das SSL-Zertifikat. Erlauben Sie nur Benutzern mit legitimen Aufgaben, sich beim System anzumelden, und vergewissern Sie sich, dass diese Anmeldeereignisse überprüft werden.

Gewähren von minimalen Rechten für Datenbankbenutzer

Der Datenbankbenutzer benötigt nur bestimmte Rechte für den Datenbankzugriff.

Einige Rechte sind nur für die Installation und das Upgrade erforderlich. Nach der Installation bzw. dem Upgrade von vCenter Server können Sie diese Rechte für den Datenbankadministrator entfernen.

Beschränken des Zugriffs auf den Datenspeicherbrowser

Weisen Sie das Recht **Datenspeicher.Datenspeicher durchsuchen** nur Benutzern oder Gruppen zu, die tatsächlich dieses Recht benötigen. Benutzer mit diesem Recht können über den Webbrowser oder den vSphere Client Dateien in Datenspeichern, die der vSphere-Bereitstellung zugeordnet sind, anzeigen, hochladen oder herunterladen.

Beschränken der Ausführung von Befehlen durch Benutzer innerhalb einer virtuellen Maschine

Standardmäßig kann ein Benutzer mit der Administratorrolle mit den Dateien und Programmen eines Gastbetriebssystems innerhalb einer virtuellen Maschine interagieren. Erstellen Sie eine benutzerdefinierte Rolle ohne das Recht **Virtuelle Maschine.Gastvorgänge**, um das Sicherheitsrisiko für die Vertraulichkeit, Verfügbarkeit und Integrität des Gastbetriebssystems zu verringern. Weitere Informationen hierzu finden Sie unter Beschränken der Ausführung von Befehlen durch Benutzer innerhalb einer virtuellen Maschine.

Ändern der Kennwortrichtlinie für vpxuser

Standardmäßig ändert vCenter Server das vpxuser-Kennwort automatisch alle 30 Tage. Stellen Sie sicher, dass diese Einstellung die Unternehmensrichtlinien erfüllt, oder konfigurieren Sie andernfalls die vCenter Server-Kennwortrichtlinie. Weitere Informationen hierzu finden Sie unter Festlegen der vCenter Server-Kennwortrichtlinie.

Hinweis Vergewissern sie sich, dass die Kennwortablaufrichtlinie nicht zu kurz festgelegt ist.

Überprüfen von Rechten nach dem Neustart von vCenter Server

Überprüfen Sie die erneute Zuweisung von Rechten, wenn Sie vCenter Server neu starten. Wenn der Benutzer oder die Gruppe mit der Administratorrolle für den Stammordner während eines Neustarts nicht überprüft werden kann, wird die Rolle für diesen Benutzer bzw. diese Gruppe entfernt. Stattdessen gewährt vCenter Server dem vCenter Single Sign On-Administrator (administrator@vsphere.local) standardmäßig die Administratorrolle. Dieses Konto kann dann als vCenter Server-Administrator fungieren.

Richten Sie erneut ein benanntes Administratorkonto ein und weisen Sie diesem Konto die Administratorrolle zu, um die Verwendung des anonymen vCenter Single Sign On-Administratorkontos (standardmäßig administrator@vsphere.local) zu vermeiden.

Verwenden hoher Verschlüsselungsebenen für das Remote-Desktop-Protokoll

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

Überprüfen der vSphere Client-Zertifikate

Weisen Sie Benutzer des vSphere Client oder anderer Clientanwendungen an, Zertifikatverifizierungswarnungen zu beachten. Ohne Zertifikatverifizierung kann der Benutzer Ziel eines MiTM-Angriffs werden.

Festlegen der vCenter Server-Kennwortrichtlinie

Standardmäßig ändert vCenter Server das vpxuser-Kennwort automatisch alle 30 Tage. Sie können diesen Wert über den vSphere Client ändern.

Verfahren

1. Melden Sie sich beim vCenter Server-System mit dem vSphere Client an.
2. Wählen Sie in der Objekthierarchie das vCenter Server-System aus.
3. Klicken Sie auf **Konfigurieren**.
4. Klicken Sie auf **Erweiterte Einstellungen** und auf **Einstellungen bearbeiten**.
5. Klicken Sie auf das Symbol **Filter** und geben Sie **`VimPasswordExpirationInDays`** ein.

6 Legen Sie `VirtualCenter.VimPasswordExpirationInDays` entsprechend Ihren Anforderungen fest.

Entfernen abgelaufener oder widerrufener Zertifikate und Protokolle fehlgeschlagener Installationen

Wenn Sie abgelaufene oder widerrufene Zertifikate oder Installationsprotokolle für eine fehlgeschlagene Installation von vCenter Server auf Ihrem vCenter Server-System beibehalten, kann dies Ihre Umgebung beeinträchtigen.

Aus den folgenden Gründen müssen abgelaufene oder widerrufene Zertifikate entfernt werden:

- Wenn abgelaufene oder widerrufene Zertifikate nicht vom vCenter Server-System entfernt werden, wird die Umgebung anfällig für Man-in-the-Middle-Angriffe (MITM).
- In bestimmten Fällen wird eine Protokolldatei, die das Datenbankkennwort als normalen Text enthält, auf dem System erstellt, wenn die Installation von vCenter Server fehlschlägt. Ein Angreifer, der in das vCenter Server eindringt, könnte sich Zugriff auf dieses Kennwort verschaffen und zugleich auf die vCenter Server-Datenbank zugreifen.

Begrenzen der vCenter Server-Netzwerkkonnektivität

Zur Erhöhung der Sicherheit sollten Sie das vCenter Server-System nur im Verwaltungsnetzwerk bereitstellen und sicherstellen, dass für den Verwaltungsdatenverkehr von vSphere ein begrenztes Netzwerk verwendet wird. Durch Einschränkung der Netzwerkkonnektivität begrenzen Sie bestimmte Angriffsarten.

vCenter Server benötigt den Zugang nur zu einem Verwaltungsnetzwerk. Stellen Sie das vCenter Server-System möglichst nicht in anderen Netzwerken wie Ihrem Produktionsnetzwerk oder Speichernetzwerk bzw. einem Netzwerk mit Zugang zum Internet bereit. vCenter Server benötigt keinen Zugriff auf das Netzwerk, in dem vMotion ausgeführt wird.

vCenter Server benötigt Netzwerkkonnektivität zu den folgenden Systemen:

- Allen ESXi-Hosts.
- Der vCenter Server-Datenbank.
- Andere vCenter Server-Systeme (wenn die vCenter Server-Systeme Teil einer gemeinsamen vCenter Single Sign On-Domäne zum Replizieren von Tags, Berechtigungen usw. sind).
- Systemen, die Verwaltungsclients ausführen dürfen. Beispielsweise der vSphere Client, ein Windows-System, in dem Sie PowerCLI verwenden, oder ein anderer SDK-basierter Client.
- Infrastrukturdiensten wie DNS, Active Directory und PTP oder NTP.
- Anderen Systemen, auf denen Komponenten laufen, die für die Funktionen des vCenter Server-Systems wesentlich sind.

Verwenden Sie die Firewall auf dem vCenter Server. Beziehen Sie IP-basierte Zugriffsbeschränkungen ein, damit nur notwendige Komponenten mit dem vCenter Server-System kommunizieren können.

Bewerten der Verwendung von Linux-Clients mit CLIs und SDKs

Die Kommunikation zwischen Clientkomponenten und einem vCenter Server-System oder ESXi-Hosts wird standardmäßig durch eine SSL-Verschlüsselung geschützt. Bei den Linux-Versionen dieser Komponenten findet keine Zertifikatvalidierung statt. Daher sollten Sie die Verwendung dieser Clients einschränken.

Um die Sicherheit zu verbessern, können Sie die VMCA-signierten Zertifikate auf dem vCenter Server-System und auf den ESXi-Hosts durch Zertifikate ersetzen, die von einer Unternehmens- oder Drittanbieter-Zertifizierungsstelle signiert sind. Allerdings wären bestimmte Kommunikationen mit Linux-Clients immer noch anfällig für Machine-in-the-Middle-Angriffe. Die folgenden Komponenten sind anfällig, wenn sie auf einem Linux-Betriebssystem laufen.

- ESXCLI-Befehle
- vSphere SDK for Perl-Skripts
- Mit vSphere Web Services SDK geschriebene Programme

Sie können die Einschränkungen bei Linux-Clients lockern, wenn Sie geeignete Kontrollen erzwingen.

- Beschränken Sie den Zugriff zum Verwaltungsnetzwerk auf autorisierte Systeme.
- Verwenden Sie Firewalls, um sicherzustellen, dass nur autorisierte Hosts die Berechtigung haben, auf vCenter Server zuzugreifen.
- Verwenden Sie Bastionhosts (Jump-Box-Systeme), um sicherzustellen, dass Linux-Clients sich hinter dem „Jump“ befinden.

Überprüfen von vSphere Client-Plug-Ins

vSphere Client-Erweiterungen werden auf der Berechtigungsstufe ausgeführt, mit der der Benutzer angemeldet ist. Eine bösartige Erweiterung kann als nützliches Plug-In maskiert sein und schädliche Vorgänge ausführen, etwa Anmeldedaten stehlen oder die Systemkonfiguration ändern. Verwenden Sie zur Verbesserung der Sicherheit eine Installation, die ausschließlich autorisierte Erweiterungen vertrauenswürdiger Quellen enthält.

Eine vCenter Server-Installation enthält ein Erweiterbarkeits-Framework für den vSphere Client. Sie können dieses Framework verwenden, um den Client mit Menüauswahlen oder Symbolleistensymbolen zu erweitern. Die Erweiterungen können den Zugriff auf vCenter Server-Add-On-Komponenten oder externe, webbasierte Funktionen ermöglichen.

Die Verwendung des erweiterbaren Frameworks birgt das Risiko, ungewollte Funktionen zu installieren. Wenn beispielsweise ein Administrator ein Plug-In in einer Instanz des vSphere Client installiert, kann das Plug-In auf der Berechtigungsstufe dieses Administrators beliebige Befehle ausführen.

Zum Schutz vor einer möglichen Manipulation des vSphere Client überprüfen Sie alle installierten Plug-Ins in regelmäßigen Abständen und stellen Sie sicher, dass jedes Plug-In aus einer vertrauenswürdigen Quelle stammt.

Voraussetzungen

Für den Zugriff auf den vCenter Single Sign On-Dienst benötigen Sie entsprechende Rechte. Diese Berechtigungen weichen von den Berechtigungen für vCenter Server ab.

Verfahren

1. Melden Sie sich beim vSphere Client als „administrator@vsphere.local“ oder als Benutzer mit vCenter Single Sign On-Rechten an.
2. Wählen Sie auf der Homepage die Option **Verwaltung** und dann unter **Lösungen** die Option **Client-Plug-Ins** aus.
3. Prüfen Sie die Liste der Client-Plug-Ins.

Empfohlene Vorgehensweisen für die Sicherheit von vCenter Server

Verwenden Sie alle empfohlenen Vorgehensweisen zum Absichern eines vCenter Server-Systems. Mit zusätzlichen Schritten können Sie die Sicherheit Ihres vCenter Server verbessern.

Konfigurieren von Precision Time Protocol oder Network Time Protocol

Stellen Sie sicher, dass alle Systeme dieselbe relative Zeitquelle verwenden. Diese Zeitquelle muss mit einem vereinbarten Zeitstandard wie z. B. der koordinierten Weltzeit (Coordinated Universal Time, UTC) synchronisiert sein. Synchronisierte Systeme sind für die Zertifikatsvalidierung wesentlich. Precision Time Protocol (PTP) und Network Time Protocol (NTP) erleichtern auch die Verfolgung eines Eindringlings in Protokolldateien. Bei falschen Zeiteinstellungen ist es schwierig, Protokolldateien zur Suche nach Angriffen zu untersuchen und abzugleichen. Dies führt zu ungenauen Ergebnissen beim Audit. Weitere Informationen hierzu finden Sie unter Synchronisieren der Uhrzeit in vCenter Server mit einem NTP-Server.

Beschränken des vCenter Server-Netzwerkzugriffs

Beschränken Sie den Zugriff auf Komponenten, die für die Kommunikation mit der vCenter Server erforderlich sind. Das Blockieren des Zugriffs von unnötigen Systemen reduziert das Risiko von Angriffen auf das Betriebssystem.

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

Konfigurieren eines Bastionhosts

Zum Schutz Ihrer Assets konfigurieren Sie einen Bastionhost (auch als „Jump Box“ bezeichnet), um Verwaltungsaufgaben mit erhöhten Rechten durchzuführen. Ein Bastionhost ist ein spezieller Computer, der eine minimale Anzahl an administrativen Anwendungen hostet. Alle anderen unnötigen Dienste werden entfernt. Der Host befindet sich in der Regel im Verwaltungsnetzwerk. Ein Bastionhost erhöht den Schutz von Assets, da er die Anmeldung auf wichtige Personen beschränkt, für den Anmeldevorgang Firewallregeln erfordert und durch Audit-Tools eine zusätzliche Überwachung stattfindet.

Kennwortanforderungen und Sperrverhalten für vCenter

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

Dieser Abschnitt befasst sich mit vCenter Single Sign-On-Kennwörtern. Unter Kennwörter und Kontosperrung für ESXi werden Kennwörter von lokalen ESXi-Benutzern besprochen.

Kennwortanforderungen für den vCenter Single Sign On-Administrator

Das Kennwort für den vCenter Single Sign On-Administrator, standardmäßig „administrator@vsphere.local“, wird in den vCenter Single Sign On-Kennwortrichtlinien angegeben. Standardmäßig muss dieses Kennwort die folgenden Anforderungen erfüllen:

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

Das Kennwort für diesen Benutzer darf nicht mehr als 20 Zeichen lang sein. Nicht-ASCII-Zeichen sind zulässig. Administratoren können die Standard-Kennwortrichtlinien ändern. Informationen finden Sie in der Dokumentation *vSphere-Authentifizierung*.

vCenter Server-Kennwortanforderungen

In vCenter Server werden die Kennwortanforderungen von vCenter Single Sign On oder einer konfigurierten Identitätsquelle vorgegeben, z. B. Active Directory oder OpenLDAP.

Sperrverhalten von vCenter Single Sign-On

Benutzer werden nach einer vorher festgelegten Anzahl von aufeinanderfolgenden Fehlversuchen gesperrt. Standardmäßig werden Benutzer nach fünf aufeinanderfolgenden Fehlerversuchen innerhalb von drei Minuten gesperrt. Ein gesperrtes Konto wird automatisch nach fünf Minuten wieder entsperrt. Sie können diese Standardeinstellungen mithilfe der vCenter Single Sign-On-Sperrrichtlinie ändern. Informationen finden Sie in der Dokumentation *vSphere-Authentifizierung*.

Der vCenter Single Sign On-Domänenadministrator, standardmäßig „administrator@vsphere.local“, ist von der Sperrrichtlinie nicht betroffen. Die Kennwortrichtlinie betrifft den Benutzer.

vCenter Server-Kennwortänderungen

Wenn Sie Ihr Kennwort kennen, können Sie es mithilfe des Befehls `dir-cli password change` ändern. Falls Sie Ihr Kennwort vergessen haben, kann ein vCenter Single Sign On-Administrator es mithilfe des Befehls `dir-cli password reset` zurücksetzen.

Suchen Sie in der VMware-Knowledgebase nach Informationen über das Ablaufen von Kennwörtern in verschiedenen Versionen von vSphere sowie nach verwandten Themen.

Überprüfen der Fingerabdrücke bei Legacy-ESXi-Hosts

In vSphere 6.0 und höher werden den Hosts standardmäßig VMCA-Zertifikate zugewiesen. Wenn Sie den Zertifikatmodus zu Fingerabdruck ändern, können Sie für Legacy-Hosts auch weiterhin den Fingerabdruckmodus verwenden. Die Fingerabdrücke werden im vSphere Client überprüft.

Hinweis Standardmäßig bleiben die Zertifikate bei Upgrades erhalten.

Verfahren

1. Navigieren Sie zum vCenter Server in der Bestandsliste des vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter **Einstellungen** auf **Allgemein**.
4. Klicken Sie auf **Bearbeiten**.
5. Klicken Sie auf **SSL-Einstellungen**.
6. Falls einer Ihrer Hosts aus ESXi 5.5 oder früher eine manuelle Validierung erfordert, vergleichen Sie die für die Hosts aufgeführten Fingerabdrücke mit den Fingerabdrücken in der Hostkonsole.

   Verwenden Sie die Benutzerschnittstelle der direkten Konsole (DCUI), um den Fingerabdruck des Hosts abzurufen.

   a. Melden Sie sich bei der direkten Konsole an und drücken Sie F2, um das Menü für die Systemanpassung aufzurufen.

   b. Wählen Sie **Support-Informationen anzeigen**.

      Der Fingerabdruck des Hosts wird in der Spalte auf der rechten Seite angezeigt.
7. Stimmen die Fingerabdrücke überein, wählen Sie das Kontrollkästchen **Überprüfen** neben dem Host aus.

   Hosts, die nicht ausgewählt sind, werden getrennt, nachdem Sie auf **OK** klicken.
8. Klicken Sie auf **Speichern**.

Erforderliche Ports für vCenter Server

Das vCenter Server-System muss in der Lage sein, Daten an jeden verwalteten Host zu senden und Daten vom vSphere Client zu erhalten. Die Quell- und Zielhosts müssen Daten über vorab festgelegte TCP- und UDP-Ports miteinander austauschen können, um Migrations- und Bereitstellungsaktivitäten zwischen verwalteten Hosts zu ermöglichen.

Der Zugriff auf vCenter Server erfolgt über vorab festgelegte TCP- und UDP-Ports. Wenn Netzwerkkomponenten, die außerhalb einer Firewall liegen, verwaltet werden müssen, muss ggf. die Firewall neu konfiguriert werden, damit auf die entsprechenden Ports zugegriffen werden kann. Eine Liste aller unterstützten Ports und Protokolle in vSphere finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com.

Wenn während der Installation ein Port verwendet wird oder mittels einer Sperrliste gesperrt ist, zeigt das Installationsprogramm für vCenter Server eine Fehlermeldung an. Sie müssen eine andere Portnummer verwenden, um mit der Installation fortfahren zu können. Es gibt interne Ports, die nur für den Datenaustausch zwischen Prozessen verwendet werden.

Für die Kommunikation verwendet VMware festgelegte Ports. Zudem überwachen die verwalteten Hosts die festgelegten Ports auf Daten von vCenter Server. Wenn zwischen diesen Elementen eine integrierte Firewall vorhanden ist, öffnet das Installationsprogramm die Ports während der Installation bzw. des Upgrades. Für benutzerdefinierte Firewalls müssen die erforderlichen Ports manuell geöffnet werden. Wenn sich eine Firewall zwischen zwei von verwalteten Hosts befindet und Sie Quell- oder Zielaktivitäten wie z. B. eine Migration oder einen Klonvorgang ausführen möchten, muss der verwaltete Host Daten empfangen können.

Wenn das vCenter Server-System einen anderen Port zum Empfangen von vSphere Client-Daten verwenden soll, lesen Sie die Dokumentation *vCenter Server und Hostverwaltung*.

Sichern von virtuellen Maschinen 5

Das Gastbetriebssystem, das in der virtuellen Maschine läuft, ist denselben Sicherheitsrisiken ausgesetzt wie ein physisches System. Sichern Sie virtuelle Maschinen genauso wie physische Maschinen und halten Sie sich an die in diesem Dokument und im *Security Configuration Guide* (Handbuch für die Sicherheitskonfiguration – früher bekannt als *Handbuch für Hardening*) besprochenen Best Practices.

Das *Handbuch für die Sicherheitskonfiguration* finden Sie unter https://core.vmware.com/security.

Lesen Sie als Nächstes die folgenden Themen:

- Aktivieren oder Deaktivieren von UEFI Secure Boot für eine virtuelle Maschine
- Virtuelle Maschine – Empfohlene Vorgehensweisen für die Sicherheit
- Sichern von virtuellen Maschinen mit Intel Software Guard-Erweiterungen
- Sichern von virtuellen Maschinen mit AMD Secure Encrypted Virtualization-Encrypted State

Aktivieren oder Deaktivieren von UEFI Secure Boot für eine virtuelle Maschine

UEFI Secure Boot ist ein Sicherheitsstandard, mit dem sichergestellt werden kann, dass ein PC nur über Software gestartet wird, die durch den entsprechenden PC-Hersteller als vertrauenswürdig eingestuft wird. Für bestimmte Hardwareversionen und Betriebssysteme von virtuellen Maschinen können Sie einen sicheren Start in der gleichen Weise wie für physische Maschinen aktivieren.

In einem Betriebssystem, das UEFI Secure Boot unterstützt, ist jedes Element der Boot-Software signiert, einschließlich dem Bootloader, dem Betriebssystem-Kernel und den Betriebssystem-Treibern. Zur Standardkonfiguration der virtuellen Maschine gehören verschiedene Code-Signaturzertifikate.

- Ein Microsoft-Zertifikat, das nur für den Start von Windows verwendet wird.
- Ein Microsoft-Zertifikat, das für Drittanbieter-Code verwendet wird, welcher von Microsoft signiert ist, wie beispielsweise Linux-Bootloader.
- Ein VMware-Zertifikat, das nur für den Start von ESXi innerhalb einer virtuellen Maschine verwendet wird.

Zur Standardkonfiguration der virtuellen Maschine gehört ein Zertifikat für Authentifizierungsanforderungen, um die Konfiguration des sicheren Starts zu ändern. Dazu gehört auch die Widerrufsliste für den sicheren Start von innerhalb der virtuellen Maschine. Dies ist ein Microsoft KEK-Zertifikat (Key Exchange Key, Schlüsselaustauschschlüssel).

VMware Tools Version 10.1 oder höher ist für virtuelle Maschinen erforderlich, die UEFI Secure Boot verwenden. Sie können diese virtuellen Maschinen auf eine höhere Version von VMware Tools aktualisieren, wenn diese verfügbar ist.

Bei Linux-basierten virtuellen Maschinen wird das VMware Host-Gast-Dateisystem im sicheren Startmodus nicht unterstützt. Entfernen Sie das VMware Host-Gast-Dateisystem aus den VMware Tools, bevor Sie den sicheren Start aktivieren.

Hinweis Wenn Sie den sicheren Start für eine virtuelle Maschine aktivieren, können Sie nur signierte Treiber in diese virtuelle Maschine laden.

In dieser Aufgabe wird beschrieben, wie der sichere Start für eine virtuelle Maschine mithilfe von vSphere Client aktiviert und deaktiviert wird. Sie können auch Skripte schreiben, um die Einstellungen für virtuelle Maschinen zu verwalten. Sie können beispielsweise das Ändern der Firmware von BIOS zu EFI für virtuelle Maschinen mit dem folgenden PowerCLI-Code automatisieren:

```
$vm = Get-VM TestVM

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

Weitere Informationen finden Sie im *VMware PowerCLI-Benutzerhandbuch*.

Voraussetzungen

Sie können einen sicheren Start nur aktivieren, wenn alle Voraussetzungen erfüllt sind. Wenn die Voraussetzungen nicht erfüllt sind, wird das Kontrollkästchen nicht im vSphere Client angezeigt.

- Stellen Sie sicher, dass das Betriebssystem und die Firmware der virtuellen Maschine UEFI Secure Boot unterstützen.
  - EFI-Firmware
  - Virtuelle Hardwareversion 13 oder höher.
  - Betriebssystem, das UEFI Secure Boot unterstützt.

  Hinweis Manche Gastbetriebssysteme unterstützten das Wechseln vom BIOS-Start zum UEFI-Start ohne Änderungen des Gastbetriebssystems nicht. Lesen Sie in der Dokumentation zum Gastbetriebssystem nach, bevor Sie einen Wechsel zum UEFI-Start vornehmen. Wenn Sie eine virtuelle Maschine, für die bereits UEFI Secure Boot verwendet wird, auf ein Betriebssystem aktualisieren, das UEFI Secure Boot unterstützt, können Sie den sicheren Start für diese virtuelle Maschine aktivieren.

- Schalten Sie die virtuelle Maschine aus. Wenn die virtuelle Maschine ausgeführt wird, ist das Kontrollkästchen abgeblendet.

Verfahren

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

Ergebnisse

Wenn die virtuelle Maschine gestartet wird, werden nur Komponenten mit gültigen Signaturen zugelassen. Der Startvorgang wird angehalten, und es wird ein Fehler angezeigt, wenn eine Komponente mit einer fehlenden oder ungültigen Signatur festgestellt wird.

Virtuelle Maschine – Empfohlene Vorgehensweisen für die Sicherheit

Die Einhaltung der empfohlenen Vorgehensweisen für die Sicherheit in Bezug auf virtuelle Maschinen ist eine wichtige Maßnahme zur Wahrung der Integrität Ihrer vSphere-Umgebung.

- Allgemeiner Schutz für virtuelle Maschinen

  Eine virtuelle Maschine ist nahezu mit einem physischen Server äquivalent. Wenden Sie in virtuellen Maschinen die gleichen Sicherheitsmaßnahmen wie für physische Systeme an.

- Verwendung von Vorlagen zum Bereitstellen von virtuellen Maschinen

  Wenn Sie Gastbetriebssysteme und Anwendungen auf einer virtuellen Maschine manuell installieren, besteht das Risiko einer fehlerhaften Konfiguration. Mithilfe einer Vorlage zum Erfassen eines abgesicherten Basisbetriebssystem-Images ohne installierte Anwendungen können Sie sicherstellen, dass alle virtuellen Maschinen mit einem bekannten Baseline-Sicherheitsniveau erstellt werden.

- Beschränken der Verwendung der VM-Konsole auf ein Minimum

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

- Verhindern, dass virtuelle Maschinen Ressourcen in Besitz nehmen

  Wenn eine virtuelle Maschine so viele Hostressourcen verbraucht, dass andere virtuelle Maschinen auf dem Host ihre Funktionen nicht mehr erfüllen können, kann es zur Dienstverweigerung (Denial of Service, DoS) kommen. Um zu verhindern, dass eine virtuelle Maschine DoS verursacht, verwenden Sie Funktionen der Hostressourcenverwaltung, beispielsweise die Einrichtung von Anteilen und die Verwendung von Ressourcenpools.

- Deaktivieren unnötiger Funktionen innerhalb von virtuellen Maschinen

  Jeder Dienst, der in einer virtuellen Maschine ausgeführt wird, ist ein potenzielles Angriffsziel. Indem Sie Systemkomponenten deaktivieren, die zur Ausführung der Anwendung bzw. des Diensts auf dem System nicht benötigt werden, verringern Sie das Angriffsrisiko.

Allgemeiner Schutz für virtuelle Maschinen

Eine virtuelle Maschine ist nahezu mit einem physischen Server äquivalent. Wenden Sie in virtuellen Maschinen die gleichen Sicherheitsmaßnahmen wie für physische Systeme an.

Befolgen Sie diese Best Practices zum Schutz Ihrer virtuellen Maschine. Weitere Informationen finden Sie im *vSphere Security Configuration Guide* unter https://core.vmware.com/security-configuration-guide.

Patchen von virtuellen Maschinen

Halten Sie alle Sicherheitsmaßnahmen immer auf dem neuesten Stand, und wenden Sie immer die entsprechenden Patches an. Beachten Sie auch die Updates für inaktive virtuelle Maschinen, die ausgeschaltet sind, weil diese leicht vergessen werden können. Vergewissern Sie sich beispielsweise, dass Schutzmechanismen wie Virenschutzsoftware, Anti-Spyware, Erkennung von Eindringversuchen usw. für virtuelle Maschine in Ihrer virtuellen Infrastruktur aktiviert sind. Stellen Sie außerdem sicher, dass ausreichend Speicherplatz für die Protokolle der virtuellen Maschinen vorhanden ist.

Prüfen von Maschinen auf Viren

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. Wägen die beiden Sicherheitsmaßnahmen gegen Leistungsvorteile ab, insbesondere wenn Sie sich sicher sind, dass sich die virtuellen Maschinen in einer vollständig vertrauenswürdigen Umgebung befinden.

Deaktivieren serieller Ports auf virtuellen Maschinen

Über serielle Schnittstellen können Peripheriegeräte an die virtuelle Maschine angeschlossen werden. Administratoren verwenden häufig serielle Ports, um eine direkte Verbindung auf niedriger Ebene mit der Konsole eines Servers bereitzustellen. Ein virtueller serieller Port ermöglicht denselben Zugriff auf eine virtuelle Maschine. Da serielle Ports einen Zugriff auf niedriger Ebene ermöglichen und über keine strengen Kontrollen wie Protokollierung oder Rechte verfügen, sollten Sie diese auf virtuellen Maschinen deaktiviert lassen.

Verwendung von Vorlagen zum Bereitstellen von virtuellen Maschinen

Wenn Sie Gastbetriebssysteme und Anwendungen auf einer virtuellen Maschine manuell installieren, besteht das Risiko einer fehlerhaften Konfiguration. Mithilfe einer Vorlage zum Erfassen eines abgesicherten Basisbetriebssystem-Images ohne installierte Anwendungen können Sie sicherstellen, dass alle virtuellen Maschinen mit einem bekannten Baseline-Sicherheitsniveau erstellt werden.

Sie können Vorlagen verwenden, die ein abgesichertes, gepatchtes und korrekt konfiguriertes Betriebssystem enthalten, um andere, anwendungsspezifische Vorlagen zu erstellen, oder mithilfe der Anwendungsvorlage virtuelle Maschinen bereitstellen.

Verfahren

- Stellen Sie Vorlagen für die Erstellung von virtuellen Maschinen bereit, die abgesicherte, gepatchte und korrekt konfigurierte Betriebssystembereitstellungen enthalten.

  Wenn möglich, stellen Sie auch Anwendungen in Vorlagen bereit. Achten Sie darauf, dass die Anwendungen nicht von Informationen abhängen, die spezifisch für eine virtuelle Maschine sind, die bereitgestellt werden soll.

Nächste Schritte

Weitere Informationen zu Vorlagen finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Beschränken der Verwendung der VM-Konsole auf ein Minimum

Die VM-Konsole bietet für eine virtuelle Maschine dieselbe Funktionalität wie ein Monitor auf einem physischen Server. Benutzer mit Zugriff auf die VM-Konsole haben Zugriff auf die Energieverwaltung der virtuellen Maschine und auf Konnektivitätssteuerelemente von

Wechselmedien. Der Zugriff auf die Konsole kann deshalb einen bösartigen Angriff auf eine virtuelle Maschine ermöglichen.

Verfahren

1 Verwenden Sie native Remoteverwaltungsdienste wie etwa Terminaldienste und SSH für die Interaktion mit virtuellen Maschinen.

   Gewähren Sie nur dann Zugriff auf die VM-Konsole, wenn dies erforderlich ist.

2 Beschränken Sie die Verbindungen auf die VM-Konsole.

   Beschränken Sie beispielsweise in einer Hochsicherheitsumgebung die Verbindungen auf eine. In manchen Umgebungen können Sie den Grenzwert erhöhen, wenn mehrere gleichzeitige Verbindungen für reguläre Aufgaben erforderlich sind.

   a Schalten Sie die virtuelle Maschine im vSphere Client aus.

   b Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

   c Klicken Sie auf die Registerkarte **VM-Optionen** und erweitern Sie **Optionen der VMware-Remotekonsole**.

   d Geben Sie die maximale Anzahl der Sitzungen ein, z. B. **2**.

   e Klicken Sie auf **OK**.

Verhindern, dass virtuelle Maschinen Ressourcen in Besitz nehmen

Wenn eine virtuelle Maschine so viele Hostressourcen verbraucht, dass andere virtuelle Maschinen auf dem Host ihre Funktionen nicht mehr erfüllen können, kann es zur Dienstverweigerung (Denial of Service, DoS) kommen. Um zu verhindern, dass eine virtuelle Maschine DoS verursacht, verwenden Sie Funktionen der Hostressourcenverwaltung, beispielsweise die Einrichtung von Anteilen und die Verwendung von Ressourcenpools.

Standardmäßig haben alle virtuellen Maschinen auf einem ESXi-Host gleiche Anteile an den Ressourcen. Sie können mithilfe von Anteilen und Ressourcenpools einen Denial-of-Service-Angriff verhindern, der bewirkt, dass eine virtuelle Maschine so viele Ressourcen des Hosts beansprucht, dass andere virtuelle Maschinen auf demselben Host ihre beabsichtigten Funktionen nicht ausführen können.

Legen Sie Grenzwerte erst fest bzw. verwenden Sie Ressourcenpools erst, wenn Sie die Auswirkungen vollständig verstanden haben.

Verfahren

1 Stellen Sie für jede virtuelle Maschine gerade genug Ressourcen (CPU und Arbeitsspeicher) bereit, sodass sie ordnungsgemäß arbeitet.

2 Verwenden Sie Anteile, um Ressourcen für kritische virtuelle Maschinen zu garantieren.

3 Gruppieren Sie virtuelle Maschinen mit ähnlichen Anforderungen in Ressourcenpools.

4 Behalten Sie in jedem Ressourcenpool die Standardwerte für Anteile bei, um sicherzustellen, dass jeder virtuellen Maschine im Pool ungefähr dieselbe Ressourcenpriorität zugeordnet ist.

   Mit dieser Einstellung kann eine einzelne virtuelle Maschine nicht mehr Ressourcen als andere virtuelle Maschinen im Ressourcenpool verwenden.

Nächste Schritte

Informationen über Ressourcenanteile und Grenzwerte finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Deaktivieren unnötiger Funktionen innerhalb von virtuellen Maschinen

Jeder Dienst, der in einer virtuellen Maschine ausgeführt wird, ist ein potenzielles Angriffsziel. Indem Sie Systemkomponenten deaktivieren, die zur Ausführung der Anwendung bzw. des Diensts auf dem System nicht benötigt werden, verringern Sie das Angriffsrisiko.

Für virtuelle Maschinen werden in der Regel weniger Dienste bzw. Funktionen benötigt als für physische Server. Wenn Sie ein System virtualisieren, prüfen Sie, ob bestimmte Dienste oder Funktionen erforderlich sind.

Hinweis Installieren Sie Gastbetriebssysteme gegebenenfalls mit den Installationsmodi „Minimal“ oder „Kern“, um die Größe, Komplexität und Angriffsfläche der Gastbetriebssysteme zu verringern.

Verfahren

- Deaktivieren Sie nicht verwendete Dienste im Betriebssystem.

  Wenn auf dem System beispielsweise ein Dateiserver ausgeführt wird, deaktivieren Sie die Webdienste.
- Trennen Sie nicht verwendete physische Geräte wie CD/DVD-Laufwerke, Diskettenlaufwerke und USB-Adapter.
- Deaktivieren Sie nicht verwendete Funktionen, wie etwa nicht verwendete Anzeigefunktionen oder VMware-Ordnerfreigaben, mit denen die Freigabe von Hostdateien an die virtuelle Maschine (Host-Gastdateisystem) aktiviert wird.
- Deaktivieren Sie Bildschirmschoner.
- Führen Sie das X Window-System auf Linux-, BSD- oder Solaris-Gastbetriebssystemen nur aus, wenn es erforderlich ist.

Entfernen nicht benötigter Hardwaregeräte von virtuellen Maschinen

Jedes aktivierte oder verbundene Gerät in einer virtuellen Maschine stellt einen potenziellen Angriffskanal dar. Benutzer und Prozesse mit Berechtigungen für die virtuelle Maschine können Hardwaregeräte wie Netzwerkadapter oder CD-ROM-Laufwerke einbinden oder trennen.

Angreifer können diese Fähigkeit nutzen, um die Sicherheit einer virtuellen Maschine zu gefährden. Das Entfernen überflüssiger Hardwaregeräte kann Angriffe verhindern.

Ein Angreifer mit Zugriff auf eine virtuelle Maschine kann ein getrenntes Hardwaregerät verbinden und auf die vertraulichen Informationen eines verbleibenden Mediums auf einem Hardwaregerät zugreifen. Der Angreifer könnte einen Netzwerkadapter trennen, um die virtuelle Maschine vom Netzwerk zu isolieren, was zu einem Denial-of-Service-Fehler führt.

- Verbinden Sie keine unzulässigen Geräte mit der virtuellen Maschine.
- Entfernen Sie Hardwaregeräte, die nicht benötigt oder nicht verwendet werden.
- Deaktivieren Sie nicht benötigte virtuelle Geräte in einer virtuellen Maschine.
- Stellen Sie sicher, dass nur erforderliche Geräte mit einer virtuellen Maschine verbunden sind. Virtuelle Maschinen verwenden selten serielle oder parallele Ports. In der Regel werden CD/DVD-Laufwerke nur während der Softwareinstallation temporär verbunden.

Verfahren

1. Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
3. Klicken Sie auf der Registerkarte **Virtuelle Hardware** auf das Symbol mit den Auslassungspunkten und wählen Sie **Gerät entfernen** aus, um nicht erforderliche Hardwaregeräte zu deaktivieren.

   Prüfen Sie insbesondere auch die folgenden Geräte:

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

   Hinweis Sie müssen PowerCLI-Befehle verwenden, um Diskettenlaufwerke in vSphere 7.0 und höher zu verwalten.

Deaktivieren nicht verwendeter Anzeigefunktionen auf virtuellen Maschinen

Angreifer können sich nicht verwendete Anzeigefunktionen zunutze machen, um Schadcode in Ihre Umgebung einzuschleusen. Deaktivieren Sie Funktionen, die in Ihrer Umgebung nicht verwendet werden.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.

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

3 Klicken Sie auf **Erweiterte Parameter**.

4 Fügen Sie ggf. die folgenden Parameter hinzu bzw. bearbeiten Sie sie.

Name	Beschreibung
svga.vgaonly	Wenn Sie diesen Parameter auf TRUE setzen, werden erweiterte Grafikfunktionen deaktiviert. Legen Sie diesen Parameter bei modernen Gastbetriebssystemen nicht auf TRUE fest, da sie nicht ordnungsgemäß funktionieren. Wenn `svga.vgaonly` auf TRUE festgelegt ist, ist nur der Textkonsolenmodus verfügbar. Bei dieser Einstellung bleibt der Parameter `mks.enable3d` wirkungslos. **Hinweis** Wenden Sie diese Einstellung nur auf virtuelle Maschinen an, die keine virtualisierte Grafikkarte benötigen.
mks.enable3d	Auf virtuellen Maschinen, die keine 3D-Funktion benötigen, können Sie diesen Parameter auf FALSE setzen.

5 Klicken Sie auf **OK**.

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 Client aktivieren.

Die Standardwerte für diese Optionen werden festgelegt, um eine sichere Umgebung zu gewährleisten. Sie müssen sie jedoch explizit auf „true“ setzen, damit die Überwachungstools überprüfen können, ob die Einstellung korrekt ist.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.

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

3 Klicken Sie auf **Erweiterte Parameter**.

4 Fügen Sie die folgenden Parameter hinzu bzw. bearbeiten Sie sie.

Name	Wert
`isolation.tools.copy.disable`	`true`
`isolation.tools.paste.disable`	`true`
`isolation.tools.setGUIOptions.enable`	`false`

Diese Optionen heben die Einstellungen in der Systemsteuerung von VMware Tools auf dem Gastbetriebssystem auf.

5 Klicken Sie auf **OK**.

6 (Optional) Starten Sie die virtuelle Maschine neu, wenn Sie Änderungen an den Konfigurationsparametern vornehmen.

Begrenzen der Offenlegung sensibler Daten, die in die Zwischenablage der Konsole der virtuellen Maschine kopiert wurden

Kopier- und Einfügevorgänge sind für Hosts standardmäßig deaktiviert, um die Offenlegung sensibler Daten durch das Kopieren in die Zwischenablage zu verhindern.

Wenn Kopier- und Einfügevorgänge auf einer virtuellen Maschine aktiviert sind, auf der VMware Tools ausgeführt wird, können Sie Kopier- und Einfügevorgänge zwischen dem Gastbetriebssystem und der Remotekonsole ausführen. Wenn sich das Konsolenfenster im Vordergrund befindet, können auf der virtuellen Maschine ausgeführte Prozesse und nicht berechtigte Benutzer auf die Zwischenablage der VM-Konsole zugreifen. Wenn ein Benutzer vor der Verwendung der Konsole vertrauliche Daten in die Zwischenablage kopiert, macht der Benutzer unter Umständen vertrauliche Daten auf der virtuellen Maschine zugänglich. Um dies zu verhindern, sind Kopier- und Einfügevorgänge für das Gastbetriebssystem standardmäßig deaktiviert.

Bei Bedarf ist es möglich, Kopier- und Einfügevorgänge für virtuelle Maschinen zu aktivieren.

Beschränken der Ausführung von Befehlen durch Benutzer innerhalb einer virtuellen Maschine

Standardmäßig kann ein Benutzer mit der vCenter Server-Administratorrolle mit Dateien und Anwendungen innerhalb des Gastbetriebssystems einer virtuellen Maschine interagieren. Erstellen Sie eine Rolle ohne das Recht **Virtuelle Maschine.Gastvorgänge**, um das Sicherheitsrisiko für die Vertraulichkeit, Verfügbarkeit und Integrität des Gastbetriebssystems zu verringern. Weisen Sie diese Rolle Administratoren zu, die keinen Zugriff auf Dateien virtueller Maschinen benötigen.

Seien Sie beim Zulassen des Zugriffs auf das virtuelle Datencenter aus Sicherheitsgründen so restriktiv wie beim physischen Datencenter. Wenden Sie eine benutzerdefinierte Rolle ohne das Recht **Virtuelle Maschine.Gastvorgänge** auf Benutzer an, die Administratorrechte benötigen, aber nicht berechtigt sind, mit Dateien und Anwendungen des Gastbetriebssystems zu interagieren.

Beispielsweise könnte eine Konfiguration eine virtuelle Maschine in der Infrastruktur mit vertraulichen Daten enthalten.

Wenn Aufgaben wie die vMotion-Migration erfordern, dass Datencenter-Administratoren auf die virtuelle Maschine zugreifen können, deaktivieren Sie einige Remote-Gastbetriebssystemoperationen, um sicherzustellen, dass diese Administratoren nicht auf vertrauliche Informationen zugreifen können.

Voraussetzungen

Stellen Sie sicher, dass Sie im vCenter Server-System, auf dem Sie die Rolle erstellen, über das **Administrator**-Recht verfügen.

Verfahren

1. Melden Sie sich beim vSphere Client als Benutzer mit **Administratorrechten** in dem vCenter Server-System an, in dem Sie die Rolle erstellen möchten.
2. Wählen Sie **Verwaltung** aus und klicken Sie auf **Rollen**.
3. Klicken Sie auf die Administratorrolle und dann auf **Klonen**.
4. Geben Sie einen Namen und eine Beschreibung für die Rolle ein und klicken Sie auf **OK**.

   Geben Sie beispielsweise **`Administrator ohne Gastzugriff`** ein.
5. Wählen Sie die geklonte Rolle aus und klicken Sie auf **Bearbeiten**.
6. Deaktivieren Sie unter dem Recht **Virtuelle Maschine** die Option „Gastvorgänge“.
7. Klicken Sie auf **Speichern**.

Nächste Schritte

Wählen Sie das vCenter Server-System oder den Host aus und weisen Sie eine Berechtigung zu, die den Benutzer bzw. die Gruppe, der/die über die neuen Berechtigungen verfügen soll, mit der neu erstellten Rolle verknüpft. Entfernen Sie diese Benutzer aus der Administratorrolle.

Verhindern, dass ein Benutzer oder Prozess auf einer virtuellen Maschine die Verbindung zu Geräten trennt

Benutzer und Prozesse ohne Root- oder Administratorberechtigungen innerhalb virtueller Maschinen können Geräte verbinden oder trennen, wie z. B. Netzwerkadapter und CD-ROM-Laufwerke, und Geräteeinstellungen ändern. Entfernen Sie diese Geräte, um die Sicherheit der virtuellen Maschinen zu verstärken.

Sie können VM-Benutzer im Gastbetriebssystem sowie auf dem Gastbetriebssystem ausgeführte Prozesse daran hindern, Änderungen an den Geräten vorzunehmen, indem Sie die erweiterten Einstellungen der virtuellen Maschine ändern.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.

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

3 Klicken Sie auf die Registerkarte **Erweiterte Parameter**.

4 Überprüfen Sie den folgenden Parameter oder fügen Sie ihn hinzu.

Name	Wert
isolation.device.connectable.disable	true

Diese Einstellung wirkt sich nicht auf die Fähigkeit eines vSphere-Administrators aus, die mit der virtuellen Maschine verbundenen Geräte zu verbinden oder zu trennen.

5 Klicken Sie auf **OK**.

Verhindern, dass Gastbetriebssystemprozesse Konfigurationsnachrichten an den Host senden

Um sicherzustellen, dass das Gastbetriebssystem keine Konfigurationseinstellungen ändert, können Sie verhindern, dass diese Prozesse Name-Werte-Paare in die Konfigurationsdatei schreiben.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.

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

3 Klicken Sie auf **Erweiterte Parameter**.

4 Überprüfen Sie den folgenden Parameter oder fügen Sie ihn hinzu.

Name	Wert
isolation.tools.setinfo.disable	true

5 Klicken Sie auf **OK**.

Vermeiden der Verwendung unabhängiger, nicht dauerhafter Festplatten mit virtuellen Maschinen

Wenn Sie unabhängige, nicht dauerhafte Festplatten mit virtuellen Maschinen verwenden, können erfolgreiche Angreifer Beweise hinsichtlich der Manipulation der Maschine durch Herunterfahren oder Neustarten des Systems beseitigen. Ohne eine dauerhafte Aufzeichnung der Aktivitäten auf einer virtuellen Maschine registrieren Administratoren einen Angriff

möglicherweise überhaupt nicht. Vermeiden Sie deshalb die Verwendung unabhängiger, nicht dauerhafter Festplatten.

Verfahren

1 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.

2 Falls die Remoteprotokollierung von Ereignissen und Aktivitäten nicht für den Gast konfiguriert ist, sollte für „scsiX:Y.mode“ eine der folgenden Einstellungen verwendet werden:

   - Nicht vorhanden
   - Nicht eingestellt auf unabhängig, nicht dauerhaft

Ergebnisse

Wenn der nicht dauerhafte Modus nicht aktiviert ist, können Sie für eine virtuelle Maschine kein Rollback auf einen bekannten Status ausführen, wenn Sie das System neu starten.

Sichern von virtuellen Maschinen mit Intel Software Guard-Erweiterungen

Mithilfe von vSphere können Sie Virtual Intel® Software Guard Extensions (vSGX) für virtuelle Maschinen konfigurieren. Indem Sie vSGX verwenden, können Sie zusätzliche Sicherheit für Ihre Arbeitslasten bereitstellen.

Einige moderne Intel-CPUs implementieren eine Sicherheitserweiterung namens Intel® Software Guard Extensions (Intel® SGX). Intel SGX ist eine prozessorspezifische Technologie für Anwendungsentwickler, die den ausgewählten Code und die ausgewählten Daten vor Offenlegung oder Änderung schützen möchten. Mit Intel SGX kann Code auf Benutzerebene private Arbeitsspeicherbereiche definieren, die als Enklaven bezeichnet werden. Der Inhalt der Enklave wird so geschützt, dass außerhalb der Enklave ausgeführter Code nicht auf den Inhalt der Enklave zugreifen kann.

vSGX ermöglicht virtuellen Maschinen die Verwendung der Intel SGX-Technologie, sofern diese auf der Hardware verfügbar ist. Um vSGX zu verwenden, muss der ESXi-Host auf einer SGX-fähigen CPU installiert sein, und SGX muss im BIOS des ESXi-Hosts aktiviert sein. Sie können den vSphere Client verwenden, um SGX für eine virtuelle Maschine zu aktivieren.

In vSphere 8.0 und höher können Sie den Remote-Nachweis für eine vSGX-fähige virtuelle Maschine verwenden. Der Intel SGX-Remote-Nachweis ist ein Sicherheitsmechanismus, mit dem Sie einen authentifizierten und sicheren Kommunikationskanal mit einer vertrauenswürdigen Remote-Einheit einrichten können. Zum Verwenden von Remote-Nachweis für virtuelle Maschinen mit SGX-Enklaven ist für Hosts mit einem einzelnen CPU-Socket keine Intel-Registrierung erforderlich. Um den Remote-Nachweis auf einer virtuellen Maschine zu aktivieren,

die auf einem Host mit mehreren CPU-Sockets ausgeführt wird, müssen Sie den Host zuerst beim Intel-Registrierungsserver registrieren. Wenn ein SGX-fähiger Host mit mehreren CPU-Sockets nicht beim Intel-Registrierungsserver registriert ist, können Sie nur vSGX-fähige virtuelle Maschinen einschalten, für die kein Remote-Nachweis erforderlich ist.

Weitere Informationen zum Registrieren eines Multi-Socket-ESXi-Hosts beim Intel-Registrierungsserver finden Sie in der *vCenter Server und Hostverwaltung*-Dokumentation.

Erste Schritte mit vSGX

Virtuelle Maschinen können die Intel SGX-Technologie verwenden, sofern diese auf der Hardware verfügbar ist.

vSphere-Voraussetzungen für vSGX

Zur Verwendung von vSGX muss die vSphere-Umgebung folgende Voraussetzungen erfüllen:

- Anforderungen an virtuelle Maschinen:
  - EFI-Firmware
  - Ab Hardwareversion 17
  - Um den Remote-Nachweis zu aktivieren, verwenden Sie die Hardwareversion 20 oder höher
- Anforderungen an Komponenten:
  - vCenter Server 7.0 und höher
  - ESXi 7.0 und höher
  - Der ESXi-Host muss auf einer SGX-fähigen CPU installiert und SGX muss im BIOS des ESXi-Hosts aktiviert sein.
  - Um den Remote-Nachweis für den Host zu aktivieren, registrieren Sie den Host beim Intel-Registrierungsserver. Auf diese Weise kann die auf dem Host ausgeführte virtuelle Maschine den Remote-Nachweis verwenden. Weitere Informationen über die Registrierung eines Multi-Socket-ESXi finden Sie in der *vCenter Server und Hostverwaltung*-Dokumentation.
- Unterstützung folgender Gastbetriebssysteme:
  - Linux
  - Windows Server 2016 (64 Bit) und höher
  - Windows 10 (64 Bit) und höher

Unterstützte Intel-Hardware für vSGX

Informationen zur unterstützten Intel-Hardware für vSGX finden Sie im vSphere-Kompatibilitätshandbuch unter https://www.vmware.com/resources/compatibility/search.php.

Möglicherweise müssen Sie Hyper-Threading auf bestimmten CPUs ausschalten, um SGX auf dem ESXi-Host zu aktivieren. Weitere Informationen finden Sie im VMware Knowledge Base-Artikel unter https://kb.vmware.com/s/article/71367.

Nicht unterstützte VMware-Funktionen auf vSGX

Die folgenden Funktionen auf einer virtuellen Maschine werden nicht unterstützt, wenn vSGX aktiviert ist:

- vMotion/DRS-Migration
- Anhalten und Fortsetzen einer virtuellen Maschine
- VM-Snapshots (VM-Snapshots werden unterstützt, wenn Sie keinen Snapshot für den Arbeitsspeicher der virtuellen Maschine erstellen.)
- Fault Tolerance
- Gastintegrität (GI, Plattformgrundlage für VMware AppDefense™ 1.0)

Hinweis Diese VMware-Funktionen werden aufgrund der Funktionsweise der Intel SGX-Architektur nicht unterstützt. Diese fehlende Unterstützung ist nicht auf Mängel bei VMware zurückzuführen.

Aktivieren von vSGX auf einer virtuellen Maschine

Sie können vSGX auf einer virtuellen Maschine aktivieren, während Sie eine virtuelle Maschine erstellen.

Voraussetzungen

Weitere Informationen finden Sie unter vSphere-Voraussetzungen für vSGX.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.
3. Klicken Sie mit der rechten Maustaste auf das Objekt, wählen Sie **Neue virtuelle Maschine** aus und befolgen Sie die Anweisungen zum Erstellen einer virtuellen Maschine.
4. Klicken Sie auf der Seite **Hardware anpassen** auf die Registerkarte **Virtuelle Hardware** und erweitern Sie **Sicherheitsgeräte**.
5. Markieren Sie zum Aktivieren von SGX das Kontrollkästchen **Aktivieren**.
6. Geben Sie im Textfeld **Cachegröße der Enclave-Seite (MB)** die Cachegröße in MB ein.

   Hinweis Die Cachegröße der Enclave-Seite muss ein Vielfaches von 2 MB sein.

7 Um zu verhindern, dass die virtuelle Maschine Hosts einschaltet, die den SGX-Remote-Nachweis nicht unterstützen, z. B. nicht registrierte SGX-Hosts mit mehreren Sockets, aktivieren Sie das Kontrollkästchen **Remote-Nachweis**.

8 Wählen Sie im Dropdown-Menü **Steuerungskonfiguration starten** den entsprechenden Modus aus.

Option	Aktion
Entsperrt	Diese Option aktiviert die Enclave-Startkonfiguration des Gastbetriebssystems.
Gesperrt	Mit dieser Option können Sie die Start-Enclave konfigurieren. a Wählen Sie die Option **Öffentlicher Schlüssel-Hash der Start-Enclave** aus. b Zur Verwendung eines der auf dem Host konfigurierten öffentlichen Schlüssel wählen Sie **Von Host verwenden** aus. Wählen Sie anschließend im Dropdown-Menü einen öffentlichen Schlüssel-Hash aus. c Zur manuellen Eingabe des öffentlichen Schlüssels wählen Sie **Manuell eingeben** aus und geben einen gültigen SHA256-Hash-Schlüssel (64 Zeichen) ein.

9 Klicken Sie auf **OK**.

Aktivieren von vSGX auf einer vorhandenen virtuellen Maschine

Sie können vSGX auf einer vorhandenen virtuellen Maschine aktivieren.

Voraussetzungen

Weitere Informationen finden Sie unter vSphere-Voraussetzungen für vSGX.

Verfahren

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

2 Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.

3 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option **Sicherheitsgeräte**.

4 Markieren Sie zum Aktivieren von SGX das Kontrollkästchen **Aktivieren**.

5 Geben Sie im Textfeld **Cachegröße der Enclave-Seite (MB)** die Cachegröße in MB ein.

Hinweis Die Cachegröße der Enclave-Seite muss ein Vielfaches von 2 MB sein.

6 Um zu verhindern, dass die virtuelle Maschine Hosts einschaltet, die den SGX-Remote-Nachweis nicht unterstützen, z. B. nicht registrierte SGX-Hosts mit mehreren Sockets, aktivieren Sie das Kontrollkästchen **Remote-Nachweis**.

7 Wählen Sie im Dropdown-Menü **Steuerungskonfiguration starten** den entsprechenden Modus aus.

Option	Aktion
Entsperrt	Diese Option aktiviert die Enclave-Startkonfiguration des Gastbetriebssystems.
Gesperrt	Mit dieser Option können Sie die Start-Enclave konfigurieren. a Wählen Sie die Option **Öffentlicher Schlüssel-Hash der Start-Enclave** aus. b Zur Verwendung eines der auf dem Host konfigurierten öffentlichen Schlüssel wählen Sie **Von Host verwenden** aus. Wählen Sie anschließend im Dropdown-Menü einen öffentlichen Schlüssel-Hash aus. c Zur manuellen Eingabe des öffentlichen Schlüssels wählen Sie **Manuell eingeben** aus und geben einen gültigen SHA256-Hash-Schlüssel (64 Zeichen) ein.

8 Klicken Sie auf **OK**.

Entfernen von vSGX von einer virtuellen Maschine

Sie können vSGX von einer virtuellen Maschine entfernen.

Verfahren

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

2 Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.

3 Deaktivieren Sie im Dialogfeld **Einstellungen bearbeiten** unter **Sicherheitsgeräte** das Kontrollkästchen **Aktivieren** für SGX.

4 Klicken Sie auf **OK**.

Stellen Sie sicher, dass der vSGX-Eintrag nicht mehr auf der Registerkarte **Übersicht** der virtuellen Maschine im Bereich **VM-Hardware** angezeigt wird.

Sichern von virtuellen Maschinen mit AMD Secure Encrypted Virtualization-Encrypted State

Secure Encrypted Virtualization-Encrypted State (SEV-ES) ist eine in neueren AMD-CPUs aktivierte Hardwarefunktion, mit der der Arbeitsspeicher und das Register des Gastbetriebssystems zustandsverschlüsselt gehalten und gegen Zugriff vom Hypervisor geschützt werden.

Sie können SEV-ES für Ihre virtuellen Maschinen als zusätzliche Sicherheitsfunktion hinzufügen. SEV-ES verhindert, dass CPU-Register Informationen aus Registern an Komponenten wie den Hypervisor weitergeben. SEV-ES kann auch böswillige Änderungen an einem CPU-Registerzustand erkennen.

vSphere und AMD-SEV-ES (Secure Encrypted Virtualization-Encrypted State)

In vSphere 7.0 Update 1 und höher können Sie Secure Encrypted Virtualization-Encrypted State (SEV-ES) auf unterstützten AMD-CPUs und Gastbetriebssystemen aktivieren.

Aktuell unterstützt SEV-ES nur AMD EPYC 7xx2- (Codename „Rome“) und höhere CPUs sowie ausschließlich Versionen von Linux-Kerneln, die spezifische Unterstützung für SEV-ES enthalten.

SEV-ES-Komponenten und -Architektur

Die SEV-ES-Architektur besteht aus den folgenden Komponenten.

- AMD-CPU, insbesondere der speziell der Platform Security Processor (PSP), der Verschlüsselungsschlüssel verwaltet und Verschlüsselung verarbeitet.
- Optimiertes Betriebssystem, d. h., ein Betriebssystem, das vom Gast initiierte Aufrufe an den Hypervisor verwendet.
- Virtual Machine Monitor (VMM) und Virtual Machine Executable (VMX) zum Initialisieren eines verschlüsselten VM-Status beim Einschalten der VM sowie zum Verarbeiten von Aufrufen des Gastbetriebssystems.
- Der VMkernel-Treiber zum Kommunizieren unverschlüsselter Daten zwischen dem Hypervisor und dem Gastbetriebssystem.

Implementieren und Verwalten von SEV-ES auf ESXi

Sie müssen SEV-ES zunächst in der BIOS-Konfiguration eines Systems aktivieren. Weitere Informationen zum Zugriff auf die BIOS-Konfiguration finden Sie in der Dokumentation zu Ihrem System. Nachdem Sie SEV-ES im BIOS für Ihr System aktiviert haben, können Sie SEV-ES zu einer virtuellen Maschine hinzufügen.

Sie verwenden entweder den vSphere Client (vSphere 7.0 Update 2 und höher) oder PowerCLI-Befehle zum Aktivieren und Deaktivieren von SEV-ES auf virtuellen Maschinen. Sie können neue virtuelle Maschinen mit SEV-ES erstellen oder SEV-ES auf vorhandenen virtuellen Maschinen aktivieren. Berechtigungen zum Verwalten virtueller Maschinen, die mit SEV-ES aktiviert sind, entsprechen denjenigen zum Verwalten regulärer VMs.

Nicht unterstützte VMware-Funktionen in SEV-ES

Die folgenden Funktionen werden nicht unterstützt, wenn SEV-ES aktiviert ist.

- Systemverwaltungsmodus
- vMotion
- Eingeschaltete Snapshots (Snapshots ohne Arbeitsspeicher hingegen werden unterstützt)
- CPU oder Arbeitsspeicher im laufenden Betrieb hinzufügen oder entfernen
- Anhalten/fortsetzen
- VMware Fault Tolerance

- Klone und Instant Clones
- Gastintegrität
- UEFI Secure Boot

Hinzufügen von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) zu einer virtuellen Maschine mithilfe des vSphere Client

In vSphere 7.0 Update 2 und höher können Sie SEV-ES mithilfe des vSphere Client zu einer virtuellen Maschine hinzufügen, um verbesserte Sicherheitseinstellungen für das Gastbetriebssystem zur Verfügung zu stellen.

Sie können SEV-ES virtuellen Maschinen unter ESXi 7.0 Update 1 oder höher hinzufügen.

Voraussetzungen

- Das System muss mit einer AMD EPYC 7xx2- (Codename „Rome“) oder höheren CPU und einem unterstützenden BIOS installiert werden.
- SEV-ES muss im BIOS aktiviert sein.
- Die Anzahl der SEV-ES-VMs pro ESXi-Host wird vom BIOS gesteuert. Geben Sie bei Aktivierung von SEV-ES im BIOS einen Wert für die Einstellung **Mindestanzahl SEV-Nicht-ES-ASID** ein, der der Anzahl an virtuellen SEV-ES-Maschinen plus eins entspricht. Wenn beispielsweise 12 virtuelle Maschinen gleichzeitig ausgeführt werden sollen, geben Sie **13** ein.

  Hinweis vSphere 7.0 Update 1 und höher bietet Unterstützung für 16 SEV-ES-fähige VMs pro ESXi-Host. Die Verwendung einer höheren Einstellung im BIOS verhindert nicht, dass SEV-ES funktioniert. Der Grenzwert von 16 gilt jedoch weiterhin. vSphere 7.0 Update 2 und höher bietet Unterstützung für 480 SEV-ES-fähige VMs pro ESXi-Host.
- Die in Ihrer Umgebung ausgeführten ESXi-Hosts müssen ESXi 7.0 Update 1 oder höher aufweisen.
- Der vCenter Server muss unter vSphere 7.0 Update 2 oder höher ausgeführt werden.
- Das Gastbetriebssystem muss SEV-ES unterstützen.

  Aktuell werden nur Linux-Kernel mit spezifischer Unterstützung für SEV-ES unterstützt.
- Die virtuelle Maschine muss die Hardwareversion 18 oder höher aufweisen.
- Für die virtuelle Maschine muss die Option **Gesamten Gastarbeitsspeicher reservieren** aktiviert sein, andernfalls kann die VM nicht eingeschaltet werden.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.

3 Klicken Sie mit der rechten Maustaste auf das Objekt, wählen Sie **Neue virtuelle Maschine** aus und befolgen Sie die Anweisungen zum Erstellen einer virtuellen Maschine.

Option	Aktion
Erstellungstyp auswählen	Erstellen Sie eine virtuelle Maschine.
Namen und Ordner auswählen	Legen Sie einen Namen und einen Zielspeicherort fest.
Computing-Ressource auswählen	Geben Sie ein Objekt an, für das Sie über Rechte zum Erstellen von virtuellen Maschinen verfügen.
Speicher auswählen	Wählen Sie in der VM-Speicherrichtlinie die entsprechende Speicherrichtlinie aus. Wählen Sie einen kompatiblen Datenspeicher aus.
Kompatibilität auswählen	Stellen Sie sicher, dass **ESXi 7.0 und höher** ausgewählt ist.
Gastbetriebssystem auswählen	Wählen Sie Linux und eine Linux-Version mit spezieller Unterstützung für SEV-ES aus.
Hardware anpassen	Stellen Sie unter **VM-Optionen > Startoptionen > Firmware** sicher, dass EFI ausgewählt ist. Wählen Sie unter **VM-Optionen > Verschlüsselung** das Kontrollkästchen **Aktivieren** für AMD SEV-ES aus.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

Ergebnisse

Die virtuelle Maschine wird mit SEV-ES erstellt.

Hinzufügen von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) zu einer virtuellen Maschine mithilfe der Befehlszeile

Sie können die Befehlszeile verwenden, um SEV-ES zu einer virtuellen Maschine hinzuzufügen, um verbesserte Sicherheit für das Gastbetriebssystem bereitzustellen.

Sie können SEV-ES virtuellen Maschinen unter ESXi 7.0 Update 1 oder höher hinzufügen.

Voraussetzungen

- Das System muss mit einer AMD EPYC 7xx2- (Codename „Rome“) oder höheren CPU und einem unterstützenden BIOS installiert werden.
- SEV-ES muss im BIOS aktiviert sein.
- Die Anzahl der SEV-ES-VMs pro ESXi-Host wird vom BIOS gesteuert. Geben Sie bei Aktivierung von SEV-ES im BIOS einen Wert für die Einstellung **Mindestanzahl SEV-Nicht-ES-ASID** ein, der der Anzahl an virtuellen SEV-ES-Maschinen plus eins entspricht. Wenn beispielsweise 12 virtuelle Maschinen gleichzeitig ausgeführt werden sollen, geben Sie **13** ein.

  Hinweis vSphere 7.0 Update 1 und höher bietet Unterstützung für 16 SEV-ES-fähige VMs pro ESXi-Host. Die Verwendung einer höheren Einstellung im BIOS verhindert nicht, dass SEV-ES funktioniert. Der Grenzwert von 16 gilt jedoch weiterhin. vSphere 7.0 Update 2 und höher bietet Unterstützung für 480 SEV-ES-fähige VMs pro ESXi-Host.

- Die in Ihrer Umgebung ausgeführten ESXi-Hosts müssen ESXi 7.0 Update 1 oder höher aufweisen.
- Das Gastbetriebssystem muss SEV-ES unterstützen.

  Aktuell werden nur Linux-Kernel mit spezifischer Unterstützung für SEV-ES unterstützt.
- Die virtuelle Maschine muss die Hardwareversion 18 oder höher aufweisen.
- Für die virtuelle Maschine muss die Option **Gesamten Gastarbeitsspeicher reservieren** aktiviert sein, andernfalls kann die VM nicht eingeschaltet werden.
- PowerCLI 12.1.0 oder höher muss auf einem System mit Zugriff auf Ihre Umgebung installiert sein.

Verfahren

1 Führen Sie in einer PowerCLI-Sitzung das Cmdlet `Connect-VIServer` aus, um als Administrator eine Verbindung mit dem vCenter Server herzustellen, der den ESXi-Host verwaltet, auf dem Sie eine virtuelle Maschine mit SEV-ES hinzufügen möchten.

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

2 Erstellen Sie die virtuelle Maschine mit dem Cmdlet `New-VM` und geben Sie `-SEVEnabled $true` an.

Beispiel: Weisen Sie die Hostinformationen zuerst zu einer Variable zu und erstellen Sie dann die virtuelle Maschine.

```
$vmhost = Get-VMHost -Name 10.193.25.83
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
```

Wenn Sie die Version der virtuelle Hardware angeben müssen, führen Sie das Cmdlet `New-VM` mit dem Parameter `-HardwareVersion vmx-18` aus. Beispiel:

```
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
-HardwareVersion vmx-18
```

Ergebnisse

Die virtuelle Maschine wird mit SEV-ES erstellt.

Aktivieren von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer vorhandenen virtuellen Maschine mithilfe des vSphere Client

In vSphere 7.0 Update 2 und höher können Sie SEV-ES mithilfe des vSphere Client zu einer vorhandenen virtuellen Maschine hinzufügen, um verbesserte Sicherheitseinstellungen für das Gastbetriebssystem zur Verfügung zu stellen.

Sie können SEV-ES virtuellen Maschinen unter ESXi 7.0 Update 1 oder höher hinzufügen.

Voraussetzungen

- Das System muss mit einer AMD EPYC 7xx2- (Codename „Rome“) oder höheren CPU und einem unterstützenden BIOS installiert werden.
- SEV-ES muss im BIOS aktiviert werden.
- Die Anzahl der SEV-ES-VMs pro ESXi-Host wird vom BIOS gesteuert. Geben Sie bei Aktivierung von SEV-ES im BIOS einen Wert für die Einstellung **Mindestanzahl SEV-Nicht-ES-ASID** ein, der der Anzahl an virtuellen SEV-ES-Maschinen plus eins entspricht. Wenn beispielsweise 12 virtuelle Maschinen gleichzeitig ausgeführt werden sollen, geben Sie **13** ein.

  Hinweis vSphere 7.0 Update 1 und höher bietet Unterstützung für 16 SEV-ES-fähige VMs pro ESXi-Host. Die Verwendung einer höheren Einstellung im BIOS verhindert nicht, dass SEV-ES funktioniert. Der Grenzwert von 16 gilt jedoch weiterhin. vSphere 7.0 Update 2 und höher bietet Unterstützung für 480 SEV-ES-fähige VMs pro ESXi-Host.
- Die in Ihrer Umgebung ausgeführten ESXi-Hosts müssen ESXi 7.0 Update 1 oder höher aufweisen.
- Der vCenter Server muss unter vSphere 7.0 Update 2 oder höher ausgeführt werden.
- Das Gastbetriebssystem muss SEV-ES unterstützen.

  Aktuell werden nur Linux-Kernel mit spezifischer Unterstützung für SEV-ES unterstützt.
- Die virtuelle Maschine muss die Hardwareversion 18 oder höher aufweisen.
- Für die virtuelle Maschine muss die Option **Gesamten Gastarbeitsspeicher reservieren** aktiviert sein, andernfalls kann die VM nicht eingeschaltet werden.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.
3. Stellen Sie unter **VM-Optionen > Startoptionen > Firmware** sicher, dass EFI ausgewählt ist.
4. Aktivieren Sie im Dialogfeld **Einstellungen bearbeiten** unter **VM-Optionen > Verschlüsselung** das Kontrollkästchen **Aktivieren** für AMD SEV-ES.
5. Klicken Sie auf **OK**.

Ergebnisse

SEV-ES wird der virtuellen Maschine hinzugefügt.

Aktivieren von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer virtuellen Maschine mithilfe der Befehlszeile

Mithilfe der Befehlszeile können Sie SEV-ES zu einer vorhandenen virtuellen Maschine hinzufügen, um verbesserte Sicherheitseinstellungen für das Gastbetriebssystem zur Verfügung zu stellen.

Sie können SEV-ES virtuellen Maschinen unter ESXi 7.0 Update 1 oder höher hinzufügen.

Voraussetzungen

- Das System muss mit einer AMD EPYC 7xx2- (Codename „Rome“) oder höheren CPU und einem unterstützenden BIOS installiert werden.
- SEV-ES muss im BIOS aktiviert werden.
- Die Anzahl der SEV-ES-VMs pro ESXi-Host wird vom BIOS gesteuert. Geben Sie bei Aktivierung von SEV-ES im BIOS einen Wert für die Einstellung **Mindestanzahl SEV-Nicht-ES-ASID** ein, der der Anzahl an virtuellen SEV-ES-Maschinen plus eins entspricht. Wenn beispielsweise 12 virtuelle Maschinen gleichzeitig ausgeführt werden sollen, geben Sie **13** ein.

  Hinweis vSphere 7.0 Update 1 und höher bietet Unterstützung für 16 SEV-ES-fähige VMs pro ESXi-Host. Die Verwendung einer höheren Einstellung im BIOS verhindert nicht, dass SEV-ES funktioniert. Der Grenzwert von 16 gilt jedoch weiterhin. vSphere 7.0 Update 2 und höher bietet Unterstützung für 480 SEV-ES-fähige VMs pro ESXi-Host.
- Die in Ihrer Umgebung ausgeführten ESXi-Hosts müssen ESXi 7.0 Update 1 oder höher aufweisen.
- Das Gastbetriebssystem muss SEV-ES unterstützen.

  Aktuell werden nur Linux-Kernel mit spezifischer Unterstützung für SEV-ES unterstützt.
- Die virtuelle Maschine muss die Hardwareversion 18 oder höher aufweisen.
- Für die virtuelle Maschine muss die Option **Gesamten Gastarbeitsspeicher reservieren** aktiviert sein, andernfalls kann die VM nicht eingeschaltet werden.
- PowerCLI 12.1.0 oder höher muss auf einem System mit Zugriff auf Ihre Umgebung installiert sein.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

Verfahren

1 Führen Sie in einer PowerCLI-Sitzung das Cmdlet `Connect-VIServer` aus, um als Administrator eine Verbindung mit dem vCenter Server herzustellen, der den ESXi-Host mit der virtuellen Maschine verwaltet, der SEV-ES hinzugefügt werden soll.

  Beispiel:

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

2 Aktivieren Sie SEV-ES auf der virtuellen Maschine mit dem Cmdlet `Set-VM` und geben Sie `-SEVEnabled $true` an.

Beispiel:

```
$vmhost = Get-VMHost -Name 10.193.25.83
Set-VM -Name MyVM2 $vmhost -SEVEnabled $true
```

Wenn Sie die Version der virtuelle Hardware angeben müssen, führen Sie das Cmdlet `Set-VM` mit dem Parameter `-HardwareVersion vmx-18` aus. Beispiel:

```
Set-VM -Name MyVM2 $vmhost -SEVEnabled $true -HardwareVersion vmx-18
```

Ergebnisse

SEV-ES wird der virtuellen Maschine hinzugefügt.

Deaktivieren von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer virtuellen Maschine mithilfe des vSphere Client

In vSphere 7.0 Update 2 und höher können Sie den vSphere Client zum Deaktivieren von SEV-ES auf einer virtuellen Maschine verwenden.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

Verfahren

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

2 Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.

3 Deaktivieren Sie im Dialogfeld **Einstellungen bearbeiten** unter **VM-Optionen > Verschlüsselung** das Kontrollkästchen **Aktivieren** für AMD SEV-ES.

4 Klicken Sie auf **OK**.

Ergebnisse

SEV-ES ist auf der virtuellen Maschine deaktiviert.

Deaktivieren von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer virtuellen Maschine mithilfe der Befehlszeile

Sie können die Befehlszeile zum Deaktivieren von SEV-ES auf einer virtuellen Maschine verwenden.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- PowerCLI 12.1.0 oder höher muss auf einem System mit Zugriff auf Ihre Umgebung installiert sein.

Verfahren

1. Führen Sie in einer PowerCLI-Sitzung das Cmdlet `Connect-VIServer` aus, um als Administrator eine Verbindung mit dem vCenter Server herzustellen, der den ESXi-Host mit der virtuellen Maschine verwaltet, von der SEV-ES entfernt werden soll.

   Beispiel:

   ```
   Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
   ```

2. Deaktivieren Sie SEV-ES auf der virtuellen Maschine mit dem `Set-VM`-Cmdlet und geben Sie `-SEVEnabled $false` an.

   Beispiel: Weisen Sie die Hostinformationen zuerst einer Variablen zu und deaktivieren Sie SEV-ES dann für die virtuelle Maschine.

   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $false
   ```

Ergebnisse

SEV-ES ist auf der virtuellen Maschine deaktiviert.

Verschlüsselung virtueller Maschinen

6

Mit der vSphere-VM-Verschlüsselung können Sie vertrauliche Arbeitslasten noch sicherer verschlüsseln. Der Zugriff auf Verschlüsselungsschlüssel kann davon abhängig gemacht werden, ob sich der ESXi-Host in einem vertrauenswürdigen Zustand befindet.

Bevor Sie mit den Verschlüsselungsaufgaben für virtuelle Maschinen beginnen können, müssen Sie einen Schlüsselanbieter einrichten. Die folgenden Schlüsselanbietertypen sind verfügbar.

Tabelle 6-1. vSphere-Schlüsselanbieter

Schlüsselanbieter	Beschreibung	Für weitere Informationen.
Standardschlüsselanbieter	Der Standardschlüsselanbieter ist in vSphere 6.5 und höher verfügbar und verwendet vCenter Server, um Schlüssel von einem externen Schlüsselserver anzufordern. Der Schlüsselserver generiert und speichert die Schlüssel und leitet sie an vCenter Server zur Verteilung weiter.	Weitere Informationen hierzu finden Sie unter Kapitel 7 Konfigurieren und Verwalten eines Standardschlüsselanbieters.
Vertrauenswürdiger Schlüsselanbieter	Der in vSphere 7.0 und höher verfügbare vertrauenswürdige vSphere Trust Authority-Schlüsselanbieter ermöglicht den Zugriff auf die Verschlüsselungsschlüssel abhängig vom Bestätigungsstatus eines Arbeitslastclusters. Für vSphere Trust Authority ist ein externer Schlüsselserver erforderlich.	Weitere Informationen hierzu finden Sie unter Kapitel 9 vSphere Trust Authority.
VMware vSphere® Nativer Schlüsselanbieter™	vSphere Native Key Provider ist ab vSphere 7.0 Update 2 verfügbar und in allen vSphere-Editionen enthalten. Dafür ist kein externer Schlüsselserver erforderlich.	Weitere Informationen hierzu finden Sie unter Kapitel 8 Konfigurieren und Verwalten eines vSphere Native Key Providers.

Lesen Sie als Nächstes die folgenden Themen:

- Vergleich von vSphere-Schlüsselanbietern
- Wie vSphere Virtual Machine Encryption Ihre Umgebung schützt

- vSphere Virtual Machine Encryption-Komponenten
- Prozessablauf bei der Verschlüsselung
- Verschlüsseln von virtuellen Festplatten
- Fehler bei der Verschlüsselung von virtuellen Maschinen
- Voraussetzungen und erforderliche Berechtigungen für VM-Verschlüsselungsaufgaben
- Was ist verschlüsseltes vSphere vMotion
- Virtuelle Maschine – Empfohlene Vorgehensweisen für die Verschlüsselung
- Vorbehalte bei der Verschlüsselung von virtuellen Maschinen
- Interoperabilität bei der Verschlüsselung von virtuellen Maschinen
- vSphere-Schlüsselpersistenz auf ESXi-Hosts

Vergleich von vSphere-Schlüsselanbietern

Mithilfe einer allgemeinen Übersicht über die Funktionen der vSphere-Schlüsselanbieter können Sie Ihre Verschlüsselungsstrategie planen.

Im Allgemeinen gibt es im Regelbetrieb der einzelnen Schlüsselanbieter nur geringe Unterschiede bei den unterstützten Funktionen und Produkten. Trotz des ähnlichen Aussehens und Verhaltens der verschiedenen Schlüsselanbieter müssen bei der Auswahl eines Schlüsselanbieters unter Umständen Anforderungen und Bestimmungen berücksichtigt werden. Diese werden in der folgenden Tabelle dargestellt:

Tabelle 6-2. Überlegungen zu Schlüsselanbietern

Schlüsselanbieter	Externer Schlüsselserver erforderlich?	Schnelle Einrichtung?	Funktioniert nur mit vSphere?	Verschlüsselungsschlüssel dauerhaft auf dem Host gespeichert?	Erneute Schlüsselerstellung beim Klonen?
Standardschlüsselanbieter	Ja	Nein	Nein	Nein	Ja
Vertrauenswürdiger Schlüsselanbieter	Ja	Nein	Nein	Nein	Ja
vSphere Native Key Provider	Nein	Ja	Ja	Ja	Ja

Hinweis Beim Start des Hosts schreibt vSphere Native Key Provider immer den Verschlüsselungsschlüssel auf die ESXi-Hosts im Cluster. Wenn Sie Bedenken über die physische Sicherheit des Clusters haben, sollten Sie entweder einen Standardschlüsselanbieter oder einen vertrauenswürdigen Schlüsselanbieter verwenden. Beides erfordert, dass der Schlüsselserver für verschlüsselte virtuelle Maschinen verfügbar ist.

Schlüsselanbieter-Verschlüsselungsfunktionen

Die folgenden Verschlüsselungsfunktionen werden von jedem Schlüsselanbietertyp unterstützt.

- Erneute Schlüsselerstellung mithilfe desselben oder eines anderen Schlüsselanbieters
- Schlüssel rotieren
- Virtuelles Trusted Platform Module (vTPM)
- Festplattenverschlüsselung
- Verschlüsselung virtueller vSphere-Maschinen
- Koexistenz mit anderen Schlüsselanbietern
- Upgrade auf einen anderen Schlüsselanbieter

Unterstützung von Schlüsselanbietern für vSphere-Funktionen

Im Folgenden wird die Unterstützung der Schlüsselanbieter für bestimmte wichtige vSphere-Funktionen beschrieben.

- Verschlüsselte vSphere vMotion: Wird von allen Schlüsselanbietertypen unterstützt. Derselbe Schlüsselanbieter muss auf dem Zielhost verfügbar sein. Weitere Informationen hierzu finden Sie unter Was ist verschlüsseltes vSphere vMotion.
- Dateibasierte Sicherung und Wiederherstellung in vCenter Server: Standardschlüsselanbieter und vSphere Native Key Provider unterstützen dateibasierte Sicherung und Wiederherstellung in vCenter Server. Da die meisten vSphere Trust Authority-Konfigurationsinformationen auf den ESXi-Hosts gespeichert werden, erfolgt keine Sicherung dieser Informationen durch den dateibasierten Sicherungsmechanismus in vCenter Server. Um sicherzustellen, dass die Konfigurationsinformationen für Ihre vSphere Trust Authority-Bereitstellung gespeichert werden, finden Sie Informationen unter Sichern der vSphere Trust Authority-Konfiguration.

Unterstützung von Schlüsselanbietern für VMware-Produkte

In der folgenden Tabelle wird die Schlüsselanbieterunterstützung für bestimmte VMware-Produkte verglichen.

Tabelle 6-3. Vergleich der Unterstützung für VMware-Produkte

Schlüsselanbieter	Verschlüsselung ruhender vSAN-Daten	Site Recovery Manager	vSphere Replication
Standardschlüsselanbieter	Ja	Ja	Ja
Vertrauenswürdiger Schlüsselanbieter	Nein	Ja Wenn dieselbe Konfiguration der vSphere Trust Authority-Dienste auf der Wiederherstellungsseite verfügbar ist, wird SRM mit Array-basierter Replizierung unterstützt.	Nein
vSphere Native Key Provider	Ja	Ja	Ja

Hinweis Standardschlüsselanbieter, vertrauenswürdiger Schlüsselanbieter und vSphere Native Key Provider unterstützen zusätzlich zu vSAN die vSphere VM-Verschlüsselung.

Erforderliche Hardware für Schlüsselanbieter

In der folgenden Tabelle werden bestimmte Mindestanforderungen an die Hardware des Schlüsselanbieters verglichen.

Tabelle 6-4. Vergleich der erforderlichen Hardware für Schlüsselanbieter

Schlüsselanbieter	TPM auf ESXi-Host
Standardschlüsselanbieter	Nicht erforderlich
Vertrauenswürdiger Schlüsselanbieter	Erforderlich auf vertrauenswürdigen Hosts (Hosts im vertrauenswürdigen Cluster). **Hinweis** Aktuell benötigen die ESXi-Hosts im Trust Authority-Cluster kein TPM. Es empfiehlt sich jedoch, neue ESXi-Hosts mit TPMs zu installieren.
vSphere Native Key Provider	Nicht erforderlich Die Verfügbarkeit des vSphere Native Key Providers kann optional auf Hosts mit einem TPM beschränkt werden.

Benennung des Schlüsselanbieters

vSphere verwendet den Schlüsselanbieternamen, um einen Schlüsselbezeichner zu suchen. Wenn zwei Schlüsselanbieter denselben Namen haben, geht vSphere davon aus, dass sie äquivalent sind und Zugriff auf dieselben Schlüssel haben. Jeder logische Schlüsselanbieter muss unabhängig von seinem Typ (Standard-, vertrauenswürdiger und nativer Schlüsselanbieter) über einen eindeutigen Namen in allen vCenter Server-Systemen verfügen.

In einigen Fällen konfigurieren Sie denselben Schlüsselanbieter über mehrere vCenter Server-Systeme hinweg, z. B. den folgenden:

- Migrieren verschlüsselter virtueller Maschinen zwischen vCenter Server-Systemen
- Einrichten eines vCenter Servers als Notfallwiederherstellungsort

Wie vSphere Virtual Machine Encryption Ihre Umgebung schützt

Unabhängig davon, welchen Schlüsselanbieter Sie verwenden, können Sie mit vSphere Virtual Machine Encryption verschlüsselte virtuelle Maschinen erstellen und vorhandene virtuelle Maschinen verschlüsseln. Da alle Dateien der virtuellen Maschine, die vertrauliche Informationen enthalten, verschlüsselt werden, ist die virtuelle Maschine geschützt. Nur Administratoren mit Berechtigungen zum Verschlüsseln können Verschlüsselungs- und Entschlüsselungsaufgaben durchführen.

Wichtig ESXi Shell-Benutzer verfügen auch über Berechtigungen für kryptografische Vorgänge. Weitere Informationen finden Sie unter Voraussetzungen und erforderliche Berechtigungen für VM-Verschlüsselungsaufgaben.

Welcher Speicher wird von vSphere Virtual Machine Encryption unterstützt

vSphere Virtual Machine Encryption funktioniert mit allen unterstützten Speichertypen (NFS, iSCSI, Fibre Channel, direkt angeschlossener Speicher usw.), einschließlich VMware vSAN. Weitere Informationen zur Verwendung von Verschlüsselung auf einem vSAN-Cluster finden Sie in der *Verwalten von VMware vSAN*-Dokumentation.

vSphere Virtual Machine Encryption und vSAN verwenden dieselben Verschlüsselungsbibliotheken, aber unterschiedliche Profile. Bei der VM-Verschlüsselung handelt es sich um eine Verschlüsselung pro VM, während es sich bei vSAN um eine Verschlüsselung auf Datenspeicherebene handelt.

vSphere-Verschlüsselungsschlüssel und -Schlüsselanbieter

vSphere verwendet zwei Verschlüsselungsebenen in Form eines Schlüsselverschlüsselungsschlüssels (Key Encryption Key, KEK) und eines Datenverschlüsselungsschlüssels (Data Encryption Key, DEK). Kurz gesagt erzeugt ein ESXi-Host einen DEK, um virtuelle Maschinen und Festplatten zu verschlüsseln. Der KEK wird von einem Schlüsselserver bereitgestellt und zur Verschlüsselung (oder „Packung“) des DEK verwendet. Der KEK verschlüsselt den DEK mit dem AES256-Algorithmus und der DEK verschlüsselt die VMDK mit dem XTS-AES-256-Algorithmus (Schlüsselgröße 512 Bit). Je nach Typ des Schlüsselanbieters werden verschiedene Methoden zum Erstellen und Verwalten des DEK und KEK verwendet.

Der Standardschlüsselanbieter funktioniert wie folgt.

1 Der ESXi-Host generiert und verwendet interne Schlüssel zum Verschlüsseln von virtuellen Maschinen und Festplatten. Diese Schlüssel werden als DEKs verwendet.

2 vCenter Server fordert Schlüssel aus dem Schlüsselserver (KMS) an. Diese Schlüssel werden als KEKs verwendet. vCenter Server speichert nur die ID jedes KEK, nicht jedoch den Schlüssel selbst.

3 ESXi verwendet den KEK zum Verschlüsseln der internen Schlüssel und speichert den verschlüsselten internen Schlüssel auf der Festplatte. ESXi speichert den KEK nicht auf der Festplatte. Wenn ein Host neu gestartet wird, fordert vCenter Server den KEK mit der entsprechenden ID beim Schlüsselserver an und macht ihn für ESXi verfügbar. ESXi kann dann die internen Schlüssel nach Bedarf entschlüsseln.

Der vertrauenswürdige vSphere Trust Authority-Schlüsselanbieter funktioniert folgendermaßen.

1 Der vCenter Server des vertrauenswürdigen Clusters überprüft, ob der ESXi-Host, auf dem die verschlüsselte virtuelle Maschine erstellt werden soll, auf den standardmäßigen vertrauenswürdigen Schlüsselanbieter zugreifen kann.

2 Der vCenter Server des vertrauenswürdigen Clusters fügt dem vertrauenswürdigen Schlüsselanbieter die Konfigurationsspezifikation der virtuellen Maschine hinzu.

3 Die Anforderung zum Erstellen der virtuellen Maschine wird an den ESXi-Host gesendet.

4 Wenn dem ESXi-Host noch kein Bestätigungstoken zur Verfügung steht, wird ein Token beim Bestätigungsdienst angefordert.

5 Der Schlüsselanbieterdienst validiert das Bestätigungstoken und erstellt einen KEK, der an den ESXi-Host gesendet werden soll. Der KEK wird mit dem auf dem Schlüsselanbieter konfigurierten primären Schlüssel verschlüsselt. Sowohl der verschlüsselte KEK-Text als auch der KEK-Klartext werden an den vertrauenswürdigen Host zurückgegeben.

6 Der ESXi-Host erzeugt einen DEK, um die Festplatten der virtuellen Maschine zu verschlüsseln.

7 Der KEK wird zum Verschlüsseln des vom ESXi-Host generierten DEK verwendet und der Verschlüsselungstext des Schlüsselanbieters wird mit den verschlüsselten Daten gespeichert.

8 Die virtuelle Maschine wird verschlüsselt und in den Speicher geschrieben.

Hinweis Die ESXi-Hosts in vSphere-Clustern enthalten den KEK für verschlüsselte virtuelle Maschinen im Hostarbeitsspeicher, um Verfügbarkeitsfunktionen wie Hochverfügbarkeit, vMotion, DRS usw. zu ermöglichen. Wenn eine virtuelle Maschine gelöscht oder die Registrierung einer virtuellen Maschine aufgehoben wird, löschen die ESXi-Hosts im Cluster den KEK aus ihrem Arbeitsspeicher. Somit kann der ESXi-Host den KEK nicht mehr verwenden. Dieses Verhalten ist für Standardschlüsselanbieter und vertrauenswürdige Schlüsselanbieter identisch.

Der vSphere Native Key Provider funktioniert folgendermaßen.

1 Wenn Sie den Schlüsselanbieter erstellen, generiert vCenter Server einen primären Schlüssel und über gibt ihn an die ESXi-Hosts im Cluster weiter. (Es ist kein externer Schlüsselserver beteiligt.)

2 Die ESXi-Hosts erzeugen bei Bedarf einen DEK.

3 Wenn Sie eine Verschlüsselungsaktivität durchführen, werden die Daten mit dem DEK verschlüsselt.

   Verschlüsselte DEKs werden neben den verschlüsselten Daten gespeichert.

4 Wenn Sie Daten entschlüsseln, wird der primäre Schlüssel verwendet, um den DEK und dann die Daten zu entschlüsseln.

Welche Komponenten werden von vSphere Virtual Machine Encryption verschlüsselt

vSphere Virtual Machine Encryption unterstützt die Verschlüsselung von Dateien der virtuellen Maschine, von virtuellen Festplattendateien und von Core-Dump-Dateien.

Dateien der virtuellen Maschine

Die meisten Dateien der virtuellen Maschine werden verschlüsselt, insbesondere Gastdaten, die nicht in der VMDK-Datei gespeichert werden. Zu diesen Dateien gehören unter anderen die NVRAM-, VSWP- und VMSN-Dateien. Der Schlüssel vom Schlüsselanbieter entsperrt ein verschlüsseltes Paket in der VMX-Datei, die interne Schlüssel und andere Geheimschlüssel enthält. Der Schlüsselabruf funktioniert je nach Schlüsselanbieter wie folgt:

- Standardschlüsselanbieter: vCenter Server verwaltet die Schlüssel vom Schlüsselserver und ESXi-Hosts können nicht direkt auf den Schlüsselanbieter zugreifen. Die Hosts warten, bis vCenter Server die Schlüssel überträgt.
- Vertrauenswürdiger Schlüsselanbieter und vSphere Native Key Provider: Die ESXi-Hosts greifen direkt auf die Schlüsselanbieter zu und rufen die angeforderten Schlüssel entweder direkt vom vSphere Trust Authority-Dienst oder vom vSphere Native Key Provider ab.

Wenn Sie den vSphere Client zum Erstellen einer verschlüsselten virtuellen Maschine verwenden, können Sie virtuelle Festplatten getrennt von VM-Dateien verschlüsseln und entschlüsseln. Alle virtuellen Festplatten sind standardmäßig verschlüsselt. Für andere Verschlüsselungsaufgaben wie das Verschlüsseln einer vorhandenen virtuellen Maschine können Sie virtuelle Festplatten getrennt von Dateien der virtuellen Maschine verschlüsseln und entschlüsseln.

Hinweis Eine verschlüsselte virtuelle Festplatte kann nicht einer unverschlüsselten virtuellen Maschine zugeordnet werden.

Virtuelle Festplattendateien

Daten in einer Datei einer verschlüsselten virtuellen Festplatte (VMDK-Datei) werden nie in Klartext in den Speicher oder auf eine physische Festplatte geschrieben und nie in Klartext über das Netzwerk übertragen. Die VMDK-Deskriptordatei besteht zum größten Teil aus Klartext, enthält jedoch eine Schlüssel-ID für den KEK und den internen Schlüssel (DEK) im verschlüsselten Paket.

Sie können den vSphere Client oder die vSphere-API verwenden, um einen flachen Neuverschlüsselungsvorgang mit einem neuen KEK durchzuführen, oder mithilfe der vSphere-API einen tiefen Neuverschlüsselungsvorgang mit einem neuen internen Schlüssel durchzuführen.

Core-Dumps

Core-Dumps auf einem ESXi-Host, auf dem der Verschlüsselungsmodus aktiviert ist, werden immer verschlüsselt. Weitere Informationen hierzu finden Sie unter vSphere VM-Verschlüsselung und Core-Dumps. Core-Dumps auf dem vCenter Server-System werden nicht verschlüsselt. Schützen Sie den Zugriff auf das vCenter Server-System.

Auslagerungsdatei der virtuellen Maschine

Die Auslagerungsdatei der virtuellen Maschine wird jedes Mal verschlüsselt, wenn Sie ein vTPM zu einer virtuellen Maschine hinzufügen. In Umgebungen mit wenig RAM kann es zu verschlüsselungsbezogenen Auslagerungen mit Auswirkungen auf die Leistung kommen.

vTPMs

Wenn Sie ein vTPM konfigurieren, werden die Dateien der virtuellen Maschine verschlüsselt, die Festplatten hingegen nicht. Sie haben die Möglichkeit, Verschlüsselung für die virtuelle Maschine und die zugehörigen Festplatten explizit hinzuzufügen. Weitere Informationen finden Sie unter Kapitel 11 Sichern von virtuellen Maschinen mit Virtual Trusted Platform Module.

Hinweis Informationen zu Einschränkungen bezüglich Geräten und Funktionen, mit denen vSphere Virtual Machine Encryption interagieren kann, finden Sie unter Interoperabilität bei der Verschlüsselung von virtuellen Maschinen.

Welche Komponenten werden von vSphere Virtual Machine Encryption nicht verschlüsselt

Einige der Dateien, die einer virtuellen Maschine zugeordnet sind, werden nicht oder teilweise verschlüsselt.

Protokolldateien

Protokolldateien werden nicht verschlüsselt, da sie keine vertraulichen Daten enthalten.

Konfigurationsdateien der virtuellen Maschine

Die meisten Informationen zur Konfiguration der virtuellen Maschine (gespeichert in den VMX- und VMSD-Dateien) werden nicht verschlüsselt.

Deskriptordatei der virtuellen Festplatte

Zur Unterstützung der Festplattenverwaltung ohne Schlüssel werden die meisten Deskriptordateien der virtuellen Festplatte nicht verschlüsselt.

Erforderliche Rechte für die Durchführung von Kryptografievorgängen

Nur Benutzer die über Berechtigungen für **Kryptografische Vorgänge** verfügen, können kryptografische Vorgänge durchführen. Die Berechtigungen sind fein unterteilt. Die standardmäßige Systemrolle „Administrator“ umfasst alle Berechtigungen für **Kryptografische Vorgänge**. Die Rolle, „Kein Kryptografie-Administrator“ unterstützt alle Administratorberechtigungen mit Ausnahme der Berechtigungen für **Kryptografievorgänge**.

Zusätzlich zur Verwendung der **Cryptographer.***-Berechtigungen kann vSphere Native Key Provider die Berechtigung **Cryptographer.ReadKeyServersInfo** verwenden, die spezifisch für vSphere Native Key Providers ist.

Weitere Informationen hierzu finden Sie unter Rechte für Verschlüsselungsvorgänge.

Sie können zusätzliche benutzerdefinierte Rollen erstellen, um beispielsweise zuzulassen, dass eine Gruppe von Benutzern virtuelle Maschinen verschlüsselt, zugleich aber zu verhindern, dass diese Benutzer virtuelle Maschinen entschlüsseln.

Wie führen Sie kryptografische Vorgänge durch

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

Tabelle 6-5. Schnittstellen für das Durchführen von kryptografischen Vorgängen

Schnittstelle	Vorgänge	Informationen
vSphere Client	Erstellen einer verschlüsselten virtuellen Maschine Verschlüsseln und Entschlüsseln virtueller Maschinen Durchführen einer flachen Neuverschlüsselung einer virtuellen Maschine (Verwendung eines anderen KEK)	Dieses Handbuch
PowerCLI	Erstellen einer verschlüsselten virtuellen Maschine Verschlüsseln und Entschlüsseln virtueller Maschinen Konfigurieren von vSphere Trust Authority	*Referenz zu VMware PowerCLI-Cmdlets*

Tabelle 6-5. Schnittstellen für das Durchführen von kryptografischen Vorgängen (Fortsetzung)

Schnittstelle	Vorgänge	Informationen
vSphere Web Services SDK	Erstellen einer verschlüsselten virtuellen Maschine Verschlüsseln und Entschlüsseln virtueller Maschinen Durchführen einer tiefen Neuverschlüsselung einer virtuellen Maschine (Verwendung eines anderen DEK) Durchführen einer flachen Neuverschlüsselung einer virtuellen Maschine (Verwendung eines anderen KEK)	*Programmierhandbuch zum vSphere Web Services SDK* *vSphere Web Services-API-Referenz*
`crypto-util`	Entschlüsseln verschlüsselter Core-Dumps Prüfen, ob Dateien verschlüsselt sind Führen Sie andere Verwaltungsaufgaben direkt auf dem ESXi-Host durch.	Befehlszeilenhilfe vSphere VM-Verschlüsselung und Core-Dumps

Vorgehensweise zum Neuverschlüsseln (erneute Schlüsselerstellung) einer verschlüsselten virtuellen Maschine

Sie können eine virtuelle Maschine mit neuen Schlüsseln neu verschlüsseln (auch als „rekey“ bezeichnet), z. B. für den Fall, dass ein Schlüssel abläuft oder manipuliert wird. Die folgenden Optionen für die erneute Schlüsselerstellung sind verfügbar.

- Eine flache Neuverschlüsselung, bei der nur der Schlüsselverschlüsselungsschlüssel (Key Encryption Key, KEK) ersetzt wird
- Eine tiefe Neuverschlüsselung, bei der sowohl der Festplattenverschlüsselungsschlüssel (DEK, Disk Encryption Key) als auch der KEK ersetzt wird

Bei einer tiefen Neuverschlüsselung muss die virtuelle Maschine ausgeschaltet sein und darf keine Snapshots enthalten. Sie können eine flache Neuverschlüsselung bei eingeschalteter virtueller Maschine durchführen, sofern auf der virtuellen Maschine Snapshots vorhanden sind. Die flache Neuverschlüsselung einer verschlüsselten virtuellen Maschine mit Snapshots ist nur in einem einzelnen Snapshot-Zweig (Festplattenkette) zulässig. Mehrere Snapshot-Zweige werden nicht unterstützt. Darüber hinaus wird eine flache Neuverschlüsselung auf einem verknüpften Klon einer virtuellen Maschine oder Festplatte nicht unterstützt. Wenn die flache Neuverschlüsselung fehlschlägt, bevor alle Verknüpfungen in der Kette mit dem neuen KEK aktualisiert werden, können Sie weiterhin auf die verschlüsselte virtuelle Maschine zugreifen, vorausgesetzt, Sie verfügen über die alten und neuen KEKs. Es erweist sich jedoch am sinnvollsten, die flache Neuverschlüsselung vor dem Durchführen von Snapshot-Vorgängen erneut auszuführen.

Sie können die erneute Schlüsselerstellung für eine virtuelle Maschine mithilfe von vSphere Client, der CLI oder der API durchführen. Weitere Informationen finden Sie unter Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe des vSphere Client, Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe der CLI und *Programmierhandbuch zum vSphere Web Services SDK*.

vSphere Virtual Machine Encryption-Komponenten

Je nachdem, welchen Schlüsselanbieter Sie verwenden, tragen ein externer Schlüsselserver, das vCenter Server-System und Ihre ESXi-Hosts potenziell zur Verschlüsselungslösung bei.

Die folgenden Komponenten umfassen vSphere Virtual Machine Encryption:

- Einen externen Schlüsselserver, auch als KMS bezeichnet (für vSphere Native Key Provider nicht erforderlich)
- vCenter Server
- ESXi-Hosts

Welche Rolle spielt ein Schlüsselserver bei der vSphere Virtual Machine Encryption?

Der Schlüsselserver ist ein KMIP-Verwaltungsserver (Key Management Interoperability Protocol), der einem Schlüsselanbieter zugeordnet ist. Ein Standardschlüsselanbieter und ein vertrauenswürdiger Schlüsselanbieter benötigen einen Schlüsselserver. vSphere Native Key Provider benötigt keinen Schlüsselserver. In der folgenden Tabelle werden die Unterschiede bei der Schlüsselanbieter- und Schlüsselserverinteraktion beschrieben.

Tabelle 6-6. Interaktion zwischen Schlüsselanbietern und Schlüsselservern

Schlüsselanbieter	Interaktion mit Schlüsselservern
Standardschlüsselanbieter	Ein Standardschlüsselanbieter verwendet vCenter Server zum Anfordern von Schlüsseln von einem Schlüsselserver. Der Schlüsselserver generiert und speichert die Schlüssel und leitet sie zur Verteilung an die ESXi-Hosts an vCenter Server weiter.
Vertrauenswürdiger Schlüsselanbieter	Ein vertrauenswürdiger Schlüsselanbieter verwendet einen Schlüsselanbieterdienst, mit dem die vertrauenswürdigen ESXi die Schlüssel direkt abrufen können. Weitere Informationen hierzu finden Sie unter Was ist der vSphere Trust Authority-Schlüsselanbieterdienst?.
vSphere Native Key Provider	vSphere Native Key Provider benötigt keinen Schlüsselserver. vCenter Server Generiert einen primären Schlüssel und über leitet ihn an die ESXi-Hosts weiter. Daraufhin generieren die ESXi-Hosts dann Datenverschlüsselungsschlüssel (auch wenn sie nicht mit dem vCenter Server verbunden sind). Weitere Informationen hierzu finden Sie unter vSphere Native Key Provider – Übersicht.

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

Wenn in Ihrer Umgebung verschiedene Schlüsselserveranbieter in unterschiedlichen Umgebungen verwendet werden, können Sie einen Schlüsselanbieter für jeden Schlüsselserver hinzufügen und einen Standardschlüsselanbieter angeben. Der erste hinzugefügte Schlüsselanbieter fungiert als Standardschlüsselanbieter. Sie können den Standardcluster auch zu einem späteren Zeitpunkt explizit festlegen.

Als KMIP-Client verwendet vCenter Server das KMIP (Key Management Interoperability Protocol), um eine problemlose Verwendung des Schlüsselservers Ihrer Wahl zu gewährleisten.

Welche Rolle spielt vCenter Server in vSphere Virtual Machine Encryption?

In der folgenden Tabelle wird die Rolle von vCenter Server beim Verschlüsselungsprozess beschrieben.

Tabelle 6-7. Schlüsselanbieter und vCenter Server

Schlüsselanbieter	Rolle von vCenter Server	Wie werden die Rechte überprüft?
Standardschlüsselanbieter	Nur vCenter Server verfügt über die Anmeldedaten für die Anmeldung beim Schlüsselserver. Ihre ESXi-Hosts verfügen nicht über diese Anmeldedaten. vCenter Server ruft Schlüssel vom Schlüsselserver ab und pusht diese an die ESXi-Hosts. Der vCenter Server speichert keine Schlüsselserver-Schlüssel, sondern nur eine Liste mit Schlüssel-IDs.	vCenter Server überprüft die Berechtigungen der Benutzer, die Kryptografie-Vorgänge durchführen.
Vertrauenswürdiger Schlüsselanbieter	Mit vSphere Trust Authority muss vCenter Server nicht länger Schlüssel vom Schlüsselserver anfordern und der Zugriff auf die Verschlüsselungsschlüssel wird somit abhängig vom Bestätigungszustand eines Arbeitslastclusters. Sie müssen getrennte vCenter Server-Systeme für den vertrauenswürdigen Cluster und den Trust Authority Cluster verwenden.	vCenter Server überprüft die Berechtigungen der Benutzer, die Kryptografie-Vorgänge durchführen. Nur Benutzer, die Mitglieder der TrustedAdmins SSO-Gruppe sind, können Verwaltungsvorgänge durchführen.
vSphere Native Key Provider	Der vCenter Server generiert die Schlüssel.	vCenter Server überprüft die Berechtigungen der Benutzer, die Kryptografie-Vorgänge durchführen.

Sie können den vSphere Client zum Zuweisen von Berechtigungen für Kryptografie-Vorgänge oder zum Zuweisen der benutzerdefinierten Rolle **Kein Kryptografie-Administrator** zu Benutzergruppen verwenden. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für VM-Verschlüsselungsaufgaben.

vCenter Server fügt Kryptografie-Ereignisse zur Ereignisliste hinzu, die Sie über die vSphere Client-Ereigniskonsole anzeigen und exportieren können. Jedes Ereignis enthält den Benutzer, die Uhrzeit, die Schlüssel-ID und den Kryptografie-Vorgang.

Die Schlüssel aus dem Schlüsselserver werden als Schlüssel für Verschlüsselungsschlüssel (KEKs) verwendet.

Welche Rolle spielen ESXi-Hosts bei der Verschlüsselung virtueller vSphere-Maschinen?

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

Tabelle 6-8. Schlüsselanbieter und ESXi-Hosts

Schlüsselanbieter	ESXi-Hostaspekte
Standardschlüsselanbieter	■ vCenter Server leitet Schlüssel an den ESXi-Host weiter, wenn dieser einen Schlüssel benötigt. Auf dem Host muss der Verschlüsselungsmodus aktiviert sein. ■ Es wird sichergestellt, dass die Gastdaten für verschlüsselte virtuelle Maschinen beim Speichern auf die Festplatte verschlüsselt werden. ■ Es wird sichergestellt, dass die Gastdaten für verschlüsselte virtuelle Maschinen nicht ohne Verschlüsselung über das Netzwerk weitergeleitet werden.
Vertrauenswürdiger Schlüsselanbieter	Die ESXi-Hosts führen vSphere Trust Authority aus, je nachdem, ob es sich um vertrauenswürdige Hosts oder Trust Authority Hosts handelt. Auf vertrauenswürdigen ESXi-Hosts werden virtuelle Arbeitslastmaschinen ausgeführt, die mithilfe der von den Trust Authority Hosts veröffentlichten Schlüsselanbieter verschlüsselt werden können. Weitere Informationen hierzu finden Sie unter Vertrauenswürdige vSphere Trust Authority-Infrastruktur.
vSphere Native Key Provider	Die ESXi-Hosts rufen Schlüssel direkt vom vSphere Native Key Provider ab.

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

Prozessablauf bei der Verschlüsselung

Nachdem Sie einen Schlüsselanbieter eingerichtet haben, können Benutzer mit den erforderlichen Berechtigungen verschlüsselte virtuelle Maschinen und Festplatten erstellen. Diese Benutzer können auch vorhandene virtuelle Maschinen verschlüsseln und verschlüsselte virtuelle Maschinen entschlüsseln sowie virtuellen Maschinen vTPMs (Virtual Trusted Platform Modules) hinzufügen.

Je nach Typ des Schlüsselanbieters kann der Prozessablauf einen Schlüsselserver, den vCenter Server und den ESXi-Host beinhalten.

Prozessablauf bei der Verschlüsselung des Standardschlüsselanbieters

Während des Verschlüsselungsvorgangs interagieren die unterschiedlichen Komponenten von vSphere folgendermaßen.

1 Wenn eine Benutzer eine Verschlüsselungsaufgabe durchführt, z. B. die Erstellung einer verschlüsselten virtuellen Maschine, fordert der vCenter Server einen neuen Schlüssel vom Standardschlüsselserver an. Dieser Schlüssel wird als KEK verwendet.

2 Der vCenter Server speichert diese Schlüssel-ID und gibt den Schlüssel an den ESXi-Host weiter. Wenn der ESXi-Host zu einem Cluster gehört, sendet der vCenter Server den KEK an jeden Host im Cluster.

   Der Schlüssel selbst wird nicht im vCenter Server-System gespeichert. Nur die Schlüssel-ID ist bekannt.

3 Der ESXi-Host generiert interne Schlüssel (DEKs) für die virtuelle Maschine und deren Festplatten. Es legt die internen Schlüssel nur im Arbeitsspeicher ab und verwendet die KEKs zum Verschlüsseln der internen Schlüssel.

   Nicht verschlüsselte interne Schlüssel werden niemals auf der Festplatte gespeichert. Es werden nur verschlüsselte Daten gespeichert. Da die KEKs vom Schlüsselserver stammen, verwendet der Host weiterhin dieselben KEKs.

4 Der ESXi-Host verschlüsselt die virtuelle Maschine mit dem verschlüsselten internen Schlüssel.

   Jeder Host, der über den KEK verfügt und auf die verschlüsselte Schlüsseldatei zugreifen kann, kann Vorgänge auf der verschlüsselten virtuellen Maschine oder Festplatte ausführen.

Prozessablauf bei der Verschlüsselung des vertrauenswürdigen Schlüsselanbieters

Der Prozessablauf bei der vSphere Trust Authority-Verschlüsselung umfasst die vSphere Trust Authority-Dienste, die vertrauenswürdigen Schlüsselanbieter sowie den vCenter Server und die ESXi-Hosts.

Das Verschlüsseln einer virtuellen Maschine mit einem vertrauenswürdigen Schlüsselanbieter entspricht der Benutzererfahrung bei der VM-Verschlüsselung bei Verwendung eines Standardschlüsselanbieters. Die VM-Verschlüsselung unter vSphere Trust Authority verlässt sich weiterhin entweder auf die Speicherrichtlinien für die Verschlüsselung von virtuellen Maschinen oder auf das Vorhandensein eines vTPM-Geräts, um zu entscheiden, wann eine virtuelle Maschine verschlüsselt werden soll. Sie verwenden weiterhin einen standardmäßig konfigurierten Schlüsselanbieter (in vSphere 6.5 und 6.7 als KMS-Cluster bezeichnet), wenn Sie eine virtuelle Maschine über den vSphere Client verschlüsseln. Darüber hinaus können Sie die APIs immer noch auf ähnliche Weise verwenden, um den Schlüsselanbieter manuell anzugeben. Die vorhandenen Kryptografierechte, die für vSphere 6.5 hinzugefügt wurden, gelten nach wie vor in vSphere 7.0 und höher für vSphere Trust Authority.

Der Verschlüsselungsprozess für den vertrauenswürdigen Schlüsselanbieter weist einige wichtige Unterschiede zum Standardschlüsselanbieter auf:

- Trust Authority-Administratoren geben Informationen nicht direkt an, wenn sie einen Schlüsselserver für eine vCenter Server-Instanz einrichten, und sie legen auch die Vertrauensstellung des Schlüsselservers nicht fest. Stattdessen veröffentlicht vSphere Trust Authority vertrauenswürdige Schlüsselanbieter, die von den vertrauenswürdigen Hosts verwendet werden können.
- vCenter Server überträgt Schlüssel nicht mehr an ESXi-Hosts und kann stattdessen jeden vertrauenswürdigen Schlüsselanbieter als einzelnen Schlüssel der obersten Ebene verarbeiten.
- Nur vertrauenswürdige Hosts können Verschlüsselungsvorgänge von Trust Authority-Hosts anfordern.

Prozessablauf bei der vSphere Native Key Provider-Verschlüsselung

vSphere Native Key Provider ist in vSphere 7.0 Update 2 und höher enthalten. Wenn Sie einen vSphere Native Key Provider konfigurieren, überträgt vCenter Server einen primären Schlüssel an alle ESXi-Hosts im Cluster. Ebenso wird die Änderung an die Hosts im Cluster übertragen, wenn Sie einen vSphere Native Key Provider aktualisieren oder löschen. Der Prozessablauf bei der Verschlüsselung ähnelt der Funktionsweise eines vertrauenswürdigen Schlüsselanbieters. Der Unterschied besteht darin, dass vSphere Native Key Provider die Schlüssel generiert und sie mit dem Primärschlüssel umhüllt und dann zur Verschlüsselung zurückgibt.

Benutzerdefinierte Attribute für Schlüsselserver

Das KMIP-Protokoll (Key Management Interoperability Protocol) bietet Unterstützung beim Hinzufügen benutzerdefinierter Attribute, die für anbieterspezifische Zwecke bestimmt sind. Mit benutzerdefinierten Attributen können Sie die in Ihrem Schlüsselserver gespeicherten Schlüssel genauer angeben. vCenter Server fügt die folgenden benutzerdefinierten Attribute für VM- und Hostschlüssel hinzu.

Tabelle 6-9. Benutzerdefinierte Attribute für die Verschlüsselung virtueller Maschinen

Benutzerdefiniertes Attribut	Wert
`x-Vendor`	VMware, Inc.
`x-Product`	VMware vSphere
`x-Product_Version`	vCenter Server-Version
`x-Component`	Virtuelle Maschine
`x-Name`	Name der virtuellen Maschine (aus ConfigInfo oder ConfigSpec erfasst)
`x-Identifier`	Instanz-UUID der virtuellen Maschine (aus ConfigInfo oder ConfigSpec erfasst)

Tabelle 6-10. Benutzerdefinierte Attribute für die Hostverschlüsselung

Benutzerdefiniertes Attribut	Wert
`x-Vendor`	VMware, Inc.
`x-Product`	VMware vSphere
`x-Product_Version`	vCenter Server-Version
`x-Component`	ESXi-Server
`x-Name`	Hostname
`x-Identifier`	Hardware-UUID des Hosts

vCenter Server fügt die Attribute `x-Vendor`, `x-Product` und `x-Product_Version` hinzu, wenn der Schlüsselserver einen Schlüssel erstellt. Wenn der Schlüssel zum Verschlüsseln einer virtuellen Maschine oder eines Hosts verwendet wird, legt vCenter Server die Attribute `x-Component`, `x-Identifier` und `x-Name` fest. Unter Umständen können Sie diese benutzerdefinierten Attribute auf der Schlüsselserver-Benutzeroberfläche anzeigen. Erkundigen Sie sich bei Ihrem Schlüsselserveranbieter.

Sowohl der Host- als auch der VM-Schlüssel enthalten die sechs benutzerdefinierten Attribute. `x-Vendor`, `x-Product` und `x-Product_Version` sind möglicherweise für beide Schlüssel identisch. Diese Attribute werden beim Erzeugen des Schlüssels festgelegt. Je nachdem, ob der Schlüssel für eine virtuelle Maschine oder einen Host verwendet wird, werden unter Umständen die Attribute `x-Component`, `x-Identifier` und `x-Name` angehängt.

Verschlüsselungsschlüsselfehler

Wenn beim Senden von Schlüsseln vom Schlüsselserver an einen ESXi-Host ein Fehler auftritt, erzeugt vCenter Server eine Meldung im Ereignisprotokoll für die folgenden Ereignisse:

- Das Hinzufügen von Schlüsseln zum ESXi-Host ist aufgrund von Problemen bei der Hostverbindung oder -unterstützung fehlgeschlagen.
- Das Abrufen von Schlüsseln aus dem Schlüsselserver ist aufgrund eines fehlenden Schlüssels im Schlüsselserver fehlgeschlagen.
- Das Abrufen von Schlüsseln aus dem Schlüsselserver ist aufgrund der Schlüsselserververbindung fehlgeschlagen.

Entschlüsseln verschlüsselter virtueller Maschinen

Wenn Sie später eine verschlüsselte virtuelle Maschine entschlüsseln möchten, ändern Sie deren Speicherrichtlinie. Sie können die Speicherrichtlinie für die virtuelle Maschine und alle Festplatten ändern. Wenn Sie individuelle Komponenten entschlüsseln möchten, entschlüsseln Sie zunächst ausgewählte Festplatten und anschließend die virtuelle Maschine, indem Sie die Speicherrichtlinie für VM-Home ändern. Beide Schlüssel sind für die Entschlüsselung jeder Komponente notwendig. Weitere Informationen hierzu finden Sie unter Entschlüsseln einer verschlüsselten virtuellen Maschine oder virtuellen Festplatte.

Verschlüsseln von virtuellen Festplatten

Wenn Sie eine verschlüsselte virtuelle Maschine anhand des vSphere Client erstellen, können Sie die Festplatten auswählen, die aus der Verschlüsselung ausgeschlossen werden sollen. Sie können später Festplatten hinzufügen und deren Verschlüsselungsrichtlinien festlegen. Sie können keine verschlüsselte Festplatte zu einer unverschlüsselten virtuellen Maschine hinzufügen und Sie können keine Festplatte verschlüsseln, wenn die virtuelle Maschine nicht verschlüsselt ist.

Die Verschlüsselung einer virtuellen Maschine und ihrer Festplatten wird durch Speicherrichtlinien gesteuert. Die Speicherrichtlinie für VM Home regelt die virtuelle Maschine selbst und jede virtuelle Festplatte verfügt über eine zugeordnete Speicherrichtlinie.

- Wenn die Speicherrichtlinien von VM Home auf eine Verschlüsselungsrichtlinie festgelegt werden, wird nur die virtuelle Maschine selbst verschlüsselt.
- Wenn die Speicherrichtlinien von VM Home und allen Festplatten auf eine Verschlüsselungsrichtlinie festgelegt werden, werden alle Komponenten verschlüsselt.

Beachten Sie die folgenden Anwendungsbeispiele.

Tabelle 6-11. Anwendungsbeispiele für die Verschlüsselung von virtuellen Festplatten

Anwendungsfall	Details
Erstellen einer verschlüsselten virtuellen Maschine.	Wenn Sie während der Erstellung einer verschlüsselten virtuellen Maschine Festplatten hinzufügen, werden die Festplatten standardmäßig verschlüsselt. Sie können die Richtlinie so ändern, dass eine oder mehrere Festplatten nicht verschlüsselt werden. Nach Erstellung der virtuellen Maschine können Sie für jede Festplatte explizit die Speicherrichtlinien ändern. Weitere Informationen hierzu finden Sie unter Ändern der Verschlüsselungsrichtlinie für virtuelle Festplatten.
Verschlüsseln einer virtuellen Maschine.	Um eine vorhandene virtuelle Maschine zu verschlüsseln, müssen Sie deren Speicherrichtlinie ändern. Sie können die Speicherrichtlinien für die virtuelle Maschine und alle virtuellen Festplatten ändern. Wenn Sie nur die virtuelle Maschine verschlüsseln möchten, können Sie für VM Home eine Verschlüsselungsrichtlinie und für jede virtuelle Festplatte eine andere Speicherrichtlinie angeben, z. B. Standarddatenspeicher. Weitere Informationen hierzu finden Sie unter Erstellen einer verschlüsselten virtuellen Maschine.
Hinzufügen einer vorhandenen unverschlüsselten Festplatte zu einer verschlüsselten virtuellen Maschine (Speicherrichtlinie für die Verschlüsselung)	Schlägt mit Fehlermeldung fehl. Sie müssen die Festplatte mit der Standard-Speicherrichtlinie hinzufügen, können aber die Speicherrichtlinie später ändern. Weitere Informationen hierzu finden Sie unter Ändern der Verschlüsselungsrichtlinie für virtuelle Festplatten.
Hinzufügen einer vorhandenen unverschlüsselten Festplatte mit einer Speicherrichtlinie zu einer verschlüsselten virtuellen Maschine, die keine Verschlüsselung enthält, z. B. Standarddatenspeicher.	Die Festplatte verwendet die Standard-Speicherrichtlinie. Nach dem Hinzufügen der Festplatte können Sie die Speicherrichtlinie explizit ändern, wenn Sie eine verschlüsselte Festplatte möchten. Weitere Informationen hierzu finden Sie unter Ändern der Verschlüsselungsrichtlinie für virtuelle Festplatten.
Hinzufügen einer verschlüsselten Festplatte zu einer verschlüsselten virtuellen Maschine; Die VM Home-Speicherrichtlinie ist „Verschlüsselung“.	Wenn Sie die Festplatte hinzufügen, bleibt sie verschlüsselt. Der vSphere Client zeigt die Größe und andere Attribute sowie den Verschlüsselungsstatus an.

Tabelle 6-11. Anwendungsbeispiele für die Verschlüsselung von virtuellen Festplatten (Fortsetzung)

Anwendungsfall	Details
Hinzufügen einer vorhandenen verschlüsselten Festplatte zu einer unverschlüsselten virtuellen Maschine	Dieser Anwendungsfall wird nicht unterstützt. Wenn Sie jedoch den vSphere Client verwenden, um die VM-Home-Dateien zu verschlüsseln, können Sie die unverschlüsselte virtuelle Maschine mit der verschlüsselten Festplatte neu konfigurieren.
Registrieren einer verschlüsselten virtuellen Maschine	Wenn Sie eine verschlüsselte virtuelle Maschine aus vCenter Server entfernen, aber nicht von der Festplatte löschen, können Sie sie in die vCenter Server-Bestandsliste zurücksetzen, indem Sie die VMX-Datei (Konfiguration der virtuellen Maschine) der VM registrieren. Um die verschlüsselte VM zu registrieren, muss der Benutzer über das Recht **Verschlüsselungsvorgänge.VM registrieren** verfügen. Wenn die VM mithilfe eines Standardschlüsselanbieters verschlüsselt wurde und die verschlüsselte VM registriert ist, überträgt vCenter Server die erforderlichen Schlüssel an den ESXi-Host. Wenn der Benutzer, der die VM registriert, nicht über das Recht **Verschlüsselungsvorgänge.VM registrieren** verfügt, sperrt vCenter Server die VM bei Registrierung, und die VM kann nicht verwendet werden, bis sie entsperrt wird. Wenn die VM mithilfe eines vertrauenswürdigen Schlüsselanbieters oder vSphere Native Key Provider verschlüsselt wurde und die verschlüsselte VM registriert ist, überträgt vCenter Server keine Schlüssel mehr an den ESXi-Host. Stattdessen werden die Schlüssel vom Hosts abgerufen, wenn die VM registriert ist. Wenn der Benutzer, der die VM registriert, nicht über das Recht **Verschlüsselungsvorgänge.VM registrieren** verfügt, lässt vCenter Server den Vorgang nicht zu.

Fehler bei der Verschlüsselung von virtuellen Maschinen

Wenn vCenter Server auf einen kritischen Fehler bei der VM-Verschlüsselung stößt, wird ein Ereignis erstellt. Sie können diese Ereignisse anzeigen, um Verschlüsselungsfehler zu beheben.

vCenter Server erstellt Ereignisse für die folgenden kritischen Fehler bei der VM-Verschlüsselung.

- Fehler beim Generieren eines KEK.
- Nicht genügend Festplattenspeicher auf dem Datenspeicher, um eine verschlüsselte virtuelle Maschine zu erstellen.
- Unzureichende Benutzerberechtigung zum Initiieren des Verschlüsselungsvorgangs.
- Der angegebene Schlüssel fehlt beim Schlüsselanbieter, sodass der ESXi-Hostschlüssel mit einem neuen Schlüssel erneuert wird.

- Beim Schlüsselanbieter mit dem angegebenen Schlüssel ist ein Fehler aufgetreten. Daher wird der ESXi-Hostschlüssel mit einem neuen Schlüssel erneuert.

Voraussetzungen und erforderliche Berechtigungen für VM-Verschlüsselungsaufgaben

VM-Verschlüsselungsaufgaben sind nur in Umgebungen mit vCenter Server möglich. Zusätzlich muss für die meisten Verschlüsselungsaufgaben bei dem ESXi-Host der Verschlüsselungsmodus aktiviert sein. Der Benutzer, der diese Aufgaben durchführt, muss über die entsprechenden Berechtigungen verfügen. Eine Gruppe von Berechtigungen für **Kryptografievorgänge** ermöglicht eine detaillierte Steuerung. Wenn bei Verschlüsselungsaufgaben für virtuelle Maschinen ein Wechsel in den Hostverschlüsselungsmodus erforderlich ist, sind zusätzliche Berechtigungen erforderlich.

Hinweis vSphere Trust Authority weist zusätzliche Voraussetzungen und notwendige Berechtigungen auf. Weitere Informationen hierzu finden Sie unter Voraussetzungen und notwendige Berechtigungen für vSphere Trust Authority.

Verwenden von Kryptografieberechtigungen und -rollen

Standardmäßig verfügt der Benutzer mit der Rolle des vCenter Server-Administrators über alle Berechtigungen, einschließlich der Berechtigungen für Kryptografievorgänge. Die Rolle **Kein Kryptografie-Administrator** ist mit den folgenden, für Kryptografie-Vorgänge erforderlichen Berechtigungen ausgestattet.

Wichtig ESXi Shell-Benutzer verfügen auch über Berechtigungen für kryptografische Vorgänge.

- Fügen Sie Berechtigungen für **Kryptografievorgänge** hinzu.
- **Global.Diagnose**
- **Host.Bestandsliste.Host zu Cluster hinzufügen**
- **Host.Bestandsliste.Eigenständigen Host hinzufügen**
- **Host.Lokale Vorgänge.Benutzergruppen verwalten**

Sie können die Rolle **Kein Kryptografie-Administrator** vCenter Server-Administratoren zuweisen, die die Berechtigungen **Kryptografievorgänge** nicht benötigen.

Um den Handlungsspielraum der Benutzer weiter einzuschränken, können Sie die Rolle **Kein Kryptografie-Administrator** klonen und eine benutzerdefinierte Rolle erstellen, die nur bestimmte Berechtigungen der **Kryptografievorgänge** umfasst. Sie können beispielsweise eine Rolle erstellen, die Benutzern das Verschlüsseln virtueller Maschinen erlaubt, das Entschlüsseln jedoch nicht. Weitere Informationen hierzu finden Sie unter Verwenden von vCenter Server-Rollen zum Zuweisen von Rechten.

Was ist der Hostverschlüsselungsmodus?

Der Hostverschlüsselungsmodus entscheidet darüber, ob ein ESXi-Host bereit ist, kryptografisches Material zum Verschlüsseln virtueller Maschinen und virtueller Festplatten zu akzeptieren. Bevor Kryptografievorgänge auf einem Host stattfinden können, muss der Verschlüsselungsmodus aktiviert werden. Der Hostverschlüsselungsmodus wird häufig automatisch festgelegt, wenn er benötigt wird. Sie können ihn jedoch explizit festlegen. Sie können den aktuellen Hostverschlüsselungsmodus über den vSphere Client oder die vSphere API festlegen.

Wenn der Hostverschlüsselungsmodus aktiviert ist, installiert vCenter Server auf dem Host einen Hostschlüssel, der sicherstellt, dass der Host in kryptografischer Hinsicht „sicher“ ist. Nachdem der Hostschlüssel installiert wurde, können andere Kryptografievorgänge ablaufen, einschließlich des Abrufens von Schlüsseln aus dem Schlüsselanbieter und deren Weitergabe an die ESXi-Hosts seitens vCenter Server.

Im „sicheren“ Modus werden die Core-Dumps von Benutzer-Worlds (d. h. hostd) und verschlüsselten virtuellen Maschinen verschlüsselt. Die Core-Dumps von nicht verschlüsselten virtuellen Maschinen werden nicht verschlüsselt.

Weitere Informationen zu verschlüsselten Core-Dumps und deren Verwendung seitens des technischen Supports von VMware finden Sie im VMware Knowledgebase-Artikel unter https://kb.vmware.com/s/article/2147388.

Eine Anleitung dafür finden Sie in Explizites Aktivieren des Hostverschlüsselungsmodus.

Nach dem Festlegen des Hostverschlüsselungsmodus ist dessen einfache Deaktivierung nicht mehr möglich. Weitere Informationen hierzu finden Sie unter Deaktivieren des Hostverschlüsselungsmodus mithilfe der API.

Es werden automatische Änderungen vorgenommen, wenn Verschlüsselungsvorgänge versuchen, den Hostverschlüsselungsmodus festzulegen. Angenommen, Sie möchten einem eigenständigen Host eine verschlüsselte virtuelle Maschine hinzufügen. Der Hostverschlüsselungsmodus ist nicht festgelegt. Wenn Sie über die erforderlichen Berechtigungen auf dem Host verfügen, wird der Verschlüsselungsmodus automatisch festgelegt.

Angenommen, ein Cluster umfasst die drei ESXi-Hosts A, B und C. Sie erstellen eine verschlüsselte virtuelle Maschine auf Host A. Was daraufhin geschieht, hängt von mehreren Faktoren ab.

- Wenn für die Hosts A, B und C der Hostverschlüsselungsmodus bereits festgelegt ist, benötigen Sie nur die Berechtigungen **Kryptografievorgänge.Neue verschlüsseln**, um die virtuelle Maschine zu erstellen.

- Wenn für die Hosts A und B die Hostverschlüsselung festgelegt ist und für C nicht, geht das System wie folgt vor.
  - Nehmen wir an, dass Sie auf jedem Host über die Berechtigungen **Kryptografievorgänge.Neue verschlüsseln** und **Kryptografievorgänge.Host registrieren** verfügen. In diesem Fall legt der Verschlüsselungsvorgang den Hostverschlüsselungsmodus auf Host C fest und überträgt den Schlüssel an jeden Host im Cluster.

    In diesem Fall können Sie die Hostverschlüsselung auf Host C auch explizit festlegen.
  - Angenommen, Sie verfügen auf der virtuellen Maschine bzw. dem VM-Ordner nur über die Berechtigungen **Kryptografievorgänge.Neue verschlüsseln**. In diesem Fall gelingt die Erstellung der virtuellen Maschine und der Schlüssel steht auf Host A und Host B zur Verfügung. Host C bleibt für die Verschlüsselung deaktiviert und verfügt nicht über den Schlüssel der virtuellen Maschine.
- Wenn der Hostverschlüsselungsmodus für keinen der Hosts festgelegt ist und Sie auf Host A über die Berechtigungen **Kryptografievorgänge.Host registrieren** verfügen, wird der Hostverschlüsselungsmodus auf diesem Host durch den Prozess zum Erstellen der virtuellen Maschine festgelegt. Andernfalls tritt bei den Hosts B und C ein Fehler auf.
- Sie können auch die vSphere API verwenden, um den Verschlüsselungsmodus eines Clusters auf „Aktivierung erzwingen“ festzulegen. Mit „Aktivierung erzwingen“ wird erreicht, dass alle Hosts im Cluster in kryptografischer Hinsicht „sicher“ sind, d. h., vCenter Server hat einen Hostschlüssel auf dem Host installiert. Weitere Informationen hierzu finden Sie unter *Programmierhandbuch zum vSphere Web Services SDK*.

Festplattenspeicheranforderungen beim Verschlüsseln virtueller Maschinen

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

Was ist verschlüsseltes vSphere vMotion

Verschlüsseltes vSphere vMotion sichert die Vertraulichkeit, Integrität und Authentizität der mit vSphere vMotion übertragenen Daten. vSphere unterstützt verschlüsseltes vMotion nicht verschlüsselter und verschlüsselter virtueller Maschinen für vCenter Server-Instanzen.

vSphere vMotion verwendet beim Migrieren verschlüsselter virtueller Maschinen immer Verschlüsselung. Bei nicht verschlüsseln virtuellen Maschinen können Sie eine der verschlüsselten vSphere vMotion-Optionen auswählen.

Was wird in verschlüsseltem vSphere vMotion verschlüsselt

Bei verschlüsselten Festplatten werden die übertragenen Daten immer verschlüsselt übertragen. Bei unverschlüsselten Festplatten gilt Folgendes:

- Wenn Festplattendaten innerhalb eines Hosts übertragen werden, also ohne den Host zu ändern, ändern Sie nur den Datenspeicher; die Übertragung wird nicht verschlüsselt.
- Wenn Festplattendaten zwischen Hosts übertragen und verschlüsseltes vMotion verwendet wird, wird die Übertragung verschlüsselt. Wenn verschlüsseltes vMotion nicht verwendet wird, wird die Übertragung unverschlüsselt.

Bei verschlüsselten virtuellen Maschinen wird für die Migration mit vSphere vMotion immer verschlüsseltes vSphere vMotion verwendet. Sie können verschlüsseltes vSphere vMotion für verschlüsselte virtuelle Maschinen nicht deaktivieren.

Zustände von verschlüsseltem vSphere vMotion für unverschlüsselte virtuelle Maschinen

Bei nicht verschlüsselten virtuellen Maschinen können Sie für die Verschlüsselung von vSphere vMotion einen der folgenden Zustände festlegen. Der Standard ist „Opportunistisch“.

Deaktiviert

Verschlüsseltes vSphere vMotion wird nicht verwendet.

Opportunistisch

Verschlüsseltes vSphere vMotion wird verwendet, wenn diese Funktion von Quell- und Zielhosts unterstützt wird. Nur ESXi-Hosts der Version 6.5 und höher unterstützen verschlüsseltes vSphere vMotion.

Erforderlich

Nur verschlüsseltes vSphere vMotion zulassen. Wenn der Quell- oder Zielhost verschlüsseltes vSphere vMotion nicht unterstützt, ist die Migration mit vSphere vMotion nicht zulässig.

Wenn Sie eine virtuelle Maschine verschlüsseln, speichert die virtuelle Maschine einen Eintrag der aktuellen Verschlüsselungseinstellung von vSphere vMotion. Wenn Sie zu einem späteren Zeitpunkt die Verschlüsselung der virtuellen Maschine deaktivieren, verbleibt die verschlüsselte vMotion-Einstellung im Zustand „Erforderlich“, bis Sie diese Einstellung explizit ändern. Sie können diese Einstellungen über **Einstellungen bearbeiten** ändern.

Weitere Informationen zum Aktivieren und Deaktivieren von verschlüsseltem vSphere vMotion für nicht verschlüsselte virtuelle Maschinen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Hinweis Derzeit müssen Sie die vSphere APIs verwenden, um verschlüsselte virtuelle Maschinen über vCenter Server-Instanzen hinweg zu migrieren oder zu klonen. Weitere Informationen finden Sie unter *Programmierhandbuch zum vSphere Web Services SDK* und *vSphere Web Services-API-Referenz*.

Migrieren oder Klonen verschlüsselter virtueller Maschinen über vCenter Server-Instanzen hinweg

vSphere vMotion bietet Unterstützung für die Migration und das Klonen verschlüsselter virtueller Maschinen über vCenter Server-Instanzen hinweg.

Beim Migrieren oder Klonen verschlüsselter virtueller Maschinen über vCenter Server-Instanzen müssen die Quell- und Zielinstanz von vCenter Server für die gemeinsame Nutzung des Schlüsselanbieters konfiguriert werden, der zum Verschlüsseln der virtuellen Maschine verwendet wurde. Darüber hinaus muss der Name des Schlüsselanbieters sowohl auf der Quell- als auch auf der Zielinstanz in vCenter Server identisch sein und folgende Eigenschaften aufweisen:

- Standardschlüsselanbieter: Derselbe Schlüsselserver (oder mehrere Schlüsselserver) muss sich im Schlüsselanbieter befinden.
- Vertrauenswürdiger Schlüsselanbieter: Derselbe vSphere Trust Authority-Dienst muss auf dem Zielhost konfiguriert werden.
- vSphere Native Key Provider: Muss denselben KDK aufweisen.

  Hinweis Sie können eine verschlüsselte virtuelle Maschine nicht mithilfe des vSphere Native Key Provider auf einen eigenständigen Host klonen oder migrieren, unabhängig davon, ob sich der Quellhost in einem Cluster befindet.

Der Ziel-vCenter Server stellt sicher, dass auf dem ESXi-Host der Verschlüsselungsmodus festgelegt ist. Dadurch wird sichergestellt, dass der Host kryptografisch „sicher“ ist.

Die folgenden Rechte sind erforderlich, wenn Sie vSphere vMotion verwenden, um eine verschlüsselte virtuelle Maschine über vCenter Server-Instanzen hinweg zu migrieren oder zu klonen.

- Migrieren: **Kryptografievorgänge.Migrieren** auf der virtuellen Maschine
- Klonen: **Kryptografievorgänge.Klonen** auf der virtuellen Maschine

Außerdem muss der Ziel-vCenter Server die Berechtigung **Kryptografievorgänge.Neue verschlüsseln** aufweisen. Wenn der ESXi-Zielhost nicht im sicheren Modus ausgeführt wird, muss sich die Berechtigung **Kryptografievorgänge.Host registrieren** ebenfalls auf dem Ziel-vCenter Server befinden.

Bestimmte Aufgaben sind nicht zulässig, wenn virtuelle Maschinen (nicht verschlüsselt oder verschlüsselt) auf demselben vCenter Server oder auf mehreren vCenter Server-Instanzen migriert werden.

- Sie können die VM-Speicherrichtlinie nicht ändern.
- Sie können keine Schlüsseländerung vornehmen.

Hinweis Sie können die VM-Speicherrichtlinie beim Klonen virtueller Maschinen ändern.

Mindestanforderungen zum Migrieren oder Klonen verschlüsselter virtueller Maschinen über vCenter Server-Instanzen hinweg

Die Mindestanforderungen an die Version zum Migrieren oder Klonen verschlüsselter virtueller Maschinen des Standardschlüsselanbieters über vCenter Server-Instanzen mithilfe von vSphere vMotion lauten:

- Auf der Quell- und Zielinstanz von vCenter Server muss Version 7.0 oder höher installiert sein.
- Auf dem Quell- und Zielhost von ESXi muss Version 6.7 oder höher installiert sein.

Die Mindestanforderungen an die Version zum Migrieren oder Klonen verschlüsselter virtueller Maschinen des vertrauenswürdigen Schlüsselanbieters über vCenter Server-Instanzen mithilfe von vSphere vMotion lauten:

- Der vSphere Trust Authority-Dienst muss für den Zielhost konfiguriert werden und der Zielhost muss bestätigt sein.
- Die Verschlüsselung kann bei der Migration nicht geändert werden. Eine nicht verschlüsselte Festplatte kann beispielsweise nicht verschlüsselt werden, während die virtuelle Maschine auf den neuen Speicher migriert wird.
- Sie können eine verschlüsselte virtuelle Standardmaschine auf einen vertrauenswürdigen Host migrieren. Der Name des Schlüsselanbieters muss sowohl auf der Quell- als auch auf der Zielinstanz von vCenter Server identisch sein.
- Sie können eine verschlüsselte virtuelle vSphere Trust Authority-Maschine nicht auf einen nicht vertrauenswürdigen Host migrieren.

vMotion des vertrauenswürdigen Schlüsselanbieters und vCenter Server-übergreifendes vMotion

Der vertrauenswürdige Schlüsselanbieter bietet vollständige Unterstützung für vMotion über mehrere ESXi-Hosts hinweg.

vCenter Server übergreifendes vMotion wird mit den folgenden Einschränkungen unterstützt.

1. Der benötigte vertrauenswürdige Dienst muss auf dem Zielhost konfiguriert und der Zielhost muss bestätigt werden.
2. Die Verschlüsselung kann bei der Migration nicht geändert werden. Eine Festplatte kann beispielsweise nicht verschlüsselt werden, während die virtuelle Maschine auf den neuen Speicher migriert wird.

Bei der Durchführung von vCenter Server-übergreifendem vMotion überprüft vCenter Server, ob der vertrauenswürdige Schlüsselanbieter auf dem Zielhost verfügbar ist und ob der Host darauf zugreifen kann.

vMotion des vSphere Native Key Providers und vCenter Server-übergreifendes vMotion

vSphere Native Key Provider unterstützt vMotion und Verschlüsseltes vMotion für ESXi-Hosts. vCenter Server-übergreifendes vMotion wird unterstützt, wenn vSphere Native Key Provider auf dem Zielhost konfiguriert ist.

Virtuelle Maschine – Empfohlene Vorgehensweisen für die Verschlüsselung

Die folgenden empfohlenen Vorgehensweisen für die Verschlüsselung von virtuellen Maschinen sollten zwecks Vermeidung späterer Probleme befolgt werden, zum Beispiel wenn Sie ein `vm-support`-Paket erstellen.

Best Practices für die Verschlüsselung virtueller Maschinen für die ersten Schritte

Befolgen Sie bei Verwendung der Verschlüsselung virtueller Maschinen die folgenden allgemeinen Best Practices.

- Verschlüsseln Sie keine virtuellen Maschinen der vCenter Server Appliance.
- Wenn Ihr ESXi-Host fehlschlägt, rufen Sie schnellstmöglich das Support-Paket ab. Sie benötigen den Hostschlüssel zum Generieren eines Support-Pakets mit einem Kennwort oder zum Entschlüsseln des Core-Dumps. Wenn der Host neu gestartet wird, ändert sich der Hostschlüssel möglicherweise. Ist dies der Fall, können Sie mit diesem Hostschlüssel kein Support-Paket mehr mit einem Kennwort generieren bzw. keine Core-Dumps im Support-Paket entschlüsseln.
- Verwalten Sie die Namen von Schlüsselanbietern sorgfältig. Wenn sich der Name des Schlüsselanbieters für einen bereits verwendeten Schlüsselserver ändert, wechseln VMs, die mit Schlüsseln aus diesem Schlüsselserver verschlüsselt sind, beim Einschalten oder bei der Registrierung in einen gesperrten Zustand. Entfernen Sie in diesem Fall den Schlüsselserver aus dem vCenter Server und fügen Sie ihn mit dem Schlüsselanbieternamen hinzu, den Sie anfänglich verwendet haben.
- Bearbeiten Sie keine VMX-Dateien und VMDK-Deskriptordateien. Diese Dateien enthalten das Verschlüsselungspaket. Möglicherweise kann die virtuelle Maschine nach Ihren Änderungen nicht mehr wiederhergestellt werden und dieses Wiederherstellungsproblem kann nicht behoben werden.
- Der vSphere-Prozess zur Verschlüsselung virtueller Maschinen verschlüsselt die Daten auf dem Host, bevor die Daten in den Speicher geschrieben werden. Die Effektivität von Back-End-Speicherfunktionen wie Deduplizierung, Komprimierung, Replizierung usw. kann beeinträchtigt werden, wenn virtuelle Maschinen auf diese Weise verschlüsselt werden.

- Wenn Sie mehrere Verschlüsselungsebenen verwenden, z. B. die Verschlüsselung virtueller Maschinen von vSphere und In-Guest-Verschlüsselung (BitLocker, dm-crypt usw.), kann dies die Gesamtleistung der virtuellen Maschinen beeinträchtigen, da die Verschlüsselungsprozesse zusätzliche CPU- und Arbeitsspeicherressourcen verwenden.
- Sorgen Sie dafür, dass replizierte Kopien von virtuellen Maschinen, die über die Verschlüsselung virtueller Maschinen von vSphere verschlüsselt wurden, in der Wiederherstellungs-Site Zugriff auf die Verschlüsselungsschlüssel haben. Für Standardschlüsselanbieter ist dies Teil des Designs des Schlüsselverwaltungssystems außerhalb von vSphere. Stellen Sie für vSphere Native Key Provider sicher, dass eine Sicherungskopie des Schlüssels von Native Key Provider vorhanden ist und vor Verlust geschützt ist. Weitere Informationen finden Sie unter Sichern eines vSphere Native Key Providers.
- Die Verschlüsselung ist CPU-intensiv. Mit AES-NI wird die Verschlüsselungsleistung deutlich gesteigert. Aktivieren Sie AES-NI im BIOS.

Empfohlene Vorgehensweisen für verschlüsselte Core-Dumps

Befolgen Sie diese empfohlenen Vorgehensweisen, damit keine Probleme auftreten, wenn Sie einen Core-Dump zwecks Problemdiagnose untersuchen möchten.

- Erstellen Sie eine Richtlinie bezüglich Core-Dumps. Core-Dumps sind verschlüsselt, da sie vertrauliche Informationen wie etwa Schlüssel enthalten können. Wenn Sie einen Core-Dump entschlüsseln, gehen Sie sehr sorgfältig mit den enthaltenen vertraulichen Informationen um. ESXi- Core-Dumps können Schlüssel für den ESXi-Host und die sich darauf befindlichen virtuellen Maschinen enthalten. Sie sollten den Hostschlüssel ändern und verschlüsselte virtuelle Maschinen erneut verschlüsseln, nachdem Sie einen Core-Dump entschlüsselt haben. Beide Aufgaben können mit der vSphere API durchgeführt werden.

  Weitere Informationen finden Sie unter vSphere VM-Verschlüsselung und Core-Dumps.
- Verwenden Sie immer ein Kennwort, wenn Sie ein `vm-support`-Paket erfassen. Sie können das Kennwort angeben, wenn Sie das Support-Paket vom vSphere Client generieren oder den `vm-support`-Befehl verwenden.

  Das Kennwort verschlüsselt Core-Dumps erneut, die interne Schlüssel zur Verwendung von auf diesem Kennwort basierenden Schlüsseln verwenden. Sie können das Kennwort zu einem späteren Zeitpunkt zum Entschlüsseln und Verschlüsseln von Core-Dumps verwenden, die möglicherweise im Support-Paket enthalten sind. Nicht verschlüsselte Core-Dumps und Protokolle sind bei Verwendung der Kennwortoption nicht betroffen.
- Das von Ihnen während der `vm-support`-Paketerstellung angegebene Kennwort wird in vSphere-Komponenten nicht dauerhaft gespeichert. Sie müssen Ihre Kennwörter für Support-Pakete selbst speichern bzw. diese notieren.
- Bevor Sie den Hostschlüssel ändern, generieren Sie ein `vm-support`-Paket mit einem Kennwort. Sie können das Kennwort später für den Zugriff auf alle Core-Dumps verwenden, die ggf. mit dem alten Hostschlüssel verschlüsselt wurden.

Best Practices für Key Lifecycle Management

Implementieren Sie empfohlene Vorgehensweisen, die Schlüsselserver-Verfügbarkeit garantieren und Schlüssel auf dem Schlüsselserver überwachen.

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

  Wenn der Schlüsselserver nicht verfügbar ist, sind VM-Vorgänge nicht möglich, bei denen vCenter Server den Schlüssel vom Schlüsselserver abrufen muss. Laufende virtuelle Maschinen werden daher fortwährend ausgeführt und Sie können sie ausschalten, einschalten und neu konfigurieren. Sie können eine virtuelle Maschine jedoch nicht auf einen Host verlagern, der nicht über die Schlüsselinformationen verfügt.

  Die meisten Schlüsselserver-Lösungen beinhalten HA (High Availability)-Funktionen. Sie können den vSphere Client oder die API verwenden, um einen Schlüsselanbieter und die verbundenen Schlüsselserver anzugeben.

  Hinweis Ab Version 7.0 Update 2 können verschlüsselte virtuelle Maschinen und virtuelle TPMs auch dann weiterhin funktionieren, wenn der Schlüsselserver vorübergehend offline oder nicht verfügbar ist. Die ESXi-Hosts können die Verschlüsselungsschlüssel beibehalten, um die Verschlüsselung und vTPM-Vorgänge fortzusetzen. Weitere Informationen hierzu finden Sie unter vSphere-Schlüsselpersistenz auf ESXi-Hosts.

- Sie müssen die Schlüssel speichern und eine Standardisierung durchführen, wenn sich die Schlüssel für vorhandene virtuelle Maschinen nicht im aktiven Zustand befinden.

  Der KMIP-Standard definiert die folgenden Zustände für Schlüssel.

  - Voraktiv
  - Aktiv
  - Deaktiviert
  - Manipuliert
  - Zerstört
  - Zerstört/Manipuliert

  Bei der Verschlüsselung der virtuellen vSphere-Maschinen werden nur aktive Schlüssel verwendet. Wenn ein Schlüssel voraktiv ist, wird dieser über die Funktion „Verschlüsselung der virtuellen vSphere-Maschine“ aktiviert. Wenn der Schlüsselzustand „Deaktiviert“, „Manipuliert“, „Zerstört“ oder „Zerstört/Manipuliert“ ist, können Sie eine virtuelle Maschine oder Festplatte nicht mit diesem Schlüssel verschlüsseln.

  Für Schlüssel, die andere Zustände aufweisen, werden virtuelle Maschinen unter Verwendung dieser Schlüssel weiterhin ausgeführt. Ob ein Klon- oder Migrationsvorgang erfolgreich ist, hängt davon ab, ob sich der Schlüssel bereits auf dem Host befindet.

  - Wenn sich der Schlüssel auf einem Zielhost befindet, wird der Vorgang erfolgreich ausgeführt, auch wenn der Schlüssel auf dem Schlüsselserver nicht aktiv ist.

- Wenn sich die erforderlichen Schlüssel für die virtuellen Maschinen und die virtuellen Festplatten nicht auf dem Zielhost befinden, muss vCenter Server die Schlüssel vom Schlüsselserver abrufen. Wenn es sich bei dem Schlüsselzustand um „Deaktiviert“, „Manipuliert“, „Zerstört“ oder „Zerstört/Manipuliert“ handelt, zeigt vCenter Server eine Fehlermeldung an und der Vorgang wird nicht erfolgreich durchgeführt.

  Ein Klon- oder Migrationsvorgang wird erfolgreich durchgeführt, wenn sich der Schlüssel bereits auf dem Host befindet. Der Vorgang schlägt fehl, wenn vCenter Server die Schlüssel vom Schlüsselserver abruft.

  Wenn ein Schlüssel nicht aktiv ist, führen Sie eine erneute Verschlüsselung unter Verwendung der API durch. Weitere Informationen finden Sie im *Programmierhandbuch zum vSphere Web Services SDK*.

- Entwickeln Sie Richtlinien für die Schlüsselrotation, sodass Schlüssel nach einer bestimmten Zeit stillgelegt und ein Rollover durchgeführt wird.
  - Vertrauenswürdiger Schlüsselanbieter: Ändern Sie den primären Schlüssel eines vertrauenswürdigen Schlüsselanbieters.
  - vSphere Native Key Provider: Ändern Sie die `key_id` eines vSphere Native Key Provider.

Best Practices für Sicherung und Wiederherstellung

Erstellen Sie Richtlinien für Sicherungs- und Wiederherstellungsvorgänge.

- Es werden nicht alle Sicherungsarchitekturen unterstützt. Weitere Informationen hierzu finden Sie unter Interoperabilität bei der Verschlüsselung von virtuellen Maschinen.
- Erstellen Sie Richtlinien für Wiederherstellungsvorgänge. Da die Sicherung immer auf Klartextdaten beruht, sollten Sie virtuelle Maschinen direkt nach Beendigung der Wiederherstellung verschlüsseln. Sie können angeben, dass die virtuelle Maschine als Teil des Wiederherstellungsvorgangs verschlüsselt wird. Wenn möglich, verschlüsseln Sie die virtuelle Maschine als Teil des Wiederherstellungsvorgangs, um die Offenlegung von vertraulichen Informationen zu vermeiden. Um die Verschlüsselungsrichtlinie für Festplatten zu ändern, die mit der virtuellen Maschine verbunden sind, ändern Sie die Speicherrichtlinie für diese Festplatte.
- Da die VM-Home-Dateien verschlüsselt sind, stellen Sie sicher, dass die Verschlüsselungsschlüssel zum Zeitpunkt der Wiederherstellung verfügbar sind.

Best Practices für die Verschlüsselungsleistung

- Die Verschlüsselungsleistung richtet sich nach der CPU- und Speicherkapazität.
- Die Verschlüsselung von vorhandenen virtuellen Maschinen nimmt mehr Zeit in Anspruch als die Verschlüsselung einer virtuellen Maschine bei deren Erstellung. Verschlüsseln Sie also eine virtuelle Maschine wenn möglich bei deren Erstellung.

Best Practices für die Beispielspeicherrichtlinie

Ändern Sie nicht die im Paket enthaltene Beispielspeicherrichtlinie für die VM-Verschlüsselung. Klonen Sie stattdessen die Richtlinie und bearbeiten Sie den Klon.

Hinweis Die Zurücksetzung der VM-Verschlüsselungsrichtlinie auf ihre ursprünglichen Einstellungen ist nicht möglich.

Details zur Anpassung von Speicherrichtlinien finden Sie in der *vSphere-Speicher*-Dokumentation.

Best Practices für das Entfernen von Verschlüsselungsschlüsseln

Um sicherzustellen, dass Verschlüsselungsschlüssel aus einem Cluster entfernt werden, starten Sie nach dem Löschen, Aufheben der Registrierung oder Verschieben der verschlüsselten virtuellen Maschine in einen anderen vCenter Server die ESXi-Hosts im Cluster neu.

Vorbehalte bei der Verschlüsselung von virtuellen Maschinen

Machen Sie sich mit den Vorbehalten bei der Verschlüsselung von virtuellen Maschinen vertraut, um möglicherweise später auftretende Probleme zu vermeiden.

Informationen darüber, welche Geräte und Funktionen nicht bei der Verschlüsselung von virtuellen Maschinen verwendet werden können, finden Sie unter Interoperabilität bei der Verschlüsselung von virtuellen Maschinen.

Beschränkungen für verschlüsselte virtuelle Maschinen

Beachten Sie die folgenden Vorbehalte bei der Planung Ihrer Strategie zur Verschlüsselung von virtuellen Maschinen.

- Wenn Sie eine verschlüsselte Maschine klonen oder einen Storage vMotion-Vorgang durchführen, können Sie versuchen, das Festplattenformat zu ändern. Diese Konvertierungen sind jedoch nicht immer erfolgreich. Wenn Sie beispielsweise eine virtuelle Maschine klonen und versuchen, das Festplattenformat von „lazy-zeroed thick“ in „thin“ zu ändern, behält die Festplatte der virtuellen Maschine das Format „lazy-zeroed thick“ bei.
- Wenn Sie eine Festplatte von einer virtuellen Maschine trennen, werden die Informationen der Speicherrichtlinie für die virtuelle Festplatte nicht gespeichert.
  - Wenn die virtuelle Festplatte verschlüsselt ist, müssen Sie die Speicherrichtlinie explizit auf „VM-Speicherrichtlinie“ oder auf eine Speicherrichtlinie festlegen, die Verschlüsselung enthält.
  - Wenn die virtuelle Festplatte nicht verschlüsselt ist, können Sie die Speicherrichtlinie ändern, wenn Sie die Festplatte zu einer virtuellen Maschine hinzufügen.

  Weitere Informationen finden Sie unter Verschlüsseln von virtuellen Festplatten.

- Entschlüsseln Sie Core-Dumps, bevor Sie eine virtuelle Maschine auf einen anderen Cluster verschieben.

  Der vCenter Server speichert keine Schlüsselserver-Schlüssel, sondern nur die Schlüssel-IDs. vCenter Server speichert daher den ESXi-Hostschlüssel nicht dauerhaft. In vSphere 7.0 Update 2 und höher können verschlüsselte Geräte auch dann funktionieren, wenn der Zugriff auf einen Schlüsselserver unterbrochen ist. Weitere Informationen finden Sie unter vSphere-Schlüsselpersistenz auf ESXi-Hosts.

  Unter gewissen Umständen, zum Beispiel beim Verschieben des ESXi-Hosts auf einen anderen Cluster und beim Neustart des Hosts weist vCenter Server dem Host einen neuen Hostschlüssel zu. Sie können keine vorhandenen Core-Dumps mit dem neuen Hostschlüssel entschlüsseln.
- OVF-Export wird für eine verschlüsselte virtuelle Maschine nicht unterstützt.
- Die Verwendung des VMware Host Client zum Registrieren einer verschlüsselten virtuellen Maschine wird nicht unterstützt.

Virtuelle Maschine im gesperrten Zustand

Wenn der Schlüssel für eine virtuelle Maschine oder mindestens ein Schlüssel für die virtuellen Festplatten fehlt, wechselt die virtuelle Maschine in einen gesperrten Zustand. In einem gesperrten Zustand können Sie keine Vorgänge für die virtuelle Maschine durchführen.

- Wenn Sie eine virtuelle Maschine und deren Festplatten über den vSphere Client verschlüsseln, wird derselbe Schlüssel für beide Vorgänge verwendet.
- Wenn Sie die Verschlüsselung mit der API durchführen, können Sie verschiedene Verschlüsselungsschlüssel für die virtuelle Maschine und deren Festplatten verwenden. Wenn Sie in diesem Fall versuchen, eine virtuelle Maschine einzuschalten, und einer der Festplattenschlüssel fehlt, schlägt das Einschalten fehl. Wenn Sie die virtuelle Festplatte entfernen, können Sie die virtuelle Maschine einschalten.

Vorschläge zur Fehlerbehebung finden Sie unter Beheben von Problemen in Bezug auf fehlende Verschlüsselungsschlüssel.

Interoperabilität bei der Verschlüsselung von virtuellen Maschinen

vSphere Virtual Machine Encryption weist einige Einschränkungen in Bezug auf Geräte und Funktionen auf, mit denen Interoperabilität möglich ist.

Die folgenden Einschränkungen und Anmerkungen beziehen sich auf die Verwendung von vSphere Virtual Machine Encryption. Ähnliche Informationen zur Verwendung der vSAN-Verschlüsselung finden Sie in der Dokumentation *Verwalten von VMware vSAN*.

Einschränkungen bei bestimmten Verschlüsselungsaufgaben

Für die Durchführung bestimmter Aufgaben auf einer verschlüsselten virtuellen Maschine gelten einige Einschränkungen.

- Bei den meisten verschlüsselten virtuellen Maschinen müssen Sie die virtuelle Maschine ausschalten. Sie können eine verschlüsselte virtuelle Maschine klonen und beim Einschalten der virtuellen Maschine eine oberflächliche erneute Verschlüsselung vornehmen.

  Hinweis Virtuelle Maschinen, die mit IDE-Controllern konfiguriert sind, müssen ausgeschaltet werden, um eine flache erneute Schlüsselerstellung durchzuführen.

- Auf einer virtuellen Maschine mit Snapshots kann keine tiefe Neuverschlüsselung durchgeführt werden. Auf einer virtuellen Maschine mit Snapshots kann eine flache Neuverschlüsselung durchgeführt werden.

Virtual Trusted Platform Module-Geräte und vSphere Virtual Machine Encryption

Ein vTPM (Virtual Trusted Platform Module) ist eine softwarebasierte Darstellung eines physischen Trusted Platform Module 2.0-Chips. Sie können ein vTPM zu einer neuen oder einer vorhandenen virtuellen Maschine hinzufügen. Zum Hinzufügen eines vTPM zu einer virtuellen Maschine müssen Sie einen Schlüsselanbieter in Ihrer vSphere-Umgebung konfigurieren. Wenn Sie ein vTPM konfigurieren, werden die Home-Dateien der virtuellen Maschine verschlüsselt (Arbeitsspeicherauslagerung, NVRAM-Dateien usw.). Die Festplattendateien oder VMDK-Dateien werden nicht automatisch verschlüsselt. Sie haben die Möglichkeit, Verschlüsselung für die Festplatten der virtuellen Maschine explizit hinzuzufügen.

Vorsicht Durch das Klonen einer virtuellen Maschine wird die gesamte virtuelle Maschine, einschließlich der virtuellen Geräte, wie z. B. eines vTPM, dupliziert. Die im vTPM gespeicherten Informationen, einschließlich der Eigenschaften des vTPM, mit denen die Software die Identität eines Systems ermitteln kann, werden ebenfalls dupliziert.

Ab vSphere 8.0 können Sie beim Klonen einer virtuellen Maschine, die ein vTPM enthält, mit einem neuen, leeren vTPM beginnen, das seine eigenen geheimen Schlüssel und Identität erhält.

vSphere Virtual Machine Encryption sowie Zustand „Angehalten“ und Snapshots

Sie können eine im angehaltenen Zustand befindliche verschlüsselte virtuelle Maschine fortsetzen oder einen Arbeitsspeicher-Snapshot einer verschlüsselten Maschine wiederherstellen. Sie können eine im angehaltenen Zustand befindliche verschlüsselte virtuelle Maschine mit einem Arbeitsspeicher-Snapshot zwischen ESXi-Hosts migrieren.

vSphere Virtual Machine Encryption und IPv6

Sie können vSphere Virtual Machine Encryption im reinen IPv6- oder gemischten Modus verwenden. Sie können den Schlüsselserver mit IPv6-Adressen konfigurieren. Sie können sowohl den vCenter Server als auch den Schlüsselserver nur mit IPv6-Adressen konfigurieren.

Einschränkungen beim Klonen in vSphere Virtual Machine Encryption

Für alle Schlüsselanbietertypen wird das Klonen bedingt unterstützt. Sie können die Verschlüsselungsschlüssel auf dem Klon ändern. Bestimmte Klonfunktionen können mit vSphere Virtual Machine Encryption nicht ausgeführt werden.

- Vollständige Klone werden unterstützt. Der Klon erbt den übergeordneten Verschlüsselungszustand und alle Schlüssel. Sie können den vollständigen Klon verschlüsseln, ihn zur Verwendung neuer Schlüssel erneut verschlüsseln oder entschlüsseln.

  Verknüpfte Klone werden unterstützt und der Klon erbt den übergeordneten Verschlüsselungsstatus einschließlich der Schlüssel. Sie können den verknüpften Klon nicht entschlüsseln oder einen verknüpften Klon nicht mit unterschiedlichen Schlüsseln erneut verschlüsseln.

  Hinweis Überprüfen Sie, ob andere Anwendungen verknüpfte Klone unterstützen. Beispiel: VMware Horizon® 7 unterstützt sowohl vollständige Klone als auch Instant Clones, aber keine verknüpften Klone.

- Instant Clone wird von allen Schlüsselanbietertypen unterstützt. Verschlüsselungsschlüssel können beim Klonen jedoch nicht geändert werden.
- Sie können eine verknüpfte Klon-VM aus einer verschlüsselten virtuellen Maschine erstellen. Die verknüpfte Klon-VM enthält dieselben Schlüssel. Sie können die Home-Dateien der verschlüsselten virtuellen Maschine eines verknüpften Klons erneut verschlüsseln. Sie können die Festplatten aber nicht erneut verschlüsseln.

Einschränkungen bei vSphere Native Key Provider

Bestimmte Vorgänge werden mit vSphere Native Key Provider nicht unterstützt.

- Sie können vSphere Native Key Provider nicht verwenden, um virtuelle Maschinen auf einem eigenständigen Host zu verschlüsseln. Der Host muss sich in einem Cluster befinden, um vSphere Native Key Provider verwenden zu können.
- Sie können einen Host, der virtuelle Maschinen enthält, die mit vSphere Native Key Provider verschlüsselt wurden, nur dann in einen anderen Cluster verschieben, wenn der Zielcluster denselben vSphere Native Key Provider enthält. (Die verschlüsselten virtuellen Maschinen auf dem verschobenen Host werden gesperrt, wenn die Verschlüsselungsschlüssel nicht vorhanden sind und der Zielcluster nicht denselben vSphere Native Key Provider aufweist.)
- Sie können eine von vSphere Native Key Provider verschlüsselte virtuelle Maschine nicht bei einem Legacy-Host registrieren, da vSphere Native Key Provider nicht unterstützt wird.

- Sie können eine von vSphere Native Key Provider verschlüsselte virtuelle Maschine nicht auf einem eigenständigen Host registrieren, da sich der Host in einem Cluster befinden muss.

Nicht unterstützte Festplattenkonfigurationen bei vSphere Virtual Machine Encryption

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

- RDM (Raw Device Mapping). vSphere Virtual Volumes (vVols) werden jedoch unterstützt.
- Multiwriter- oder freigegebene Festplatten (MSCS, WSFC oder Oracle RAC). Verschlüsselte VM-Home-Dateien werden bei Multiwriter-Festplatten unterstützt. Verschlüsselte virtuelle Festplatten werden bei Multiwriter-Festplatten nicht unterstützt. Wenn Sie versuchen, Multiwriter auf der Seite **Einstellungen bearbeiten** der virtuellen Maschine mit verschlüsselten virtuellen Festplatten auszuwählen, ist die Schaltfläche **OK** deaktiviert.

Verschiedene Einschränkungen bei vSphere Virtual Machine Encryption

Zu den anderen Funktionen, die nicht mit vSphere Virtual Machine Encryption funktionieren, gehören:

- vSphere ESXi Dump Collector
- Inhaltsbibliothek
  - Inhaltsbibliotheken unterstützen zwei Arten von Vorlagen: OVF- und VM-Vorlagen. Sie können eine verschlüsselte virtuelle Maschine nicht in den OVF-Vorlagentyp exportieren. Das OVF-Tool unterstützt keine verschlüsselten virtuellen Maschinen. Sie können verschlüsselte VM-Vorlagen mithilfe des VM-Vorlagentyps erstellen. Ab vSphere 8.0 enthält der Befehl `ovftool` eine Option zum Hinzufügen eines vTPM-Platzhalters zur OVF-Deskriptordatei. Bei der Bereitstellung einer virtuellen Maschine anhand einer solchen Vorlage erstellt vCenter Server ein vTPM mit eindeutigen geheimen Schlüsseln auf der virtuellen Zielmaschine. Weitere Informationen finden Sie im *Administratorhandbuch für vSphere Virtual Machine*.
- Software zum Sichern verschlüsselter virtueller Festplatten muss die VMware vSphere Storage API - Data Protection (VADP) verwenden, damit die Festplatten entweder im Hot-Add-Modus oder im NBD-Modus bei aktiviertem SSL gesichert werden können. Es werden jedoch nicht alle Sicherungslösungen unterstützt, die VADP für die Sicherung virtueller Festplatten verwenden. Weitere Informationen erhalten Sie von Ihrem Backupanbieter.
  - Lösungen für den VADP-SAN-Transportmodus werden für die Sicherung verschlüsselter virtueller Festplatten nicht unterstützt.
  - VADP-Hot-Add-Lösungen werden für verschlüsselte virtuelle Festplatten unterstützt. Die Sicherungssoftware muss die Verschlüsselung der Proxy-VM, die als Teil des Hot-Add-Sicherungsworkflows verwendet wird, unterstützen. Der Anbieter muss über die Rechte für **Verschlüsselungsvorgänge.Virtuelle Maschine verschlüsseln** verfügen.

  - Sicherungslösungen mithilfe der NBD-SSL-Transportmodi werden für die Sicherung verschlüsselter virtueller Festplatten unterstützt. Die Anwendung des Anbieters muss über die Rechte für **Verschlüsselungsvorgänge.Direkter Zugriff** verfügen.
- Sie können keine Ausgabe von einer verschlüsselten virtuellen Maschine an einen seriellen oder parallelen Port senden. Selbst wenn die Konfiguration scheinbar erfolgreich ist, wird die Ausgabe an eine Datei gesendet.
- vSphere Virtual Machine Encryption wird in VMware Cloud on AWS nicht unterstützt. Einzelheiten finden Sie unter *Verwalten des VMware Cloud on AWS-Datencenters.*

vSphere-Schlüsselpersistenz auf ESXi-Hosts

In vSphere 7.0 Update 2 und höher können verschlüsselte virtuelle Maschinen und virtuelle TPMs auch dann weiterhin optional funktionieren, wenn der Schlüsselserver vorübergehend offline oder nicht verfügbar ist. Die ESXi-Hosts können die Verschlüsselungsschlüssel beibehalten, um die Verschlüsselung und vTPM-Vorgänge fortzusetzen.

Vor vSphere 7.0 Update 2 ist es für verschlüsselte virtuelle Maschinen und vTPMs erforderlich, dass der Schlüsselserver immer verfügbar ist. In vSphere 7.0 Update 2 und höher können verschlüsselte Geräte auch dann funktionieren, wenn der Zugriff auf einen Schlüsselserver unterbrochen ist.

In vSphere 7.0 Update 3 und höher können verschlüsselte vSAN-Cluster auch dann funktionieren, wenn der Zugriff auf einen Schlüsselanbieter unterbrochen ist.

Hinweis Die Schlüsselpersistenz ist nicht erforderlich, wenn vSphere Native Key Provider verwendet wird. vSphere Native Key Provider ist sofort einsatzbereit und kann ohne Zugriff auf einen Schlüsselserver ausgeführt werden. Weitere Informationen finden Sie im folgenden Abschnitt „Schlüsselpersistenz und vSphere Native Key Provider“.

Funktionsweise der Schlüsselpersistenz auf ESXi-Hosts

Bei Verwendung eines Standardschlüsselanbieters verlässt sich der ESXi-Host auf vCenter Server, um Verschlüsselungsschlüssel zu verwalten. Wenn Sie einen vertrauenswürdigen Schlüsselanbieter verwenden, verlässt sich der ESXi-Host direkt auf die Trust Authority-Hosts für Schlüssel und vCenter Server ist nicht beteiligt. vSphere Native Key Provider verarbeitet Schlüssel unterschiedlich. Weitere Informationen finden Sie im nächsten Abschnitt.

Unabhängig vom Typ des Schlüsselanbieters erhält der ESXi-Host die Schlüssel anfänglich und behält sie im Schlüssel-Cache bei. Wenn der ESXi-Host neu gestartet wird, verliert er seinen Schlüssel-Cache. Der ESXi-Host fordert die Schlüssel dann erneut an, entweder vom Schlüsselserver (Standardschlüsselanbieter) oder vom Trust Authority-Host (vertrauenswürdiger Schlüsselanbieter). Wenn der ESXi-Host versucht, Schlüssel abzurufen, und der Schlüsselserver offline oder nicht erreichbar ist, können vTPMs und die Arbeitslastverschlüsselung nicht funktionieren. Bei Bereitstellungen im Edge-Stil, bei denen ein Schlüsselserver normalerweise nicht vor Ort bereitgestellt wird, kann ein Verlust der Konnektivität mit einem Schlüsselserver zu unnötigen Ausfallzeiten für verschlüsselte Arbeitslasten führen.

In vSphere 7.0 Update 2 und höher können verschlüsselte Arbeitslasten auch dann weiterhin funktionieren, wenn der Schlüsselserver offline oder nicht erreichbar ist. Wenn der ESXi-Host über ein TPM verfügt, werden die Verschlüsselungsschlüssel im TPM über Neustarts hinweg beibehalten. Selbst wenn ein ESXi-Host neu gestartet wird, muss der Host keine Verschlüsselungsschlüssel anfordern. Darüber hinaus können Verschlüsselungs- und Entschlüsselungsvorgänge fortgesetzt werden, wenn der Schlüsselserver nicht verfügbar ist, da die Schlüssel im TPM beibehalten wurden. Wenn also entweder der Schlüsselserver oder die Trust Authority-Hosts nicht verfügbar sind, können Sie je nach Schlüsselanbieter verschlüsselte Arbeitslasten weiterhin „ohne Schlüsselserver“ ausführen. Darüber hinaus können vTPMs auch dann weiterhin funktionieren, wenn der Schlüsselserver nicht erreichbar ist.

Schlüsselpersistenz und vSphere Native Key Provider

Wenn Sie einen vSphere Native Key Provider verwenden, generiert vSphere die Verschlüsselungsschlüssel, und es ist kein Schlüsselserver erforderlich. Die ESXi-Hosts erhalten einen KDK (Key Derivation Key), der zum Ableiten anderer Schlüssel verwendet wird. Nach dem Empfang des KDK und dem Generieren weiterer Schlüssel benötigen die ESXi-Hosts keinen Zugriff auf vCenter Server, um Verschlüsselungsvorgänge durchzuführen. Im Prinzip wird ein vSphere Native Key Provider immer „ohne Schlüsselserver“ ausgeführt.

Der KDK bleibt nach einem Neustart standardmäßig auf einem ESXi-Host erhalten, auch wenn vCenter Server nach dem Neustart des Hosts nicht verfügbar ist.

Sie können Schlüsselpersistenz mit vSphere Native Key Provider aktivieren, dies ist jedoch normalerweise nicht erforderlich. Die ESXi-Hosts haben vollständigen Zugriff auf vSphere Native Key Provider, sodass zusätzliche Schlüsselpersistenz redundant ist. Der Anwendungsfall für die Aktivierung der Schlüsselpersistenz mit vSphere Native Key Provider ist gegeben, wenn Sie auch einen Standardschlüsselanbieter (externer KMIP-Server) konfiguriert haben.

Vorgehensweise zum Einrichten von Schlüsselpersistenz

Informationen zum Aktivieren oder Deaktivieren der Schlüsselpersistenz finden Sie unter Aktivieren und Deaktivieren von Schlüsselpersistenz auf einem ESXi-Host.

Konfigurieren und Verwalten eines Standardschlüsselanbieters

7

Die Verwendung eines Standardschlüsselanbieters in Ihrer vSphere-Umgebung muss vorbereitet werden. Wenn Sie Ihre Umgebung eingerichtet haben, können Sie verschlüsselte virtuelle Maschinen und virtuelle Festplatten erstellen und vorhandene virtuelle Maschinen und Festplatten verschlüsseln.

Wenn Sie Ihre Umgebung für einen Standardschlüsselanbieter eingerichtet haben, können Sie mithilfe des vSphere Client verschlüsselte virtuelle Maschinen und virtuelle Festplatten erstellen und vorhandene virtuelle Maschinen und Festplatten verschlüsseln. Weitere Informationen hierzu finden Sie unter Kapitel 10 Verwenden der Verschlüsselung in Ihrer vSphere-Umgebung.

Unter Verwendung der API und der crypto-util-Befehlszeilenschnittstelle können Sie zusätzliche Aufgaben ausführen. Die API-Dokumentation finden Sie im *Programmierhandbuch zum vSphere Web Services SDK*. Informationen zu diesem Tool finden Sie der `crypto-util`-Befehlszeilenhilfe.

Lesen Sie als Nächstes die folgenden Themen:

- Definition eines Standardschlüsselanbieters
- Einrichten des Standardschlüsselanbieters
- Einrichten separater Schlüsselanbieter für verschiedene Benutzer
- Löschen eines Standardschlüsselanbieters

Definition eines Standardschlüsselanbieters

Sie können einen Standardschlüsselanbieter verwenden, um Verschlüsselungsaufgaben für virtuelle Maschinen durchzuführen.

In vSphere ruft ein Standardschlüsselanbieter die Verschlüsselungsschlüssel direkt von einem Schlüsselserver ab, und der vCenter Server verteilt die Schlüssel an die notwendigen ESXi-Hosts in einem Datencenter.

Sie können separate Standardschlüsselanbieter für verschiedene Benutzer hinzufügen und den Standardschlüsselanbieter festlegen.

Standardschlüsselanbieter – Anforderungen

- vSphere 6.5 oder höher
- Ein externer Schlüsselserver (KMS)

Der Schlüsselserver muss den KMIP 1.1-Standard (Key Management Interoperability Protocol) unterstützen. Weitere Informationen finden Sie unter *vSphere-Kompatibilitätstabellen*.

Informationen über von VMware zertifizierte Schlüsselserver-Anbieter finden Sie im VMware-Kompatibilitätshandbuch unter „Plattform und Computing“. Wenn Sie „Kompatibilitätshandbücher“ auswählen, können Sie die KMS-Kompatibilitätsdokumentation öffnen. Diese Dokumentation wird häufig aktualisiert.

Standardschlüsselanbieter – Berechtigungen

Standardschlüsselanbieter verwenden **Cryptographer.***-Berechtigungen Weitere Informationen hierzu finden Sie unter Rechte für Verschlüsselungsvorgänge.

Einrichten des Standardschlüsselanbieters

Bevor Sie mit den Verschlüsselungsaufgaben für virtuelle Maschinen beginnen können, müssen Sie den Standardschlüsselanbieter einrichten.

Zum Einrichten eines Standardschlüsselanbieters gehört das Hinzufügen des Schlüsselanbieters und das Einrichten einer Vertrauensstellung mit dem Schlüsselserver. Wenn Sie einen Schlüsselanbieter hinzufügen, werden Sie aufgefordert, ihn als Standardwert festzulegen. Sie können den Standardschlüsselanbieter explizit ändern. vCenter Server stellt Schlüssel über den Standardschlüsselanbieter bereit.

Hinweis Was zuvor in vSphere 6.5 und 6.7 als KMS-Cluster bezeichnet wurde, heißt nun Schlüsselanbieter.

Hinzufügen eines Standardschlüsselanbieters mithilfe des vSphere Client

Sie können Ihrem vCenter Server-System über den vSphere Client oder über die öffentliche API einen Standardschlüsselanbieter hinzufügen.

Mithilfe des vSphere Client können Sie Ihrem vCenter Server-System einen Standardschlüsselanbieter hinzufügen und eine Vertrauensstellung zwischen dem Schlüsselserver und vCenter Server einrichten.

- Sie können mehrere Schlüsselserver desselben Anbieters hinzufügen.
- Wenn Ihre Umgebung Lösungen anderer Anbieter unterstützt, können Sie mehrere Schlüsselanbieter hinzufügen.
- Wenn Ihre Umgebung mehrere Schlüsselanbieter enthält und Sie den Standardschlüsselanbieter löschen, müssen Sie explizit einen anderen Standardschlüsselanbieter festlegen.
- Sie können den Schlüsselserver mit IPv6-Adressen konfigurieren.
  - Das vCenter Server-System und der Schlüsselserver können nur mit IPv6-Adressen konfiguriert werden.

Voraussetzungen

- Stellen Sie sicher, dass der Schlüsselserver (KMS) im *VMware-Kompatibilitätshandbuch für Schlüsselverwaltungsserver (KMS)* aufgeführt und mit KMIP 1.1 kompatibel ist und dass er als Foundry und Server für symmetrische Schlüssel dienen kann.
- Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen: **Verschlüsselungsvorgänge.Schlüsselserver verwalten**
- Stellen Sie Hochverfügbarkeit für den Schlüsselserver sicher. Bei einem Abbruch der Verbindung zum Schlüsselserver, beispielsweise bei einem Stromausfall oder einer Notfallwiederherstellung, ist ein Zugriff auf verschlüsselte virtuelle Maschinen nicht mehr möglich.

  Hinweis In vSphere 7.0 Update 2 und höher können verschlüsselte virtuelle Maschinen und virtuelle TPMs auch dann weiterhin funktionieren, wenn der Schlüsselserver vorübergehend offline oder nicht verfügbar ist. Weitere Informationen hierzu finden Sie unter vSphere-Schlüsselpersistenz auf ESXi-Hosts.

- Führen Sie eine sorgfältige Prüfung der Infrastrukturabhängigkeiten auf dem Schlüsselserver durch. Bestimmte KMS-Lösungen werden als virtuelle Appliances bereitgestellt, wodurch eine Abhängigkeitsschleife oder ein anderes Verfügbarkeitsproblem aufgrund einer schlechten Platzierung der KMS-Appliance auftreten kann.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.
4. Klicken Sie auf **Standardschlüsselanbieter hinzufügen** und geben Sie die Daten des Schlüsselanbieters ein.

Option	Wert
Name	Name des Schlüsselanbieters. Jeder logische Schlüsselanbieter muss unabhängig von seinem Typ (Standard-, vertrauenswürdiger und nativer Schlüsselanbieter) über einen eindeutigen Namen in allen vCenter Server-Systemen verfügen. Weitere Informationen finden Sie unter Benennung des Schlüsselanbieters.
KMS	Alias für den Schlüsselserver (KMS).
Adresse	IP-Adresse oder FQDN des Schlüsselservers.
Port	Port, auf dem vCenter Server eine Verbindung zum Schlüsselserver herstellt.
Proxyserver	Optionale Proxyserveradresse für die Verbindung mit dem Schlüsselserver.
Proxyport	Optionaler Proxyport für die Verbindung mit dem Schlüsselserver.

Option	Wert
Benutzername	Bestimmte Schlüsselserveranbieter lassen zu, dass Benutzer Verschlüsselungsschlüssel isolieren, die von verschiedenen Benutzern oder Gruppen verwendet werden, indem sie einen Benutzernamen und ein Kennwort angeben. Geben Sie nur dann einen Benutzernamen an, wenn Ihr Schlüsselserver diese Funktion unterstützt und Sie die Funktion verwenden möchten.
Kennwort	Bestimmte Schlüsselserveranbieter lassen zu, dass Benutzer Verschlüsselungsschlüssel isolieren, die von verschiedenen Benutzern oder Gruppen verwendet werden, indem sie einen Benutzernamen und ein Kennwort angeben. Geben Sie nur dann ein Kennwort an, wenn Ihr Schlüsselserver diese Funktion unterstützt und Sie die Funktion verwenden möchten.

Sie können auf **KMS hinzufügen** klicken, um weitere Schlüsselserver hinzuzufügen.

5 Klicken Sie auf **Schlüsselanbieter hinzufügen**.

6 Klicken Sie auf **Vertrauenswürdigkeit**.

vCenter Server fügt den Schlüsselanbieter hinzu und zeigt den Status als „Verbunden“ an.

Nächste Schritte

Weitere Informationen hierzu finden Sie unter Herstellen einer vertrauenswürdigen Standardschlüsselanbieter-Verbindung durch den Austausch von Zertifikaten.

Herstellen einer vertrauenswürdigen Standardschlüsselanbieter-Verbindung durch den Austausch von Zertifikaten

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

Voraussetzungen

Fügen Sie den Standardschlüsselanbieter hinzu.

Verfahren

1 Navigieren Sie zum vCenter Server.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus.

Der KMS für den Schlüsselanbieter wird angezeigt.

4 Wählen Sie den KMS aus.

5 Wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.

6 Wählen Sie die entsprechende Option für den Server aus und befolgen Sie die entsprechenden Schritte.

Option	Informationen hierzu finden Sie unter
CA-Root-Zertifikat von vCenter Server	Verwenden der Option „Root-CA-Zertifikat“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.
vCenter Server-Zertifikat	Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.
Zertifikat und privaten Schlüssel hochladen	Verwenden der Option „Zertifikat und privaten Schlüssel hochladen“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.
Neue Zertifikatssignieranforderung	Verwenden der Option „Neue Zertifikatssignierungsanforderung“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.

Verwenden der Option „Root-CA-Zertifikat“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass Sie das Root-CA-Zertifikat auf den KMS hochladen. Alle von Ihrer Root-Zertifizierungsstelle signierten Zertifikate werden dann von diesem KMS als vertrauensvoll angesehen.

Das von der vSphere VM-Verschlüsselung verwendete Root-CA-Zertifikat ist ein selbst signiertes Zertifikat, das in einem separaten Speicher im VECS (VMware Endpoint Certificate Store) auf dem vCenter Server-System gespeichert wird.

Hinweis Generieren Sie ein Root-CA-Zertifikat nur dann, wenn Sie vorhandene Zertifikate ersetzen möchten. Wenn Sie das tun, werden andere von dieser Root-Zertifizierungsstelle signierten Zertifikate ungültig. Sie können ein neues Root-CA-Zertifikat als Teil dieses Workflows generieren.

Verfahren

1 Navigieren Sie zum vCenter Server.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der Schlüsselserver (KMS) für den Schlüsselanbieter wird angezeigt.

4 Wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.

5 Wählen Sie **vCenter-Zertifikat der Stammzertifizierungsstelle herunterladen** aus und klicken Sie auf **Weiter**.

   Im Dialogfeld „Root-CA-Zertifikat herunterladen“ steht bereits das Root-Zertifikat, das vCenter Server zur Verschlüsselung verwendet. Dieses Zertifikat wird in VECS gespeichert.

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

7 Folgen Sie den Anweisungen des KMS-Anbieters, um das Zertifikat auf sein System hochzuladen.

Hinweis Einige KMS-Anbieter verlangen, dass der KMS-Anbieter den KMS neu startet, um das von Ihnen hochgeladene Root-Zertifikat abzuholen.

Nächste Schritte

Schließen Sie den Zertifikatsaustausch ab. Weitere Informationen hierzu finden Sie unter Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass Sie das vCenter Server-Zertifikat auf den KMS hochladen. Nach dem Upload akzeptiert der KMS den Datenverkehr, der von einem System mit diesem Zertifikat stammt.

vCenter Server generiert ein Zertifikat, um Verbindungen mit dem KMS zu schützen. Das Zertifikat wird in einem getrennten Keystore im VMware Endpoint Certificate Store (VECS) auf dem vCenter Server-System gespeichert.

Verfahren

1 Navigieren Sie zum vCenter Server.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

Der Schlüsselserver (KMS) für den Schlüsselanbieter wird angezeigt.

4 Wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.

5 Wählen Sie **vCenter-Zertifikat** aus und klicken Sie auf **Weiter**.

Im Dialogfeld „Zertifikat herunterladen“ steht bereits das Root-Zertifikat, das vCenter Server zur Verschlüsselung verwendet. Dieses Zertifikat wird in VECS gespeichert.

Hinweis Generieren Sie kein neues Zertifikat, es sei denn, Sie möchten vorhandene Zertifikate ersetzen.

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

7 Folgen Sie den Anweisungen des KMS-Anbieters, um das Zertifikat auf den KMS hochzuladen.

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

Verwenden der Option „Zertifikat und privaten Schlüssel hochladen“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass Sie das KMS-Serverzertifikat und den privaten Schlüssel in das vCenter Server-System hochladen.

Einige KMS-Anbieter generieren ein Zertifikat und einen privaten Schlüssel für die Verbindung und stellen Ihnen diese zur Verfügung. Sobald Sie die Dateien hochgeladen haben, wird Ihre vCenter Server-Instanz vom KMS für vertrauenswürdig erachtet.

Voraussetzungen

- Fordern Sie ein Zertifikat und einen privaten Schlüssel vom KMS-Anbieter an. Bei den Dateien handelt es sich um X509-Dateien im PEM-Format.

Verfahren

1. Navigieren Sie zum vCenter Server.
2. Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.
3. Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der Schlüsselserver (KMS) für den Schlüsselanbieter wird angezeigt.
4. Wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.
5. Wählen Sie **KMS-Zertifikat und privater Schlüssel** aus und klicken Sie auf **Weiter**.
6. Fügen Sie das Zertifikat, das Sie vom KMS-Anbieter erhalten haben, in das obere Textfeld ein oder klicken Sie auf **Datei hochladen**, um die Zertifikatsdatei hochzuladen.
7. Fügen Sie die Schlüsseldatei in das untere Textfeld ein oder klicken Sie auf **Datei hochladen**, um die Schlüsseldatei hochzuladen.
8. Klicken Sie auf **Vertrauenswürdige Verbindung einrichten**.

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

Verwenden der Option „Neue Zertifikatssignierungsanforderung“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass vCenter Server eine Zertifikatsignierungsanforderung (CSR) generiert und an den KMS übermittelt. Der KMS signiert die Zertifikatsignierungsanforderung und sendet das signierte Zertifikat zurück. Sie können das signierte Zertifikat auf den vCenter Server hochladen.

Bei der Verwendung der Option **Neue Zertifikatsignierungsanforderung** handelt es sich um einen Vorgang mit zwei Schritten. Zuerst generieren Sie die Zertifikatsignierungsanforderung und senden diese an den KMS-Anbieter. Anschließend laden Sie das signierte Zertifikat, das Sie vom KMS-Anbieter erhalten, auf den vCenter Server hoch.

Verfahren

1. Navigieren Sie zum vCenter Server.
2. Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.
3. Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der Schlüsselserver (KMS) für den Schlüsselanbieter wird angezeigt.
4. Wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.
5. Wählen Sie **Neue Zertifikatsignierungsanforderung (CSR)** aus und klicken Sie auf **Weiter**.
6. Kopieren Sie im Dialogfeld das vollständige Zertifikat aus dem Textfeld in die Zwischenablage oder laden es als Datei herunter.

   Klicken Sie auf die Schaltfläche **Neue CSR generieren** des Dialogfelds nur dann, wenn Sie explizit eine Zertifikatsignierungsanforderung generieren möchten.
7. Folgen Sie den Anweisungen Ihres KMS-Anbieters zum Einreichen der Zertifikatsignierungsanforderung.
8. Wenn Sie das signierte Zertifikat vom KMS-Anbieter erhalten, klicken Sie erneut auf **Schlüsselanbieter**, wählen Sie den Schlüsselanbieter aus und wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **Signiertes CSR-Zertifikat hochladen** aus.
9. Fügen Sie das signierte Zertifikat in das untere Textfeld ein oder klicken Sie auf **Datei hochladen** und laden Sie die Datei hoch. Klicken Sie anschließend auf **Hochladen**.

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Siehe Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter

Sofern Sie im Dialogfeld **Standardschlüsselanbieter hinzufügen** nicht aufgefordert wurden, eine vertrauenswürdige Verbindung mit dem KMS herzustellen, müssen Sie die vertrauenswürdige Verbindung nach erfolgtem Zertifikatsaustausch explizit einrichten.

Eine vertrauenswürdige Verbindung zwischen vCenter Server und dem KMS-Server können Sie einrichten, indem Sie entweder den KMS-Server als vertrauenswürdig einstufen oder ein KMS-Zertifikat hochladen. Die folgenden beiden Möglichkeiten stehen zur Verfügung:

- Legen Sie das Zertifikat mithilfe der Option **KMS-Zertifikat hochladen** explizit als vertrauenswürdig fest.
- Laden Sie ein untergeordnetes KMS-Zertifikat oder das KMS-CA-Zertifikat in vCenter Server hoch, indem Sie die Option **vCenter für KMS vertrauenswürdig machen** verwenden.

Hinweis Wenn Sie das CA-Root-Zertifikat oder das Zwischen-CA-Zertifikat hochladen, vertraut vCenter Server allen Zertifikaten, die von dieser Zertifizierungsstelle signiert wurden. Um hohe Sicherheit zu gewährleisten, laden Sie ein untergeordnetes Zertifikat oder ein Zwischen-CA-Zertifikat hoch, das vom KMS-Anbieter kontrolliert wird.

Verfahren

1. Navigieren Sie zum vCenter Server.
2. Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.
3. Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der Schlüsselserver (KMS) für den Schlüsselanbieter wird angezeigt.
4. Wählen Sie den KMS aus.
5. Wählen Sie eine der folgenden Optionen im Dropdown-Menü **Vertrauensstellung herstellen** aus.

Option	Aktion
vCenter für KMS vertrauenswürdig machen	Klicken Sie im daraufhin angezeigten Dialogfeld auf **Vertrauenswürdigkeit**.
KMS-Zertifikat hochladen	a Fügen Sie im angezeigten Dialogfeld entweder das Zertifikat ein oder klicken Sie auf **Datei hochladen** und navigieren Sie zur Zertifikatsdatei. b Klicken Sie auf **Hochladen**.

Einrichten separater Schlüsselanbieter für verschiedene Benutzer

Sie können in Ihrer Umgebung mehrere Schlüsselanbieter für verschiedene Benutzer der gleichen KMS-Instanz einrichten. Mehrere Schlüsselanbieter sind hilfreich, wenn Sie beispielsweise

verschiedenen Abteilungen in Ihrem Unternehmen Zugriff auf unterschiedliche Sätze von Verschlüsselungsschlüsseln erteilen möchten.

Sie können mehrere Schlüsselanbieter für denselben KMS verwenden, um Schlüssel zu trennen. Das Vorhandensein getrennter Schlüsselsätze ist im Fall verschiedener Geschäftsbereiche oder Kunden entscheidend.

Hinweis Nicht alle KMS-Anbieter unterstützen mehrere Benutzer.

Voraussetzungen

Richten Sie die Verbindung mit dem KMS ein.

Verfahren

1. Erstellen Sie zwei Benutzer mit entsprechenden Benutzernamen und Kennwörtern im KMS, z. B. C1 und C2.
2. Melden Sie sich bei vCenter Server an und erstellen Sie den ersten Schlüsselanbieter.
3. Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie Informationen an, die für den ersten Benutzer eindeutig sind.
4. Erstellen Sie einen zweiten Schlüsselanbieter und fügen Sie den gleichen KMS hinzu, aber verwenden Sie den zweiten Benutzernamen und das zweite Kennwort (C2).

Ergebnisse

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

Löschen eines Standardschlüsselanbieters

Sie können den vSphere Client zum Löschen eines Standardschlüsselanbieters aus vCenter Server verwenden.

Nachdem Sie einen Standardschlüsselanbieter gelöscht haben, werden virtuelle Maschinen, die über vTPMs verfügen oder verschlüsselt sind, weiterhin ausgeführt. Wenn Sie den ESXi-Host neu starten, wechseln die zugehörigen verschlüsselten VMs in den gesperrten Modus. Nachdem Sie die Registrierung dieser virtuellen Maschinen aufgehoben haben, wechseln sie in den gesperrten Modus, wenn Sie versuchen, sie erneut zu registrieren. Die einzige Möglichkeit zum Entsperren der virtuellen Maschinen besteht in der Wiederherstellung des vorigen Standardschlüsselanbieters.

Voraussetzungen

Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**

Verschlüsseln Sie vor dem Löschen eines Standardschlüsselanbieters alle verschlüsselten virtuellen Maschinen und Datenspeicher, die mithilfe dieses Schlüsselanbieters verschlüsselt wurden, erneut mit einem anderen Schlüsselanbieter. Weitere Informationen finden Sie unter Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe des vSphere Client.

Behalten Sie zudem eine Sicherung des Standardschlüsselanbieters bei für den Fall, dass Sie eine verschlüsselte virtuelle Maschine nach dem Löschen des Schlüsselanbieters erneut verschlüsseln müssen.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.
4. Wählen Sie den Standardschlüsselanbieter aus, den Sie löschen möchten.
5. Klicken Sie auf **Löschen**.
6. Lesen Sie die Warnmeldung und ziehen Sie den Schieberegler ganz nach rechts.
7. Klicken Sie auf **Löschen**.

Ergebnisse

Der Standardschlüsselanbieter wird aus dem vCenter Server entfernt.

Konfigurieren und Verwalten eines vSphere Native Key Providers

8

Die Verwendung eines VMware vSphere® Native Key Providers™ in Ihrer vSphere-Umgebung muss vorbereitet werden. Nach dem Konfigurieren des vSphere Native Key Providers können Sie vTPMs (virtual Trusted Platform Modules) auf Ihren virtuellen Maschinen erstellen.

Nach der Einrichtung Ihrer Umgebung für einen vSphere Native Key Provider können Sie den vSphere Client und die API zum Erstellen von vTPMs verwenden. Bei Erwerb der VMware vSphere® Enterprise Plus Edition™ können Sie auch virtuelle Maschinen und Festplatten sowie vorhandene virtuelle Maschinen und Festplatten verschlüsseln.

 (Konfigurieren eines vSphere Native Key Providers)

Lesen Sie als Nächstes die folgenden Themen:

- vSphere Native Key Provider – Übersicht
- vSphere Native Key Provider – Prozessablauf
- Konfigurieren eines vSphere Native Key Providers
- Sichern eines vSphere Native Key Providers
- Wiederherstellen eines vSphere Native Key Providers
- Aktualisieren eines vSphere Native Key Providers
- Löschen eines vSphere Native Key Providers

vSphere Native Key Provider – Übersicht

In vSphere 7.0 Update 2 und höher können Sie den integrierten vSphere Native Key Provider verwenden, um Verschlüsselungstechnologien wie virtuelle TPMs (vTPM) zu aktivieren.

vSphere Native Key Provider ist in allen vSphere Editionen enthalten und benötigt keinen externen Schlüsselserver – in der Branche auch als Schlüsselmanagementserver (Key Management Server oder KMS) bezeichnet. Sie können auch vSphere Native Key Provider für vSphere Virtual Machine Encryption verwenden. Dazu müssen Sie jedoch die VMware vSphere® Enterprise Plus Edition™ erwerben.

Was ist vSphere Native Key Provider?

Bei einem Standardschlüsselanbieter oder vertrauenswürdigen Schlüsselanbieter müssen Sie einen externen Schlüsselserver konfigurieren. In einer Standardschlüsselanbieter-Konfiguration ruft vCenter Server Schlüssel vom externen Schlüsselserver ab und verteilt sie an die ESXi-Hosts. In der Konfiguration eines vertrauenswürdigen Schlüsselanbieters (vSphere Trust Authority) rufen die vertrauenswürdigen ESXi-Hosts die Schlüssel direkt ab.

Mit vSphere Native Key Provider benötigen Sie keinen externen Schlüsselserver mehr. vCenter Server generiert einen primären Schlüssel, den so genannten Key Derivation Key (KDK), und leitet ihn an alle ESXi-Hosts im Cluster weiter. Daraufhin generieren die ESXi-Hosts Datenverschlüsselungsschlüssel (auch wenn sie nicht mit vCenter Server verbunden sind), um Sicherheitsfunktionalität wie vTPMs zu aktivieren. Die vTPM-Funktionalität ist in allen vSphere Editionen enthalten. Um einen vSphere Native Key Provider für vSphere Virtual Machine Encryption zu verwenden, müssen Sie die vSphere Enterprise Plus Edition erwerben. vSphere Native Key Provider kann mit einer vorhandenen Schlüsselserverinfrastruktur koexistieren.

vSphere Native Key Provider:

- Aktiviert die Verwendung von vTPMs, vSphere Virtual Machine Encryption und die vSAN-Verschlüsselung ruhender Daten, wenn Sie keinen externen Schlüsselserver benötigen oder möchten.
- Funktioniert nur mit VMware-Infrastrukturprodukten.
- Bietet keine externe Interoperabilität, KMIP-Unterstützung, Hardware-Sicherheitsmodule oder andere Funktionen, die ein herkömmlicher, externer Schlüsselserver von Drittanbietern für die Interoperabilität oder die Einhaltung behördlicher Auflagen anbieten kann. Wenn Ihre Organisation diese Funktionalität für Nicht-VMware-Produkte und -Komponenten benötigt, installieren Sie den herkömmlichen Schlüsselserver eines Drittanbieters.
- Hilft bei der Abwicklung der Anforderungen von Organisationen, die einen externen Schlüsselserver entweder nicht verwenden können oder nicht verwenden möchten.
- Verbessert die Methoden der Datenbereinigung und der Systemwiederverwendung, indem die frühere Verwendung von Verschlüsselungstechnologien auf schwer zu bereinigenden Medien wie Flash und SSD aktiviert wird.
- Stellt einen Übergangspfad zwischen Schlüsselanbietern bereit. vSphere Native Key Provider ist mit dem VMware-Standardschlüsselanbieter und dem vertrauenswürdigen vSphere Trust Authority-Schlüsselanbieter kompatibel.
- Funktioniert mit mehreren vCenter Server-Systemen, die eine Konfiguration im erweiterten verknüpften Modus oder eine vCenter Server-Hochverfügbarkeitskonfiguration verwenden.
- Kann verwendet werden, um vTPM in allen Editionen von vSphere zu aktivieren und virtuelle Maschinen mit dem Kauf der vSphere Enterprise Plus Edition zu verschlüsseln, die vSphere Virtual Machine Encryption enthält. vSphere Virtual Machine Encryption funktioniert mit vSphere Native Key Provider wie bei VMware und vertrauenswürdigen Schlüsselanbietern.

- Kann verwendet werden, um vSAN-Verschlüsselung ruhender Daten mithilfe einer entsprechenden vSAN-Lizenz zu aktivieren.
- Kann ein Trusted Platform Module (TPM) 2.0 verwenden, um die Sicherheit zu erhöhen, wenn eins auf einem ESXi-Host installiert ist. Sie können vSphere Native Key Provider auch so konfigurieren, dass er nur für Hosts verfügbar ist, auf denen ein TPM 2.0 installiert ist. Wenn Sie ein TPM verwenden, muss es sich um TPM 2.0 handeln. vSphere Native Key Provider unterstützt TPM 1.2 nicht.

Hinweis Ein ESXi-Host benötigt kein TPM 2.0 zur Verwendung eines vSphere Native Key Providers. Ein TPM 2.0 bietet jedoch erweiterte Sicherheit.

Wie bei allen Sicherheitslösungen sollten Sie das Systemdesign, Implementierungsüberlegungen und Konflikte bei der Verwendung des nativen Schlüsselanbieters berücksichtigen. Beispielsweise vermeidet ESXi-Schlüsselpersistenz die Abhängigkeit von einem Schlüsselserver, der immer verfügbar ist. Da die Schlüsselpersistenz jedoch die kryptografischen Informationen des nativen Schlüsselanbieters auf den Clusterhosts speichert, sind Sie weiterhin gefährdet, wenn böswillige Akteure die ESXi-Hosts selbst stehlen. Da die Umgebungen unterschiedlich sind, sollten Sie Ihre Sicherheitskontrollen entsprechend den gesetzlichen und sicherheitstechnischen Anforderungen, den betrieblichen Anforderungen und der Risikotoleranz Ihres Unternehmens bewerten und implementieren.

Weitere Informationen zum vSphere Native Key Provider finden Sie unter https://core.vmware.com/native-key-provider.

vSphere Native Key Provider – Anforderungen

Um vSphere Native Key Provider zu verwenden, müssen Sie Folgendes ausführen:

- Stellen Sie sicher, dass sowohl das vCenter Server-System als auch ESXi-Hosts vSphere 7.0 Update 2 oder höher ausführen.
- Konfigurieren Sie die ESXi-Hosts in einem Cluster.
- Obwohl dies nicht erforderlich ist, wird empfohlen, möglichst identische ESXi-Hosts zu verwenden, einschließlich TPMs. Clusterverwaltung und Funktionsaktivierung werden durch identische Clusterhosts stark vereinfacht.
- Konfigurieren Sie die dateibasierte vCenter Server-Sicherung und -Wiederherstellung und speichern Sie die Backups auf sichere Weise, da sie den KDK (Key Derivation Key) enthalten. Weitere Informationen finden Sie im Thema zur vCenter Server-Sicherung und -Wiederherstellung in der *Installation und Einrichtung von vCenter Server*-Dokumentation.

Um vSphere Virtual Machine Encryption oder vSAN-Verschlüsselung mit vSphere Native Key Provider durchführen zu können, müssen Sie diejenigen Editionen dieser Produkte erwerben, die die entsprechende Lizenz enthalten.

vSphere Native Key Provider und erweiterter verknüpfter Modus

Sie können einen einzelnen vSphere Native Key Provider konfigurieren, der über vCenter Server-Systeme hinweg gemeinsam nutzbar ist, die in einer Konfiguration des erweiterten verknüpften Modus konfiguriert sind. Die allgemeinen Schritte in diesem Szenario:

1 Erstellen des vSphere Native Key Providers auf einem der vCenter Server-Systeme

2 Sichern des nativen Schlüsselanbieters auf dem vCenter Server, auf dem er erstellt wurde

3 Exportieren des nativen Schlüsselanbieters

4 Wiederherstellen des nativen Schlüsselanbieters auf den anderen vCenter Server-Systemen in der Konfiguration mit erweitertem verknüpftem Modus (siehe Wiederherstellen eines vSphere Native Key Providers mithilfe des vSphere Client)

vSphere Native Key Provider – Rechte

Wie bei Standardschlüsselanbietern und vertrauenswürdigen Schlüsselanbietern verwendet vSphere Native Key Provider den **Cryptographer.***-Berechtigungen Darüber hinaus verwendet vSphere Native Key Provider zum Auflisten der vSphere Native Key Provider das Recht **Cryptographer.ReadKeyServersInfo**, das speziell für vSphere Native Key Provider gilt. Weitere Informationen hierzu finden Sie unter Rechte für Verschlüsselungsvorgänge.

vSphere Native Key Provider – Alarme

Sie müssen einen vSphere Native Key Provider sichern. Wenn ein vSphere Native Key Provider nicht gesichert wird, generiert vCenter Server einen Alarm. Wenn Sie den vSphere Native Key Provider, für den ein Alarm generiert wurde, sichern, setzt vCenter Server den Alarm zurück. Standardmäßig überprüft vCenter Server einmal täglich, ob vSphere Native Key Provider gesichert wurden. Sie können das Prüfintervall ändern, indem Sie die Option `vpxd.KMS.backupCheckInterval` ändern.

vSphere Native Key Provider – regelmäßige Standardisierungsprüfung

vCenter Server Prüft regelmäßig, ob die vSphere Native Key Provider-Konfiguration auf den vCenter Server- und ESXi-Hosts übereinstimmt. Wenn sich ein Hoststatus ändert, z. B. wenn Sie einen Host zum Cluster hinzufügen, weicht die Konfiguration des Schlüsselanbieters auf dem Cluster von der Konfiguration auf dem Host ab. Wenn die Konfiguration (keyID) auf dem Host abweicht, aktualisiert vCenter Server die Konfiguration des Hosts automatisch. Es ist kein manueller Eingriff erforderlich.

Standardmäßig überprüft vCenter Server die Konfiguration alle fünf Minuten. Sie können das Intervall mit der Option `vpxd.KMS.remediationInterval` ändern.

Verwenden von vSphere Native Key Provider mit einer Site für die Notfallwiederherstellung

Sie können vSphere Native Key Provider mit einer Site für die Notfallwiederherstellung als Backup verwenden. Durch den Import des vSphere Native Key Provider-Backups vom primären vCenter Server zum vCenter Server-Backup am Disaster Recovery-Standort kann dieser Cluster Ihre verschlüsselten virtuellen Maschinen entschlüsseln und ausführen.

Testen Sie immer Ihre Notfallwiederherstellungslösung. Verlassen Sie sich nicht darauf, dass Ihre Lösung funktioniert, ohne testweise eine Wiederherstellung durchzuführen. Stellen Sie sicher, dass eine Kopie der vSphere Native Key Provider-Sicherung auch für Ihre DR-Site verfügbar ist.

Nicht unterstützte Funktionen in vSphere Native Key Provider

Aktuell bietet vSphere Native Key Provider keine Unterstützung für Folgendes:

- FCD-Verschlüsselung (First Class Disk)

Migrieren von virtuellen Maschinen mithilfe von vSphere Native Key Provider über nicht verknüpfte vCenter Server-Systeme hinweg

Zu den allgemeinen Schritten zum Migrieren einer verschlüsselten oder mit einem vTPM über vSphere Native Key Provider aktivierten virtuellen Maschine von einem nicht verknüpften vCenter Server-System zu einem anderen gehören:

1. Wiederherstellen des vSphere Native Key Provider auf dem vCenter Server-System, das als Migrationsziel vorgesehen ist.
2. Migrieren der virtuellen Maschine mithilfe von vMotion.

vSphere Native Key Provider – Prozessablauf

Das Verstehen der vSphere Prozessabläufe von vSphere Native Key Provider ist wichtig, um zu erfahren, wie Sie Ihren vSphere Native Key Provider konfigurieren und verwalten können.

Sie können den integrierten vSphere Native Key Provider verwenden, um verschlüsselungsbasierte virtuelle TPMs (vTPM) zu aktivieren. vSphere Native Key Provider ist in allen vSphere Editionen enthalten und erfordert keinen externen Schlüsselserver (KMS). Um einen vSphere Native Key Provider für vSphere Virtual Machine Encryption zu verwenden, müssen Sie die vSphere Enterprise+ Edition erwerben.

Konfigurieren von vSphere Native Key Provider

Die Konfiguration von vSphere Native Key Provider umfasst die folgenden grundlegenden Vorgänge:

1. Ein Benutzer mit den entsprechenden Administratorrechten generiert mit vSphere Client einen vSphere Native Key Provider auf einem vCenter Server.

2 Daraufhin konfiguriert vCenter Server dann den vSphere Native Key Provider für alle ESXi-Host-Cluster.

   In diesem Schritt pusht vCenter Server einen primären Schlüssel an alle ESXi-Hosts im Cluster. Ebenso wird die Änderung an die Hosts im Cluster übertragen, wenn Sie einen vSphere Native Key Provider aktualisieren oder löschen.

3 Benutzer mit den entsprechenden kryptografischen Rechten erstellen vTPMs und verschlüsselte virtuelle Maschinen (vorausgesetzt, Sie haben die vSphere Enterprise+ Edition erworben).

   Weitere Informationen finden Sie unter Kapitel 10 Verwenden der Verschlüsselung in Ihrer vSphere-Umgebung und Kapitel 11 Sichern von virtuellen Maschinen mit Virtual Trusted Platform Module.

Prozessablauf bei der vSphere Native Key Provider-Verschlüsselung

Informationen dazu, wie verschiedene Komponenten interagieren, um eine Verschlüsselungsaufgabe mit vSphere Native Key Provider durchzuführen, finden Sie unter Prozessablauf bei der vSphere Native Key Provider-Verschlüsselung.

Konfigurieren eines vSphere Native Key Providers

Ein Schlüsselanbieter ist für die Durchführung von Verschlüsselungsaufgaben erforderlich. Sie können den vSphere Client zum Konfigurieren des vSphere Native Key Providers unter vCenter Server verwenden.

vSphere 7.0 Update 2 und höhere Versionen enthalten einen Schlüsselanbieter mit der Bezeichnung „vSphere Native Key Provider“. vSphere Native Key Provider ermöglicht die Verwendung verschlüsselungsbezogener Funktionen, ohne dass ein externer Schlüsselserver (KMS) erforderlich ist. vCenter Server ist zunächst nicht mit einem vSphere Native Key Provider konfiguriert. Sie müssen einen vSphere Native Key Provider manuell konfigurieren.

Ein ESXi-Host benötigt kein TPM 2.0 zur Verwendung eines vSphere Native Key Providers. Ein TPM 2.0 bietet jedoch erweiterte Sicherheit.

Hinweis Wenn Sie einen vSphere Native Key Provider konfigurieren, stehen die Schlüsselanbieter auf allen Clustern für den vCenter Server zur Verfügung, auf dem Sie sie konfigurieren. Folglich haben alle mit dem vCenter Server verbundenen Hosts Zugriff auf alle von Ihnen konfigurierten vSphere Native Key Provider.

Voraussetzungen

Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**

Verfahren

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

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

3 Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.

4 Klicken Sie auf **Hinzufügen** und dann auf **Nativen Schlüsselanbieter hinzufügen**.

5 Geben Sie einen Namen für den vSphere Native Key Provider ein.

Jeder logische Schlüsselanbieter muss unabhängig von seinem Typ (Standard-, vertrauenswürdiger und nativer Schlüsselanbieter) über einen eindeutigen Namen in allen vCenter Server-Systemen verfügen.

Weitere Informationen finden Sie unter Benennung des Schlüsselanbieters.

6 Wenn dieser vSphere Native Key Provider nur von Hosts mit einem TPM 2.0 verwendet werden soll, aktivieren Sie das Kontrollkästchen **Schlüsselanbieter nur mit TPM-geschützten ESXi-Hosts verwenden**.

Bei aktiviertem Kontrollkästchen steht der vSphere Native Key Provider nur auf Hosts mit einem TPM 2.0 zur Verfügung.

7 Klicken Sie auf **Schlüsselanbieter hinzufügen**.

Hinweis Es dauert etwa fünf Minuten, bis alle geclusterten ESXi-Hosts in einem Datencenter den Schlüsselanbieter erhalten und der Cache des vCenter Server aktualisiert ist. Aufgrund der Art und Weise der Informationsweiterleitung müssen Sie unter Umständen einige Minuten warten, bis Sie den Schlüsselanbieter für wichtige Vorgänge auf bestimmten Hosts verwenden können.

Ergebnisse

Der vSphere Native Key Provider wird hinzugefügt und im Bereich **Schlüsselanbieter** angezeigt. Zu diesem Zeitpunkt wird der vSphere Native Key Provider nicht gesichert. Sie müssen den vSphere Native Key Provider sichern, bevor Sie ihn verwenden können.

Nächste Schritte

Weitere Informationen hierzu finden Sie unter Sichern eines vSphere Native Key Providers.

Sichern eines vSphere Native Key Providers

Wenn Sie die Konfiguration eines Schlüsselanbieters wiederherstellen müssen, ist die Sicherung eines vSphere Native Key Providers im Rahmen eines Notfallwiederherstellungsszenarios erforderlich. Sie können den vSphere Client, die PowerCLI oder API verwenden, um den vSphere Native Key Provider zu sichern.

Der vSphere Native Key Provider wird im Rahmen der dateibasierten vCenter Server-Sicherung gesichert. Sie müssen den vSphere Native Key Provider jedoch mindestens einmal sichern, bevor Sie ihn verwenden können. Wenn Sie einen vSphere Native Key Provider erstellen, wird dieser nicht gesichert.

Eine Sicherung ist dann notwendig, wenn die Konfiguration wiederhergestellt werden muss. Informationen zum Wiederherstellen eines vSphere Native Key Providers finden Sie unter Wiederherstellen eines vSphere Native Key Providers mithilfe des vSphere Client.

Speichern Sie die Sicherungsdatei an einem sicheren Ort. Sie können die Sicherung beim Erstellen mit einem Kennwort schützen. Die Sicherungsdatei liegt im Format PKCS#12 vor.

vCenter Server erstellt einen Alarm, wenn ein vSphere Native Key Provider nicht gesichert wurde. Sie können den Alarm zwar bestätigen, bis zur Sicherung des vSphere Native Key Providers wird dieser jedoch alle 24 Stunden erneut angezeigt.

Voraussetzungen

Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**

Hinweis In einer Konfiguration mit erweitertem verknüpftem Modus müssen Sie die Sicherung auf dem vCenter Server durchführen, zu dem der Schlüsselanbieter gehört.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.
4. Wählen Sie den zu sichernden vSphere Native Key Provider aus.

   Für nicht gesicherte Schlüsselanbieter wird der Status „Nicht gesichert“ angezeigt.
5. Klicken Sie auf **Sichern**.
6. Zum Schützen der Sicherung mit einem Kennwort aktivieren Sie das Kontrollkästchen **Daten des nativen Kennwortanbieters mit Kennwort schützen**.
   a. Geben Sie ein Kennwort ein und speichern Sie es an einem sicheren Ort.
   b. Aktivieren Sie das Kontrollkästchen **Ich habe das Kennwort an einem sicheren Ort gespeichert**, um anzugeben, dass Sie das Kennwort an einem sicheren Ort gespeichert haben.
7. Klicken Sie auf **Schlüsselanbieter sichern**.

   Die Sicherungsdatei liegt im Format PKCS#12 vor.
8. Speichern Sie die Sicherungsdatei an einem sicheren Ort.

Ergebnisse

Der Status des vSphere Native Key Provider ändert sich von „Nicht gesichert“ in „Warnung“ und „Aktiv“. Mit „Warnung“ wird angegeben, dass der vCenter Server die Informationen weiterhin an alle ESXi-Hosts im Datencenter überträgt. „Aktiv“ bedeutet, dass die Informationen an alle Hosts übertragen wurden.

Nächste Schritte

Informationen zum Hinzufügen von vTPMs zu virtuellen Maschinen finden Sie unter Kapitel 11 Sichern von virtuellen Maschinen mit Virtual Trusted Platform Module. Informationen zum Verschlüsseln virtueller Maschinen finden Sie unter Kapitel 10 Verwenden der Verschlüsselung in Ihrer vSphere-Umgebung.

Wiederherstellen eines vSphere Native Key Providers

Sie können den vSphere Native Key Provider entweder über den -vSphere Client oder über die vCenter Server Appliance wiederherstellen.

Bei Bedarf können Sie einen vSphere Native Key Provider auf folgende Arten wiederherstellen.

1. Wenn Sie Ihre vCenter Server Appliance nicht neu erstellen müssen, verwenden Sie den vSphere Client, um den Schlüsselanbieter wiederherzustellen. Weitere Informationen hierzu finden Sie unter Wiederherstellen eines vSphere Native Key Providers mithilfe des vSphere Client.
2. Wenn Sie Ihre vCenter Server Appliance neu erstellen müssen, müssen Sie den Schlüsselanbieter aus Ihrer vCenter Server Appliance-Sicherung wiederherstellen. Wenn Sie eine vCenter Server Appliance-Sicherung durchführen, wird der native Schlüsselanbieter gespeichert. Unter https://blogs.vmware.com/vsphere/2018/05/vcenter-server-appliance-6-7-file-based-backup-and-restore-walkthroughs.html finden Sie Informationen zum Wiederherstellen von vCenter Server Appliance aus der Sicherung.

Wiederherstellen eines vSphere Native Key Providers mithilfe des vSphere Client

Sie können den vSphere Client zum Wiederherstellen des vSphere Native Key Providers verwenden.

Sie können einen vSphere Native Key Provider wiederherstellen, falls er versehentlich gelöscht wurde oder wenn Sie eine Notfallwiederherstellung durchführen müssen.

Wenn Sie einen vSphere Native Key Provider wiederherstellen, müssen Sie den Schlüsselanbieter nicht erneut sichern. Die anfängliche Sicherung ist nicht ausreichend. Verwalten Sie die Sicherungsdatei weiterhin an einem sicheren Ort.

Hinweis Sie können diese Aufgabe auch verwenden, um vSphere Native Key Provider für vCenter Server-Systeme in einer Konfiguration im erweiterten verknüpften Modus zu konfigurieren. Nachdem Sie den vSphere Native Key Provider auf einem vCenter Server-System in der Konfiguration im erweiterten verknüpften Modus erstellt haben, verwenden Sie die Funktion **Wiederherstellen**, um die verschlüsselte Schlüsseldatei in die anderen ELM-verbundenen vCenter Server-Systeme zu importieren.

Voraussetzungen

- Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**

- Die Sicherungsdatei des Schlüsselanbieters.
- Das Kennwort für die Schlüsselanbieterdatei, sofern Sie eines beim Sichern des Schlüsselanbieters eingegeben haben.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.
4. Wählen Sie den vSphere Native Key Provider aus und klicken Sie auf **Wiederherstellen**.
5. Navigieren Sie zum Dateispeicherort und wählen Sie die verschlüsselte Schlüsseldatei für die Sicherung aus.

   Die Datei wurde im PKCS#12-Format gespeichert.
6. (Optional) Wenn die Datei kennwortgeschützt ist, geben Sie das Kennwort ein.
7. Klicken Sie auf **Weiter**.
8. (Optional) Wenn Sie sich entschieden haben, diesen Schlüsselanbieter nur mit TPM-geschützten ESXi-Hosts zu verwenden, aktivieren Sie das Kontrollkästchen.
9. Klicken Sie auf **Beenden**.

Ergebnisse

Der vSphere Native Key Provider wird in den vCenter Server importiert. Um den vSphere Native Key Provider für Verschlüsselungsaufgaben zu verwenden, stellen Sie sicher, dass Sie ihn zuerst im Bereich **Schlüsselanbieter** auswählen und auf **Als Standard festlegen** klicken.

Aktualisieren eines vSphere Native Key Providers

Im Rahmen Ihrer regelmäßigen Schlüsselrotationspläne können Sie PowerCLI verwenden, um einen vSphere Native Key Provider zu aktualisieren.

Wenn Sie über eine Richtlinie für die Schlüsselrotation verfügen, können Sie den vSphere Native Key Provider aktualisieren und erneut Schlüssel für die virtuellen Maschinen erstellen, die Sie mit diesem Schlüsselanbieter verschlüsselt haben. Sie müssen PowerCLI verwenden, um den vSphere Native Key Provider zu aktualisieren. Sie können auch erneut Schlüssel für die virtuellen Maschinen erstellen, ohne den Schlüsselanbieter zu aktualisieren. In diesem Fall werden nur die Schlüssel der virtuellen Maschinen geändert. Informationen zur erneuten Schlüsselerstellung für eine virtuelle Maschine finden Sie unter Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe des vSphere Client.

Voraussetzungen

- Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**
- PowerCLI 12.3.0

Verfahren

1 Führen Sie in einer PowerCLI-Sitzung das Cmdlet `Connect-VIServer` aus, um als Administratorbenutzer eine Verbindung mit dem vCenter Server herzustellen, auf dem Sie den zu aktualisierenden vSphere Native Key Provider konfiguriert haben.

```
Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
```

2 Zum Abrufen der vSphere Native Key Provider-Namen führen Sie das Cmdlet `Get-KeyProvider` mit dem optionalen Parameter `Type` aus.

```
Get-KeyProvider -Type NativeKeyProvider
```

3 Zum Aktualisieren des Schlüsselanbieters führen Sie das Cmdlet `Set-KeyProvider` aus und geben Sie den Namen des Schlüsselanbieters und die GUID an.

Sie können die zu verwendende GUID generieren, indem Sie das Cmdlet `New-Guid` ausführen.

```
Set-KeyProvider -KeyProvider KeyProvider_name -KeyId Guid
```

Es wird eine Warnung zum Sichern der Konfiguration angezeigt.

4 Um den Schlüsselanbieter zu sichern, führen Sie das Cmdlet `Export-KeyProvider` aus.

```
Export-KeyProvider -KeyProvider KeyProvider_name -FilePath path_file_name
```

Sie können den Schlüsselanbieter auch mithilfe des vSphere Client sichern. Weitere Informationen finden Sie unter Sichern eines vSphere Native Key Providers.

Ergebnisse

Wenn ein Schlüsselanbieter aktualisiert wird, ändert sich sein Status in „Nicht gesichert“. Nachdem Sie den Schlüsselanbieter gesichert haben, ändert sich sein Status in „Aktiv“.

Löschen eines vSphere Native Key Providers

Sie können den vSphere Client zum Löschen eines vSphere Native Key Providers aus vCenter Server verwenden.

Nachdem Sie einen vSphere Native Key Provider gelöscht haben, werden virtuelle Maschinen, die über vTPMs verfügen oder verschlüsselt sind, weiterhin ausgeführt. Wenn Sie den ESXi-Host neu starten, wechseln die zugehörigen verschlüsselten VMs in den gesperrten Modus. Nachdem Sie die Registrierung dieser virtuellen Maschinen aufgehoben haben, wechseln sie in den gesperrten Modus, wenn Sie versuchen, sie erneut zu registrieren. Die einzige Möglichkeit zum Entsperren der virtuellen Maschinen besteht in der Wiederherstellung des vorherigen vSphere Native Key Providers.

Voraussetzungen

Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**

Verschlüsseln Sie vor dem Löschen eines vSphere Native Key Providers alle verschlüsselten virtuellen Maschinen und Datenspeicher, die mithilfe dieses Schlüsselanbieters verschlüsselt wurden, erneut mit einem anderen Schlüsselanbieter. Weitere Informationen finden Sie unter Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe des vSphere Client.

Behalten Sie zudem eine Sicherung des vSphere Native Key Providers für den Fall bei, dass Sie eine verschlüsselte virtuelle Maschine nach dem Löschen des Schlüsselanbieters erneut verschlüsseln müssen.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.
4. Wählen Sie den Schlüsselanbieter aus, den Sie löschen möchten.
5. Klicken Sie auf **Löschen**.
6. Lesen Sie die Warnmeldung und ziehen Sie den Schieberegler ganz nach rechts.
7. Klicken Sie auf **Löschen**.

Ergebnisse

Der vSphere Native Key Provider wird aus dem vCenter Server entfernt.

vSphere Trust Authority

9

Mit vSphere ab Version 7.0 können Sie die Vorteile von VMware® vSphere Trust Authority™ nutzen. vSphere Trust Authority ist eine grundlegende Technologie zur Verbesserung der Sicherheit von Arbeitslasten. vSphere Trust Authority schafft ein größeres Maß an Vertrauen in Ihrer Organisation, indem Sie den Hardware-Root of Trust eines ESXi-Hosts mit der Arbeitslast selbst verknüpfen.

Lesen Sie als Nächstes die folgenden Themen:

- vSphere Trust Authority – Konzepte und Funktionen
- Konfigurieren von vSphere Trust Authority
- Verwalten vSphere Trust Authority in Ihrer vSphere-Umgebung

vSphere Trust Authority – Konzepte und Funktionen

vSphere Trust Authority schützt Ihr SDDC vor böswilligen Angriffen, indem die Vertrauenswürdigkeit einer vertrauenswürdigen Computing-Basis auf die gesamte Computing-Infrastruktur Ihres Unternehmens ausgeweitet wird. vSphere Trust Authority verwendet Remotebestätigung und kontrollierten Zugriff auf erweiterte Kryptografiefunktionen.

vSphere Trust Authority ist ein Satz von Diensten, der hohe Sicherheitsanforderungen erfüllt. Mit vSphere Trust Authority können Sie eine sichere Infrastruktur einrichten und verwalten. Sie können sicherstellen, dass vertrauliche Arbeitslasten nur auf ESXi-Hosts ausgeführt werden, auf denen nachweislich Originalsoftware gestartet wurde.

So schützt vSphere Trust Authority Ihre Umgebung

Sie konfigurieren vSphere Trust Authority-Dienste zum Bestätigen Ihrer ESXi-Hosts, die dann vertrauenswürdige Kryptografievorgänge durchführen können.

vSphere Trust Authority verwendet Remotebestätigungen für ESXi-Hosts, um die Echtheit der gestarteten Software zu bestätigen. Mithilfe von Bestätigungen wird sichergestellt, dass auf den ESXi-Hosts echte VMware-Software oder von VMware signierte Partnersoftware verwendet wird. Bestätigungen greifen auf Messungen zurück, die sich in einem TPM 2.0-Chip (Trusted Platform Module) befinden, der auf dem ESXi-Host installiert ist. In vSphere Trust Authority kann ein ESXi-Host nur dann auf Verschlüsselungsschlüssel zugreifen und Kryptografievorgänge durchführen, wenn er bestätigt wurde.

vSphere Trust Authority-Glossar

vSphere Trust Authority führt bestimmte wichtige Begriffe und Definitionen ein.

Tabelle 9-1. vSphere Trust Authority-Glossar

Begriff	Definition
VMware vSphere® Trust Authority™	Gibt einen Satz von Diensten an, die eine vertrauenswürdige Infrastruktur ermöglichen. Stellt sicher, dass auf ESXi-Hosts vertrauenswürdige Software ausgeführt wird und dass Verschlüsselungsschlüssel nur für vertrauenswürdige ESXi-Hosts freigegeben werden.
vSphere Trust Authority-Komponenten	Zu den vSphere Trust Authority-Komponenten gehören: ■ Bestätigungsdienst ■ Schlüsselanbieterdienst
Bestätigungsdienst	Bestätigt den Status eines ESXi-Remotehosts. Verwendet TPM 2.0 zum Aufbau eines Hardware-Root of Trust und überprüft Software-Messungen anhand einer Liste mit ESXi-Versionen, die vom Administrator genehmigt wurden.
Schlüsselanbieterdienst	Schließt einen oder mehrere Schlüsselserver ein und macht vertrauenswürdige Schlüsselanbieter verfügbar, die beim Verschlüsseln von virtuellen Maschinen angegeben werden können. Derzeit sind Schlüsselserver auf das KMIP-Protokoll beschränkt.
Vertrauenswürdige Infrastruktur	Eine vertrauenswürdige Infrastruktur besteht aus Folgendem: ■ Ein Trust Authority-vCenter Server ■ Ein Arbeitslast-vCenter Server ■ Mindestens ein vSphere Trust Authority-Cluster (konfiguriert als Teil des Trust Authority-vCenter Server) ■ Mindestens ein vertrauenswürdiger Cluster (konfiguriert als Teil des Arbeitslast-vCenter Server) ■ Verschlüsselte Arbeitslast-VMs, die im vertrauenswürdigen Cluster ausgeführt werden ■ Mindestens ein KMIP-konformer Schlüsselverwaltungsserver **Hinweis** Sie müssen getrennte vCenter Server-Systeme für den Trust Authority- und den vertrauenswürdigen Cluster verwenden.
Trust Authority-Cluster	Besteht aus einem vCenter Server-Cluster mit ESXi-Hosts, auf denen die vSphere Trust Authority-Komponenten (Bestätigungs- und Schlüsselanbieterdienst) ausgeführt werden.
Trust Authority-Host	Ein ESXi-Host, auf dem vSphere Trust Authority-Komponenten (Bestätigungs- und Schlüsselanbieterdienst) ausgeführt werden.
Vertrauenswürdiger Cluster	Besteht aus einem vCenter Server-Cluster mit vertrauenswürdigen ESXi-Hosts, die remote vom Trust Authority-Cluster bestätigt wurden. Obwohl dies nicht unbedingt erforderlich ist, erhöht ein konfigurierter Schlüsselanbieterdienst den von einem vertrauenswürdigen Cluster bereitgestellten Wert erheblich.
Vertrauenswürdiger Host	Ein ESXi-Host, dessen Software vom Bestätigungsdienst des Trust Authority-Clusters überprüft wurde. Dieser Host führt Arbeitslast-VMs aus, die mithilfe von Schlüsselanbietern verschlüsselt werden können, die vom Schlüsselanbieterdienst des Trust Authority-Clusters veröffentlicht wurden.

Tabelle 9-1. vSphere Trust Authority-Glossar (Fortsetzung)

Begriff	Definition
vSphere Encryption für virtuelle Maschinen	Mit vSphere Virtual Machine Encryption können Sie verschlüsselte virtuelle Maschinen erstellen und vorhandene virtuelle Maschinen verschlüsseln. vSphere Virtual Machine Encryption wurde in vSphere 6.5 eingeführt. Weitere Informationen dazu, wie Schlüsselanbieter mit Verschlüsselungsschlüsseln umgehen, finden Sie unter vSphere-Verschlüsselungsschlüssel und -Schlüsselanbieter.
Vertrauenswürdiger Schlüsselanbieter	Ein Schlüsselanbieter, der einen einzelnen Verschlüsselungsschlüssel auf einem Schlüsselserver kapselt. Für den Zugriff auf den Verschlüsselungsschlüssel muss vom Bestätigungsdienst bestätigt werden, dass die ESXi-Software auf dem vertrauenswürdigen Host verifiziert wurde.
Standardschlüsselanbieter	Ein Schlüsselanbieter, der Verschlüsselungsschlüssel direkt von einem Schlüsselserver abruft und Schlüssel an die notwendigen Hosts in einem Datencenter verteilt. Wurde zuvor in vSphere als KMS-Cluster bezeichnet.
Schlüsselserver	Ein KMIP-KMS (Key Management Server), der einem Schlüsselanbieter zugeordnet ist.
Arbeitslast-vCenter Server	Der vCenter Server, der einen oder mehrere vertrauenswürdige Cluster verwaltet und zu deren Konfiguration verwendet wird.

Grundlegendes zu vSphere Trust Authority

Mit vSphere Trust Authority können Sie folgende Aufgaben durchführen:

- Bereitstellen von ESXi-Hosts mit einem Hardware-Root of Trust und Funktionen für die Remotebestätigung
- Einschränken der Verschlüsselungsschlüsselverwaltung, indem Schlüssel nur für bestätigte ESXi-Hosts freigegeben werden
- Erstellen einer sichereren Verwaltungsumgebung für die Verwaltung von Vertrauensstellungen
- Zentrale Verwaltung mehrerer Schlüsselserver
- Weitere Durchführung von Kryptografievorgängen auf virtuellen Maschinen, jedoch mit erweiterter Verschlüsselungsschlüsselverwaltung.

In vSphere 6.5 und 6.7 ist die VM-Verschlüsselung auf vCenter Server angewiesen, um Verschlüsselungsschlüssel aus einem Schlüsselserver abzurufen und gegebenenfalls an ESXi-Hosts weiterzugeben. vCenter Server authentifiziert sich beim Schlüsselserver unter Verwendung von Client- und Serverzertifikaten, die in VMware Endpoint Certificate Store (VECS) gespeichert sind. Vom Schlüsselserver gesendete Verschlüsselungsschlüssel geben vCenter Server-Arbeitsspeicher an die erforderlichen ESXi-Hosts weiter (mit Datenverschlüsselung, die von TLS über das Netzwerk bereitgestellt wird). Darüber hinaus ist vSphere auf Berechtigungsprüfungen in vCenter Server angewiesen, um Benutzerberechtigungen zu validieren und Schlüsselserver-Zugriffsbeschränkungen zu erzwingen. Diese Architektur ist zwar sicher, berücksichtigt aber nicht die Gefahren durch einen manipulierten vCenter Server, einen böswilligen vCenter Server-Administrator oder einen Verwaltungs- bzw. Konfigurationsfehler, der dazu führen kann, dass geheime Schlüssel manipuliert oder gestohlen werden.

In vSphere 7.0 und höher werden diese Probleme mithilfe von vSphere Trust Authority behoben. Sie können eine vertrauenswürdige Computerbasis (Trusted Computing Base) erstellen, die aus einem sicheren, verwaltbaren Satz von ESXi-Hosts besteht. vSphere Trust Authority implementiert einen Remotebestätigungsdienst für die ESXi-Hosts, die Sie als vertrauenswürdig einstufen möchten. Darüber hinaus bietet vSphere Trust Authority verbesserte Unterstützung für TPM 2.0-Bestätigungen (ab Version 6.7 zu vSphere hinzugefügt), um Zugriffsbeschränkungen für Verschlüsselungsschlüssel zu implementieren und somit besseren Schutz für die geheimen Schlüssel der Arbeitslast-VM bereitzustellen. Darüber hinaus erlaubt vSphere Trust Authority nur autorisierten Trust Authority-Administratoren, vSphere Trust Authority-Dienste und Trust Authority-Hosts zu konfigurieren. Der Trust Authority-Administrator kann mit dem vSphere-Administratorbenutzer übereinstimmen oder ein separater Benutzer sein.

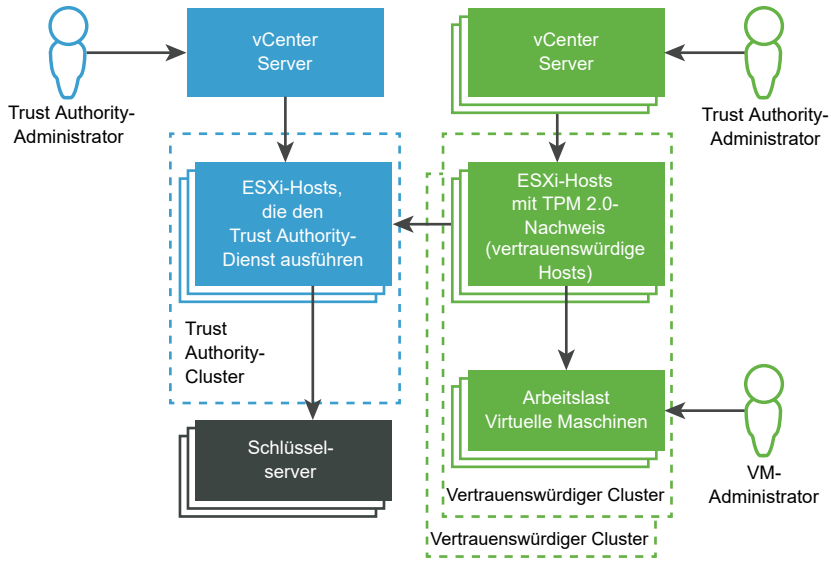
Schließlich können Sie Ihre Arbeitslasten mithilfe von vSphere Trust Authority in einer sichereren Umgebung ausführen, indem Sie:

- Manipulationen erkennen
- Nicht autorisierte Änderungen verweigern
- Malware und Änderungen verhindern
- Vertrauliche Arbeitslasten ausschließlich mit verifizierter, sicherer Hardware und Software ausführen

vSphere Trust Authority – Architektur

Die folgende Abbildung zeigt eine vereinfachte Darstellung der vSphere Trust Authority-Architektur.

Abbildung 9-1. vSphere Trust Authority – Architektur



In dieser Abbildung:

1 vCenter Server-Systeme

Der Trust Authority-Cluster und die vertrauenswürdigen Cluster werden in separaten vCenter Server-Systemen verwaltet.

2 Trust Authority-Cluster

Besteht aus den ESXi-Hosts, die die vSphere Trust Authority-Komponenten ausführen.

3 Schlüsselserver

Speichern Sie Verschlüsselungsschlüssel, die beim Durchführen von Verschlüsselungsvorgängen vom Schlüsselanbieterdienst verwendet werden. Die Schlüsselserver befinden sich außerhalb von vSphere Trust Authority.

4 Vertrauenswürdige Cluster

Bestehen aus den vertrauenswürdigen ESXi-Hosts, die remote mit einem TPM bestätigt wurden und die verschlüsselte Arbeitslasten ausführen.

5 Trust Authority-Administrator

Administrator, der Mitglied der vCenter Server-Gruppe „TrustedAdmins“ ist und die vertrauenswürdige Infrastruktur konfiguriert.

vSphere Trust Authority ermöglicht Flexibilität beim Festlegen von Trust Authority-Administratoren. Bei den Trust Authority-Administratoren in der Abbildung kann es sich um separate Benutzer handeln. Die Trust Authority-Administratoren können aber auch derselbe Benutzer sein, wobei Anmeldedaten verwendet werden, die über die vCenter Server-Systeme hinweg verknüpft sind. In diesem Fall handelt es sich um denselben Benutzer und dieselbe TrustedAdmins-Gruppe.

6 VM-Administrator

Administrator, dem Berechtigungen zum Verwalten der verschlüsselten Arbeitslast-VMs auf den vertrauenswürdigen Hosts erteilt wurden.

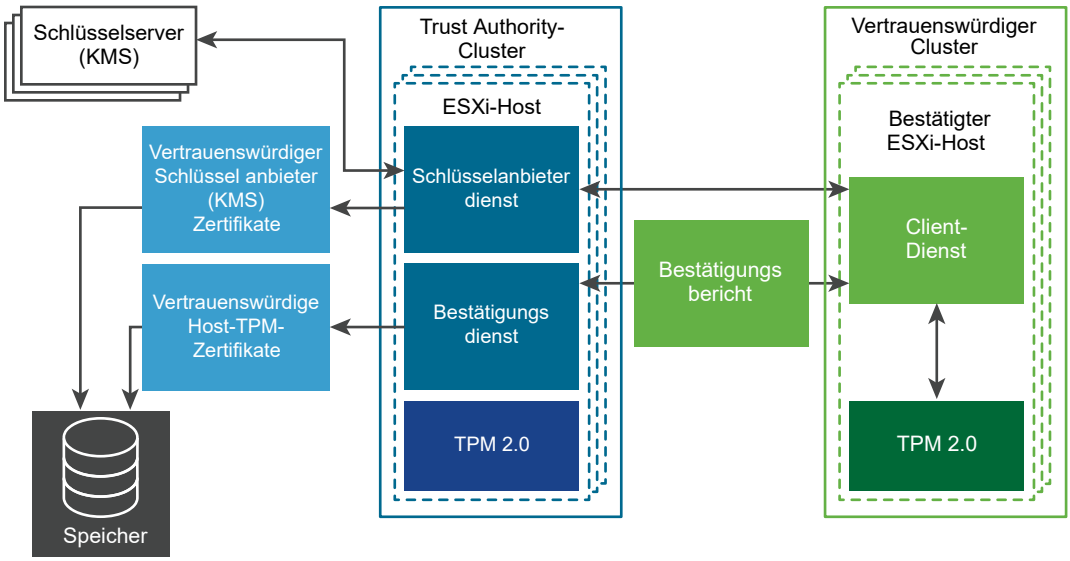
Vertrauenswürdige vSphere Trust Authority-Infrastruktur

Die vertrauenswürdige Infrastruktur setzt sich aus vSphere Trust Authority-Diensten, mindestens einem KMIP-kompatiblen Schlüsselserver, den vCenter Server-Systemen und Ihren ESXi-Hosts zusammen.

Was ist eine vertrauenswürdige Infrastruktur?

Eine vertrauenswürdige Infrastruktur besteht aus mindestens einem vSphere Trust Authority-Cluster, mindestens einem vertrauenswürdigen Cluster und mindestens einem externen KMIP-kompatiblen Schlüsselserver. Jeder Cluster enthält ESXi-Hosts, auf denen bestimmte vSphere Trust Authority-Dienste ausgeführt werden (siehe folgende Abbildung).

Abbildung 9-2. vSphere Trust Authority-Dienste



Durch die Konfiguration des Trust Authority-Clusters werden zwei Dienste aktiviert:

- Bestätigungsdienst
- Schlüsselanbieterdienst

Wenn Sie vSphere Trust Authority konfigurieren, kommunizieren die ESXi-Hosts im vertrauenswürdigen Cluster mit dem Bestätigungsdienst. Der Schlüsselanbieterdienst befindet sich zwischen den vertrauenswürdigen Hosts und einem oder mehreren vertrauenswürdigen Schlüsselanbietern.

Hinweis Aktuell benötigen die ESXi-Hosts im Trust Authority-Cluster kein TPM. Es empfiehlt sich jedoch, neue ESXi-Hosts mit TPMs zu installieren.

Was ist der vSphere Trust Authority-Nachweisdienst?

Der Bestätigungsdienst erzeugt ein signiertes Dokument, das Assertionen enthält, die den Binär- und Konfigurationsstatus der ESXi-Remotehosts im vertrauenswürdigen Cluster beschreiben. Der Bestätigungsdienst bescheinigt den Status der ESXi-Hosts unter Verwendung eines TPM 2.0-Chips (Trusted Platform Module) als Basis für Softwaremessungen und Berichterstellung. Das TPM auf dem ESXi-Remotehost misst den Software-Stack und sendet die Konfigurationsdaten an den Bestätigungsdienst. Der Bestätigungsdienst stellt sicher, dass die Signatur der Softwaremessung einem zuvor konfigurierten vertrauenswürdigen TPM-Endorsement Key (EK) zugewiesen werden kann. Der Bestätigungsdienst stellt außerdem sicher, dass die Softwaremessung mit einem von mehreren zuvor angegebenen ESXi-Images übereinstimmt. Der Bestätigungsdienst signiert ein JSON-Web-Token (JWT), das er an den ESXi-Host ausgibt, indem er die Assertionen über die Identität, Gültigkeit und Konfiguration des ESXi-Hosts bereitstellt.

Was ist der vSphere Trust Authority-Schlüsselanbieterdienst?

Aufgrund des Schlüsselanbieterdiensts benötigen die vCenter Server- und ESXi-Hosts keine direkten Anmeldedaten für den Schlüsselserver. Damit in vSphere Trust Authority ein ESXi-Host auf einen Verschlüsselungsschlüssel zugreifen kann, muss sich der Host beim Schlüsselanbieterdienst authentifizieren.

Der Trust Authority-Administrator muss eine vertrauenswürdige Verbindung konfigurieren, damit der Schlüsselanbieterdienst eine Verbindung zu einem Schlüsselanbieter herstellen kann. Für die meisten KMIP-kompatiblen Server umfasst die Einrichtung einer vertrauenswürdigen Verbindung das Konfigurieren von Client- und Serverzertifikaten.

Um sicherzustellen, dass die Schlüssel nur für vertrauenswürdige ESXi-Hosts freigegeben werden, fungiert der Schlüsselanbieterdienst als Gatekeeper für die Schlüsselserver. Der Schlüsselanbieterdienst verbirgt die Schlüsselserverspezifikationen vor dem verbleibenden Software-Stack des Datencenters, indem er das Konzept eines vertrauenswürdigen Schlüsselanbieters verwendet. Jeder vertrauenswürdige Schlüsselanbieter verfügt über einen einzelnen konfigurierten primären Verschlüsselungsschlüssel und verweist auf einen oder mehrere Schlüsselserver. Der Schlüsselanbieterdienst kann mehrere konfigurierte vertrauenswürdige Schlüsselanbieter enthalten. Beispiel: Angenommen, Sie benötigen einen separaten vertrauenswürdigen Schlüsselanbieter für jede Abteilung in einer Organisation. Jeder vertrauenswürdige Schlüsselanbieter verwendet einen anderen primären Schlüssel, kann aber auf denselben unterstützenden Schlüsselserver zurückgreifen.

Nach der Erstellung eines vertrauenswürdigen Schlüsselanbieters kann der Schlüsselanbieterdienst Anforderungen von den vertrauenswürdigen ESXi-Hosts akzeptieren, um kryptografische Vorgänge für diesen vertrauenswürdigen Schlüsselanbieter auszuführen.

Wenn ein vertrauenswürdiger ESXi-Host Vorgänge für einen vertrauenswürdigen Schlüsselanbieter anfordert, stellt der Schlüsselanbieterdienst sicher, dass der ESXi-Host, der den Verschlüsselungsschlüssel anfordert, bestätigt wird. Nach Durchlaufen aller Prüfungen nimmt der vertrauenswürdige ESXi-Host Verschlüsselungsschlüssel vom Schlüsselanbieterdienst entgegen.

Welche Ports werden von vSphere Trust Authority verwendet?

Die vSphere Trust Authority-Dienste überwachen Verbindungen hinter dem Reverse-Proxy des ESXi-Hosts. Die gesamte Kommunikation erfolgt über HTTPS auf Port 443.

Was sind vertrauenswürdige vSphere Trust Authority-Hosts?

Die vertrauenswürdigen ESXi-Hosts sind so konfiguriert, dass sie vertrauenswürdige Schlüsselanbieter zum Durchführen kryptografischer Vorgänge verwenden. Die vertrauenswürdigen ESXi-Hosts führen wichtige Vorgänge durch, indem sie mit dem Schlüsselanbieter- und dem Bestätigungsdienst kommunizieren. Zur Authentifizierung und Autorisierung verwenden die vertrauenswürdigen ESXi-Hosts ein Token, das sie vom Bestätigungsdienst erhalten haben. Um ein gültiges Token zu erhalten, muss der vertrauenswürdige ESXi-Host den Bestätigungsdienst erfolgreich bestätigen. Das Token enthält bestimmte Beanspruchungen, anhand derer ermittelt werden kann, ob der vertrauenswürdige ESXi-Host für den Zugriff auf einen vertrauenswürdigen Schlüsselanbieter autorisiert ist.

vSphere Trust Authority und Schlüsselserveranforderung

vSphere Trust Authority erfordert die Verwendung mindestens eines Schlüsselservers. In früheren vSphere-Versionen wurde ein Schlüsselserver als Schlüsselverwaltungsserver oder KMS bezeichnet. Derzeit bietet die vSphere Virtual Machine Encryption-Lösung Unterstützung für KMIP 1.1-kompatible Schlüsselserver.

Wie speichert vSphere Trust Authority Konfigurations- und Statusinformationen?

vCenter Server fungiert hauptsächlich als Passthrough-Dienst für Informationen zu vSphere Trust Authority-Konfiguration und -Status. Die meisten vSphere Trust Authority-Konfigurations- und -Statusinformationen werden auf den ESXi-Hosts in der ConfigStore-Datenbank gespeichert. Bestimmte Statusinformationen werden auch in der vCenter Server-Datenbank gespeichert.

Hinweis Da die meisten vSphere Trust Authority-Konfigurationsinformationen auf den ESXi-Hosts gespeichert werden, sichert der dateibasierte vCenter Server-Sicherungsmechanismus diese Informationen nicht. Um sicherzustellen, dass die Konfigurationsinformationen für Ihre vSphere Trust Authority-Bereitstellung gespeichert werden, finden Sie Informationen unter Sichern der vSphere Trust Authority-Konfiguration.

Vorgehensweise zur Integration von vSphere Trust Authority in vCenter Server

Sie konfigurieren separate vCenter Server-Instanzen, um den Trust Authority-Cluster und den vertrauenswürdigen Cluster zu verwalten. Weitere Informationen hierzu finden Sie unter Konfigurieren von vSphere Trust Authority.

In einem vertrauenswürdigen Cluster verwaltet der vCenter Server die API-Aufrufe der Trust Authority und übergibt sie an die ESXi-Hosts. Der vCenter Server repliziert die API-Aufrufe auf allen ESXi-Hosts im vertrauenswürdigen Cluster.

Nachdem Sie vSphere Trust Authority erstmals konfiguriert haben, können Sie ESXi-Hosts zu einem Trust Authority- oder vertrauenswürdigen Cluster hinzufügen oder daraus entfernen. Weitere Informationen hierzu finden Sie unter Hinzufügen und Entfernen von vSphere Trust Authority-Hosts.

vSphere Trust Authority – Prozessabläufe

Sie müssen sich mit den Prozessabläufen in vSphere Trust Authority vertraut machen, um Ihre vertrauenswürdige Infrastruktur konfigurieren und verwalten zu können.

Vorgehensweise zum Konfigurieren von vSphere Trust Authority

vSphere Trust Authority ist standardmäßig nicht aktiviert. Sie müssen vSphere Trust Authority in Ihrer Umgebung manuell konfigurieren. Weitere Informationen hierzu finden Sie unter Konfigurieren von vSphere Trust Authority.

Wenn Sie vSphere Trust Authority konfigurieren, müssen Sie angeben, welche Versionen der ESXi-Software vom Bestätigungsdienst akzeptiert werden und welche TPMs (Trusted Platform Modules) vertrauenswürdig sind.

TPM und Bestätigung in vSphere Trust Authority

In diesem Handbuch werden die folgenden Definitionen zur Erläuterung von TPMs und Bestätigung verwendet.

Tabelle 9-2. TPM und Bestätigung – Glossar

Begriff	Definition
Endorsement Key (EK)	Ein TPM wird mit einem öffentlichen/privaten RSA-Schlüsselpaar hergestellt, das in die Hardware eingebaut ist und als Endorsement Key (EK) bezeichnet wird. Der EK ist für ein bestimmtes TPM eindeutig.
EK – Öffentlicher Schlüssel	Der öffentliche Teil des EK-Schlüsselpaars.
EK – Privater Schlüssel	Der private Teil des EK-Schlüsselpaars.
EK-Zertifikat	Der öffentliche EK-Schlüssel, der von einer Signatur umschlossen wird. Das EK-Zertifikat wird vom TPM-Hersteller erstellt, der den privaten Schlüssel seiner Zertifizierungsstelle verwendet, um den öffentlichen EK-Schlüssel zu signieren. Nicht alle TPMs enthalten ein EK-Zertifikat. In diesem Fall ist der öffentliche EK-Schlüssel nicht signiert.
TPM-Bestätigung	Die Fähigkeit des Bestätigungsdiensts, die auf einem Remotehost ausgeführte Software zu überprüfen. Die TPM-Bestätigung erfolgt über kryptografische Messungen, die vom TPM während des Starts des Remotehosts durchgeführt werden, und wird auf Anforderung an den Bestätigungsdienst weitergeleitet. Der Bestätigungsdienst stellt über den öffentlichen EK-Schlüssel oder das EK-Zertifikat eine Vertrauensstellung für das TPM her.

Konfigurieren der TPM-Vertrauensstellung auf den vertrauenswürdigen Hosts

Ein vertrauenswürdiger ESXi-Host muss ein TPM enthalten. Ein TPM wird mit einem öffentlichen/privaten Schlüsselpaar hergestellt, das in die Hardware eingebaut ist und als Endorsement Key (EK) bezeichnet wird. Obwohl TPM 2.0 viele Schlüssel/Zertifikat-Paare zulässt, wird am häufigsten ein RSA-2048-Schlüsselpaar verwendet. Wenn der öffentliche Schlüssel eines TPM von einer Zertifizierungsstelle signiert wird, entsteht ein EK-Zertifikat. Der TPM-Hersteller stellt in der Regel mindestens einen EK bereit, signiert den öffentlichen Schlüssel mit einer Zertifizierungsstelle und bettet das signierte Zertifikat in den nicht flüchtigen Arbeitsspeicher des TPM ein.

Sie können den Bestätigungsdienst so konfigurieren, dass TPMs wie folgt als vertrauenswürdig eingestuft werden:

- Stufen Sie alle CA-Zertifikate als vertrauenswürdig ein, mit denen der Hersteller das TPM signiert hat (öffentlicher EK-Schlüssel). Die Standardeinstellung für den Bestätigungsdienst besteht darin, CA-Zertifikate als vertrauenswürdig einzustufen. Bei dieser Vorgehensweise werden zahlreiche ESXi-Hosts vom selben CA-Zertifikat abgedeckt, wodurch der Verwaltungsaufwand reduziert wird.

- Stufen Sie das TPM-CA-Zertifikat und den öffentlichen EK-Schlüssel des ESXi-Hosts als vertrauenswürdig ein. Letzterer kann entweder das EK-Zertifikat oder der öffentliche EK-Schlüssel sein. Obwohl diese Vorgehensweise mehr Sicherheit bietet, ist es notwendig, Informationen zu jedem vertrauenswürdigen Host zu konfigurieren.
- Bestimmte TPMs enthalten kein EK-Zertifikat. In diesem Fall stufen Sie den öffentlichen EK-Schlüssel als vertrauenswürdig ein.

Die Entscheidung, allen TPM-CA-Zertifikaten zu vertrauen, erweist sich aus betrieblicher Sicht als praktisch. Sie können neue Zertifikate nur konfigurieren, wenn Sie eine neue Hardwareklasse zum Datencenter hinzufügen. Indem Sie einzelne EK-Zertifikate als vertrauenswürdig einstufen, können Sie den Zugriff auf bestimmte ESXi-Hosts einschränken.

Sie können sich auch gegen die Einstufung von TPM-CA-Zertifikaten als vertrauenswürdig entscheiden. Obwohl eine solche Konfiguration eher ungewöhnlich ist, können Sie sie verwenden, wenn ein EK nicht von einer Zertifizierungsstelle signiert ist. Derzeit ist diese Funktion nicht vollständig implementiert.

Hinweis Bestimmte TPMs enthalten keine EK-Zertifikate. Wenn Sie einzelne ESXi-Hosts als vertrauenswürdig einstufen möchten, muss das TPM ein EK-Zertifikat enthalten.

Bestätigung von TPMs durch vSphere Trust Authority

Zum Starten des Bestätigungsvorgangs sendet der vertrauenswürdige ESXi-Host im vertrauenswürdigen Cluster den vorkonfigurierten öffentlichen EK-Schlüssel und das EK-Zertifikat an den Bestätigungsdienst im Trust Authority-Cluster. Wenn der Bestätigungsdienst die Anfrage erhält, sucht er nach dem EK in seiner Konfiguration, wobei es sich je nach Konfiguration um den öffentlichen EK-Schlüssel und/oder das EK-Zertifikat handeln kann. Wenn keiner dieser Fälle zutrifft, lehnt der Bestätigungsdienst die Bestätigungsanfrage ab.

Da der EK nicht direkt für die Signierung verwendet wird, wird ein Bestätigungsschlüssel (AK oder AIK) ausgehandelt. Das Aushandlungsprotokoll stellt sicher, dass ein neu erstellter AK an den zuvor überprüften EK gebunden ist, um Man-in-the-Middle-Angriffe oder Angriffe mit gefälschten Identitäten zu verhindern. Nachdem ein AK ausgehandelt wurde, wird dieser in zukünftigen Bestätigungsanfragen wiederverwendet, statt jedes Mal neu generiert zu werden.

Der vertrauenswürdige ESXi-Host liest die Angebots- und PCR-Werte aus dem TPM. Das Angebot wird vom AK signiert. Der vertrauenswürdige ESXi-Host liest auch das TCG-Ereignisprotokoll, das alle Ereignisse enthält, die zum aktuellen PCR-Zustand geführt haben. Diese TPM-Informationen werden zur Überprüfung an den Bestätigungsdienst gesendet. Der Bestätigungsdienst überprüft die PCR-Werte mithilfe des Ereignisprotokolls.

Funktionsweise von Schlüsselanbietern mit Schlüsselservern

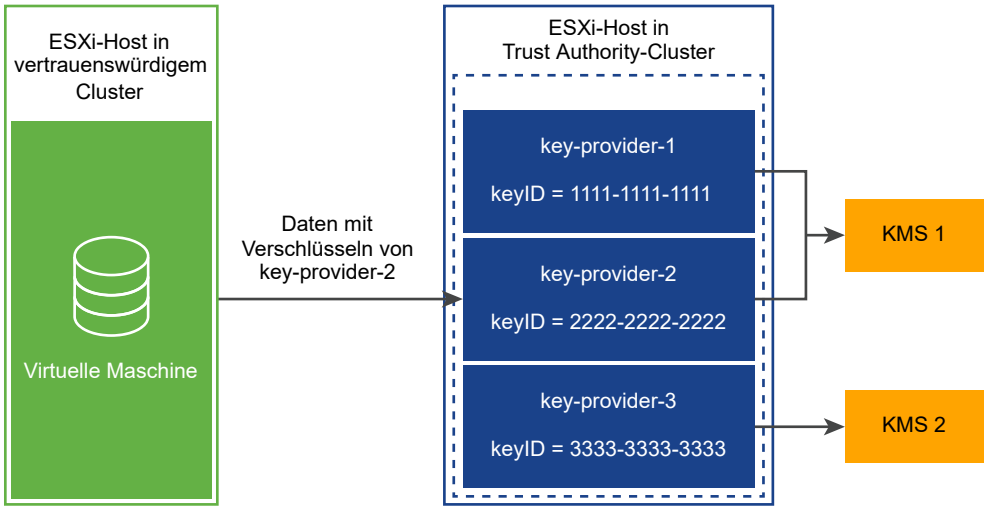
Der Schlüsselanbieterdienst verwendet das Konzept eines vertrauenswürdigen Schlüsselanbieters, um die Besonderheiten des Schlüsselservers vor der restlichen Datencenter-Software zu verbergen. Jeder vertrauenswürdige Schlüsselanbieter verfügt über einen einzelnen konfigurierten primären Verschlüsselungsschlüssel und verweist auf einen oder mehrere Schlüsselserver. Der primäre Verschlüsselungsschlüssel befindet sich auf den Schlüsselservern.

Im Rahmen der vSphere Trust Authority-Konfiguration müssen Sie den primären Schlüssel als separate Aktivität bereitstellen und aktivieren. Der Schlüsselanbieterdienst kann mehrere konfigurierte vertrauenswürdige Schlüsselanbieter enthalten. Jeder vertrauenswürdige Schlüsselanbieter verwendet einen anderen primären Schlüssel, kann aber auf denselben unterstützenden Schlüsselserver zurückgreifen.

Wenn ein neuer vertrauenswürdiger Schlüsselanbieter hinzugefügt wird, muss der Trust Authority-Administrator den Schlüsselserver und einen vorhandenen Schlüsselbezeichner auf diesem Schlüsselserver angeben.

Die folgende Abbildung zeigt die Beziehung zwischen dem Schlüsselanbieterdienst und den Schlüsselservern.

Abbildung 9-3. Schlüsselanbieter und Schlüsselserver



Nachdem Sie einen vertrauenswürdigen Schlüsselanbieter für einen vertrauenswürdigen Cluster konfiguriert haben, kann der Schlüsselanbieterdienst Anfragen zum Ausführen von Kryptografievorgängen für diesen vertrauenswürdigen Schlüsselanbieter akzeptieren. In dieser Abbildung werden beispielsweise drei vertrauenswürdige Schlüsselanbieter konfiguriert, zwei für KMS-1 und einer für KMS-2. Der vertrauenswürdige Host fordert einen Verschlüsselungsvorgang für key-provider-2 an. Der vertrauenswürdige Host fordert einen Verschlüsselungsschlüssel an, der generiert und zurückgegeben werden soll, und verwendet diesen Verschlüsselungsschlüssel zur Durchführung von Verschlüsselungsvorgängen.

Der Schlüsselanbieterdienst verwendet den über key-provider-2 referenzierten primären Schlüssel, um die angegebenen Klartextdaten zu verschlüsseln und den entsprechenden verschlüsselten Text zurückzugeben. Später kann der vertrauenswürdige Host denselben verschlüsselten Text für einen Entschlüsselungsvorgang bereitstellen und den ursprünglichen Klartext abrufen.

vSphere Trust Authority-Authentifizierung und -Autorisierung

vSphere Trust Authority-Verwaltungsvorgänge benötigen einen Benutzer, der Mitglied der TrustedAdmins-Gruppe ist. Nur Trust Authority-Administratorrechte reichen nicht aus, um alle Verwaltungsvorgänge durchzuführen, die die ESXi-Hosts beinhalten. Weitere Informationen finden Sie unter Voraussetzungen und notwendige Berechtigungen für vSphere Trust Authority.

Hinzufügen eines vertrauenswürdigen Hosts zu einem vertrauenswürdigen Cluster

Die Schritte zum erstmaligen Hinzufügen von ESXi-Hosts zum vertrauenswürdigen Cluster werden in Konfigurieren von vSphere Trust Authority beschrieben.

Wenn Sie ESXi-Hosts zu einem späteren Zeitpunkt zum vertrauenswürdigen Cluster hinzufügen möchten, muss ein anderer Workflow verwendet werden. Weitere Informationen hierzu finden Sie unter Hinzufügen und Entfernen von vSphere Trust Authority-Hosts.

Wenn Sie ESXi-Hosts erstmals zum vertrauenswürdigen Cluster hinzufügen, müssen Sie folgende Informationen zusammenstellen:

- TPM-Zertifikat für jeden Hardwaretyp im Cluster
- ESXi-Image für jede Version von ESXi im Cluster
- Informationen zum vCenter Server-Prinzipal

Wenn Sie ESXi-Hosts zu einem späteren Zeitpunkt zu einem vertrauenswürdigen Cluster hinzufügen, müssen Sie möglicherweise einige zusätzliche Informationen erfassen. Das heißt, wenn sich die neuen ESXi-Hosts in der Hardware- oder ESXi-Version von den ursprünglichen Hosts unterscheiden, müssen Sie die Informationen des neuen ESXi-Hosts zusammenstellen und in den Trust Authority-Cluster importieren. Sie müssen die Informationen zum vCenter Server-Prinzipal nur einmal pro vCenter Server-System erfassen.

vSphere Trust Authority – Topologie

vSphere Trust Authority benötigt separate vCenter Server-Systeme für den Trust Authority-Cluster und den vertrauenswürdigen Cluster.

Der Trust Authority-Cluster wird auf einem unabhängigen, isolierten vCenter Server konfiguriert und verwaltet. Der vCenter Server des Trust Authority-Clusters kann nicht gleichzeitig der vCenter Server des vertrauenswürdigen Clusters sein. Der vertrauenswürdige Cluster muss über einen eigenen, separaten vCenter Server verfügen. Ein einzelner vCenter Server kann mehrere vertrauenswürdige Cluster verwalten. Mehrere vCenter Server-Systeme für vertrauenswürdige Cluster können am erweiterten verknüpften Modus teilnehmen. Der vCenter Server für den Trust Authority-Cluster kann nicht mit anderen vCenter Server-Systemen des Trust Authority-Clusters oder mit vCenter Server-Systemen des vertrauenswürdigen Clusters am erweiterten verknüpften Modus teilnehmen.

Der Trust Authority-Administrator verwaltet den Trust Authority-Cluster und den zugehörigen vCenter Server unabhängig von anderen vCenter Server-Instanzen, da diese Vorgehensweise optimale Sicherheitsisolierung bietet.

Der Trust Authority-Administrator dokumentiert oder veröffentlicht die Hostnamen und SSL-Zertifikate, die von Administratoren vertrauenswürdiger Cluster zum Konfigurieren ihrer Cluster verwendet werden. Der Trust Authority-Administrator stellt auch vertrauenswürdige Schlüsselanbieter für das Unternehmen und seine Abteilungen oder sogar für einzelne Administratoren bereit.

Sie können vSphere Trust Authority-Dienste nicht direkt auf dem vertrauenswürdigen Cluster bereitstellen, der vom Arbeitslast-vCenter Server verwaltet wird, da der Arbeitslastadministrator über weitreichende Zugriffsrechte auf die ESXi-Hosts verfügt. Bei diesem Bereitstellungstyp wird die erforderliche Rollentrennung nicht erreicht, die zum Erfüllen der Sicherheitsziele von vSphere Trust Authority notwendig ist.

Voraussetzungen und notwendige Berechtigungen für vSphere Trust Authority

Bei der Konfiguration von vSphere Trust Authority müssen Sie die Hardware- und Softwareanforderungen berücksichtigen. Zur Verwendung von Verschlüsselung müssen Sie Kryptografieberechtigungen und -rollen festlegen. Der Benutzer, der vSphere Trust Authority-Aufgaben durchführt, muss über die entsprechenden Berechtigungen verfügen.

Anforderungen für vSphere Trust Authority

Zur Verwendung von vSphere Trust Authority muss die vSphere-Umgebung folgende Voraussetzungen erfüllen:

- Hardwareanforderungen für vertrauenswürdigen ESXi-Host:
  - TPM 2.0
  - Sicherer Start muss aktiviert sein
  - EFI-Firmware
- Anforderungen an Komponenten:
  - vCenter Server 7.0 oder höher
  - Ein dediziertes vCenter Server-System für den vSphere Trust Authority-Cluster und ESXi-Hosts
  - Ein separates vCenter Server-System für den vertrauenswürdigen Cluster und vertrauenswürdige ESXi-Hosts
  - Ein Schlüsselserver (in früheren vSphere-Versionen als Schlüsselverwaltungsserver oder KMS bezeichnet)
- Anforderungen an virtuelle Maschinen:
  - EFI-Firmware

- Sicherer Start ist aktiviert

Hinweis Stellen Sie vor der Konfiguration von vSphere Trust Authority sicher, dass Sie Ihre vCenter Server-Systeme für den Trust Authority- und den vertrauenswürdigen Cluster eingerichtet und jedem Cluster ESXi-Hosts hinzugefügt haben.

vSphere Trust Authority und Kryptografierechte

vSphere Trust Authority führt keine neuen Kryptografieberechtigungen ein. Die in Verwenden von Kryptografieberechtigungen und -rollen beschriebenen Kryptografieberechtigungen gelten ebenfalls für vSphere Trust Authority.

vSphere Trust Authority und Hostverschlüsselungsmodus

vSphere Trust Authority führt keine neuen Anforderungen für die Aktivierung des Hostverschlüsselungsmodus auf den vertrauenswürdigen ESXi-Hosts ein. Weitere Informationen zum Hostverschlüsselungsmodus finden Sie unter Voraussetzungen und erforderliche Berechtigungen für VM-Verschlüsselungsaufgaben.

Verwenden der vSphere Trust Authority-Rollen und zur TrustedAdmins-Gruppe

vSphere Trust Authority-Vorgänge benötigen einen Benutzer, der Mitglied der TrustedAdmins-Gruppe ist. Dieser Benutzer wird als Trust Authority-Administrator bezeichnet. vSphere-Administratoren müssen sich entweder selbst oder andere Benutzer zur TrustedAdmins-Gruppe hinzufügen, um die Rolle „Administrator der vertrauenswürdigen Infrastruktur“ zu erhalten. Die Rolle „Administrator der vertrauenswürdigen Infrastruktur“ ist für vCenter Server-Autorisierung erforderlich. Die TrustedAdmins-Gruppe wird für die Authentifizierung auf den ESXi-Hosts benötigt, die Teil der vertrauenswürdigen Infrastruktur sind. Benutzer mit der Berechtigung **Kryptografische Vorgänge.Host registrieren** für ESXi-Hosts können den vertrauenswürdigen Cluster verwalten. Die vCenter Server-Berechtigungen werden nicht an die Trust Authority-Hosts, sondern nur an die vertrauenswürdigen Hosts weitergegeben. Nur Mitgliedern der TrustedAdmins-Gruppe werden Berechtigungen auf den Trust Authority-Hosts erteilt. Die Gruppenmitgliedschaft wird auf dem ESXi-Host selbst überprüft.

Hinweis vSphere-Administratoren und Mitgliedern der Administratorgruppe wird die Rolle „Administrator der vertrauenswürdigen Infrastruktur“ zugewiesen. Diese Rolle allein erlaubt einem Benutzer jedoch nicht, vSphere Trust Authority-Vorgänge durchzuführen. Mitgliedschaft in der TrustedAdmins-Gruppe ist ebenfalls erforderlich.

Nachdem vSphere Trust Authority aktiviert wurde, können Trust Authority-Administratoren vertrauenswürdige Schlüsselanbieter zu vertrauenswürdigen Hosts zuweisen. Diese vertrauenswürdigen Hosts können dann die vertrauenswürdigen Schlüsselanbieter verwenden, um kryptografische Aufgaben durchzuführen.

Neben der Rolle „Administrator der vertrauenswürdigen Infrastruktur“ stellt vSphere Trust Authority die Rolle „Kein Administrator der vertrauenswürdigen Infrastruktur“ bereit, die alle Berechtigungen in vCenter Server enthält, mit Ausnahme derjenigen, die die vSphere Trust Authority-APIs aufrufen.

vSphere Trust Authority-Gruppen, -Rollen und -Benutzer funktionieren folgendermaßen:

- Beim ersten Start erteilt vSphere der TrustedAdmins-Gruppe die Rolle „Administrator der vertrauenswürdigen Infrastruktur“, die über globale Berechtigungen verfügt.
- Bei der Rolle „Administrator der vertrauenswürdigen Infrastruktur“ handelt es sich um eine Systemrolle, die über die erforderlichen Berechtigungen zum Aufrufen der vSphere Trust Authority-APIs (`TrustedAdmin.*`) sowie über die Systemrechte **System.Read**, **System.View** und **System.Anonymous** zum Anzeigen von Bestandslistenobjekten verfügt.
- Die Rolle „Kein Administrator der vertrauenswürdigen Infrastruktur“ ist eine Systemrolle, die alle Berechtigungen in vCenter Server enthält, mit Ausnahme derjenigen, die die vSphere Trust Authority-APIs aufrufen. Wenn Sie neue Berechtigungen zu vCenter Server hinzufügen, werden diese ebenfalls zur Rolle „Kein Administrator der vertrauenswürdigen Infrastruktur“ hinzugefügt. (Die Rolle „Kein Administrator der vertrauenswürdigen Infrastruktur“ ist mit der Rolle „Kein Kryptografie-Administrator“ vergleichbar.)
- Die vSphere Trust Authority-Berechtigungen (`TrustedAdmin.*`-APIs) sind nicht in der Rolle „Kein Kryptografie-Administrator“ enthalten, sodass Benutzer mit dieser Rolle keine vertrauenswürdige Infrastruktur einrichten oder Kryptografievorgänge durchführen können.

Die Anwendungsfälle für diese Benutzer, Gruppen und Rollen werden in der folgenden Tabelle angezeigt.

Tabelle 9-3. vSphere Trust Authority-Benutzer, -Gruppen und -Rollen

Benutzer, Gruppe oder Rolle	Kann vSphere Trust Authority vCenter Server-API aufrufen (enthält Aufrufe an vSphere Trust Authority ESXi-API)	Kann vSphere Trust Authority vCenter Server-API aufrufen (enthält keine Aufrufe an vSphere Trust Authority ESXi-API)	Kann Hostvorgänge im Cluster durchführen, die nicht mit vSphere Trust Authority zusammenhängen	Kommentar
Benutzer in der Gruppe „Administrators@*system.domain*“ und in der Gruppe „TrustedAdmins@*system.domain*“	Ja	Ja	Ja	–
Nur Benutzer in der Gruppe „TrustedAdmins@*system.domain*“	Ja	Ja	Nein	Ein solcher Benutzer kann keine regelmäßigen Clusterverwaltungsvorgänge durchführen.
Nur Benutzer in der Gruppe „Administrators@*system.domain*“	Ja	Nein	Ja	–

Tabelle 9-3. vSphere Trust Authority-Benutzer, -Gruppen und -Rollen (Fortsetzung)

Benutzer, Gruppe oder Rolle	Kann vSphere Trust Authority vCenter Server-API aufrufen (enthält Aufrufe an vSphere Trust Authority ESXi-API)	Kann vSphere Trust Authority vCenter Server-API aufrufen (enthält keine Aufrufe an vSphere Trust Authority ESXi-API)	Kann Hostvorgänge im Cluster durchführen, die nicht mit vSphere Trust Authority zusammenhängen	Kommentar
Benutzer mit der Rolle „Administrator der vertrauenswürdigen Infrastruktur“, die aber kein Mitglied der Gruppe „TrustedAdmins@*system.domain*“ sind	Ja	Nein	Nein	Der ESXi-Host überprüft die Gruppenmitgliedschaft des Benutzers, um Berechtigungen zu erteilen.
Nur Benutzer mit der Rolle „Kein Administrator der vertrauenswürdigen Infrastruktur“	Nein	Nein	Ja	Ein solcher Benutzer ähnelt einem Administrator, der keine vSphere Trust Authority-Vorgänge durchführen kann.

vSphere Trust Authority – Best Practices, Einschränkungen und Interoperabilität

Aus der vSphere Trust Authority-Architektur ergeben sich einige zusätzliche Empfehlungen. Berücksichtigen Sie bei der Planung Ihrer vSphere Trust Authority-Strategie Einschränkungen bezüglich der Interoperabilität.

Vertrauenswürdige Infrastruktur – Interoperabilität

Für ESXi-Versionen ist der Bestätigungsdienst rückwärts und vorwärts kompatibel. Beispiel: Sie können über einen Cluster aus ESXi-Host verfügen, die unter ESXi 7.0 im vSphere Trust Authority -Cluster ausgeführt werden, und ESXi-Hosts im vertrauenswürdigen Cluster auf eine neuere ESXi-Version upgraden oder patchen. Ebenso können Sie die ESXi-Hosts im Trust Authority-Cluster aktualisieren oder patchen, während für die ESXi-Hosts im vertrauenswürdigen Cluster die aktuelle Version beibehalten wird.

Ein Cluster kann nicht gleichzeitig als Trust Authority- und vertrauenswürdiger Cluster fungieren. Diese Konfiguration wird nicht unterstützt.

Konfigurationseinschränkungen bei vertrauenswürdigen Clustern

Sie können nur einen Trust Authority-Cluster pro Arbeitslast-vCenter Server konfigurieren. Ein vertrauenswürdiger Cluster kann nicht so konfiguriert werden, dass er auf mehrere Trust Authority-Cluster verweist.

In vSphere Trust Authority unterstützte vSphere-Funktionen

vSphere Trust Authority unterstützt Folgendes:

- vCenter High Availability (vCenter HA)
- VMware vSphere High Availability
- DRS
- DPM
- SRM unter folgenden Voraussetzungen:
  - SRM mit Array-basierter Replizierung wird unterstützt, wenn auf der Wiederherstellungsseite dieselbe vSphere Trust Authority-Dienstkonfiguration verfügbar ist.
  - SPPG
- VADP
  - Die Unterstützung entspricht derjenigen bei der Standardverschlüsselung. Die Modi „Hot-Add“ und „NFC“ werden unterstützt, der SAN-Modus jedoch nicht. Sicherungen werden entschlüsselt. VADP-Partner können die gesicherte virtuelle Maschine mit demselben Verschlüsselungsschlüssel wiederherstellen, den sie auch für die ursprüngliche virtuelle Maschine verwenden.
- vSAN
  - VM-Verschlüsselung wird zusätzlich zu vSAN vollständig unterstützt.
- OVF
  - Verschlüsselte virtuelle Maschinen können nicht in OVF exportiert werden. Virtuelle Maschinen können jedoch verschlüsselt werden, während Sie aus einer OVF-Datei importiert werden.
- vVol

In vSphere Trust Authority nicht unterstützte vSphere-Funktionen

Aktuell bietet vSphere Trust Authority keine Unterstützung für Folgendes:

- Verschlüsselung ruhender vSAN-Daten
- FCD-Verschlüsselung (First Class Disk)
- vSphere Replication
- vSphere-Hostprofile

vSphere Trust Authority – Lebenszyklus

Die vSphere Trust Authority-Dienste werden als Teil des ESXi-Basis-Image in Paketen zusammengefasst und installiert.

Starten und Beenden von vSphere Trust Authority-Diensten

Im vSphere Client können Sie die vSphere Trust Authority-Dienste starten, beenden und neu starten, die auf einem ESXi-Host ausgeführt werden. Sie können Dienste im Fall einer Konfigurationsänderung oder bei vermuteten Funktions- oder Leistungsproblemen neu starten. Zum Neustarten des Diensts auf einem vertrauenswürdigen ESXi-Host, müssen Sie sich beim Host anmelden, um den Dienst neu zu starten. Weitere Informationen hierzu finden Sie unter Starten, Stoppen und Neustarten von vSphere Trust Authority-Diensten.

Upgraden und Patchen der vSphere Trust Authority

Jedes Mal, wenn Sie einen vertrauenswürdigen ESXi-Host upgraden oder patchen, müssen Sie den vSphere Trust Authority-Cluster mit den Informationen der neuen ESXi-Version aktualisieren. Eine Möglichkeit besteht darin, ein Upgrade oder ein Patch für einen ESXi-Testhost durchzuführen, die ESXi-Basisimage-Informationen zu exportieren, die Image-Datei in den Trust Authority-Cluster zu importieren und anschließend die vertrauenswürdigen ESXi-Hosts zu aktualisieren oder zu patchen.

Best Practices für Upgrades der vSphere Trust Authority

Best Practice für das Upgrade einer vSphere Trust Authority-Infrastruktur bestehen darin, das Upgrade von Trust Authority vCenter Server und der Trust Authority-Hosts zuerst durchzuführen. Auf diese Weise profitieren Sie von den neuesten vSphere Trust Authority-Funktionen.
Sie können jedoch getrennte, eigenständige Upgrades von vCenter Server und ESXi-Hosts ausführen, um bestimmte geschäftliche Voraussetzungen zu erfüllen.

Befolgen Sie im Allgemeinen diese Reihenfolge für das Upgrade Ihrer vSphere Trust Authority-Infrastruktur:

1 Führen Sie ein Upgrade des vCenter Servers des Trust Authority Clusters durch.

2 Führen Sie ein Upgrade der Trust Authority-Hosts durch.

3 Führen Sie ein Upgrade des vCenter Servers des vertrauenswürdigen Clusters durch.

4 Führen Sie ein Upgrade der vertrauenswürdigen Hosts durch.

Um einen reibungslosen Ablauf zu gewährleisten, führen Sie das Upgrade der Trust Authority-Hosts und der vertrauenswürdigen Hosts schrittweise durch.

Upgrade von vSphere Trust Authority mit vertrauenswürdigen, mittels Quick Boot gestarteten ESXi-Hosts

Bei Quick Boot handelt es sich um eine Einstellung, die Sie in Verbindung mit Clustern verwenden können, die Sie mit vSphere Lifecycle Manager-Images und vSphere Lifecycle Manager-Baselines verwalten. Mithilfe von Quick Boot werden die Vorgänge zum ESXi-Host-Patching und -Upgrade optimiert.

Wenn Sie ein Upgrade eines ESXi-Hosts mithilfe der Quick Boot-Optimierung durchführen, meldet der Hostnachweis weiterhin die zuvor gestartete ESXi-Version bei der Messung des Vertrauensankers.

Wenn Sie also ein Upgrade eines vertrauenswürdigen ESXi-Hosts durchführen, der für Quick Boot aktiviert ist und Teil einer vSphere Trust Authority-Bereitstellung ist, achten Sie auf Folgendes:

1 Entfernen Sie die ESXi-Basisimage-Version, die Sie anfänglich als vertrauenswürdig eingestuft haben, erst dann aus dem Nachweisdienst, wenn alle ESXi-Hosts nach dem Upgrade einen vollständigen Neustart abgeschlossen haben. (Wenn Sie den Host neu starten müssen, deaktivieren Sie Quick Boot.)

2 Wenn Sie Quick Boot für mehrere Upgrades verwendet haben und eine ESXi-Zwischenversion entfernen möchten, die nicht mehr vertrauenswürdig ist, verwenden Sie die `base-images`-API, um die ESXi-Version zu bestätigen, die Sie zuletzt nachgewiesen haben.

3 Wenn Sie das ESXi-Basisimage eines für Quick Boot aktivierten ESXi-Hosts exportieren, wird eine Meldung angezeigt, dass ein Upgrade des Hosts durch Quick Boot durchgeführt wurde. Die resultierende Datei enthält die neuesten Metadaten des ESXi-Basisimages.

Wenn Sie die Hosts eines regulären Clusters mithilfe von Quick Boot aktualisieren und diesen Cluster später zu vSphere Trust Authority hinzufügen, werden die Hosts erst nach dem Neustart bestätigt. Der Nachweisfehler tritt auf, weil die exportierte ESXi-Basisimage-Datei der Hosts nur die aktuellen Metadaten enthält, während der Hostnachweis auf den Metadaten des letzten vollständigen Starts basiert. Wenn der Cluster also nicht zu vSphere Trust Authority gehört und die Metadaten des ESXi-Basisimages für den vollständigen Neustart nicht in vSphere Trust Authority importiert werden, schlägt der Nachweis fehl.

Zum Abrufen des Basisimages können Sie die folgenden PowerCLI-Befehle verwenden.

```
$vTA = Get-TrustAuthorityCluster -name trustedCluster
$bm = Get-TrustAuthorityVMHostBaseImage $vTA
$bm | select *
```

Fehlerbehebung bei vSphere Trust Authority-Upgrade-Problemen

Führen Sie die folgenden Schritte aus, wenn das Upgrade eines Trust Authority-Hosts nicht erfolgreich war.

1 Entfernen Sie den Trust Authority-Host aus dem vertrauenswürdigen Cluster.

2 Stellen Sie die vorherige Version von ESXi wieder her.

3 Fügen Sie den Trust Authority-Host erneut zum Cluster hinzu, wie im VMware Knowledgebase-Artikel unter https://kb.vmware.com/s/article/77234 beschrieben.

4 Stellen Sie sicher, dass die Konfiguration des Trust Authority-Hosts mit den anderen Trust Authority-Hosts im Trust Authority-Cluster übereinstimmt. Weitere Informationen hierzu finden Sie unter Überprüfen der Integrität des vertrauenswürdigen Clusters.

Wenn Sie ein Upgrade auf eine neue Version von ESXi auf einem vertrauenswürdigen Host durchführen, schlägt der Nachweis fehl, bis Sie den Trust Authority-Cluster mit den neuen ESXi-Basisimage-Informationen aktualisieren. Dieses Verhaltensmuster wird erwartet. Sie können virtuelle Maschinen nicht mehr verschlüsseln und keine vorhandenen virtuellen Maschinen verwenden, die vor dem Upgrade verschlüsselt wurden, bis Sie das Problem beheben. Nachweisfehlermeldungen werden im vSphere Client im Bereich **Kürzlich bearbeitete Aufgaben** und in den Dateien `attestd.log`, `kmxa.log` und `kmxa.log` angezeigt.

Um das Problem zu beheben, gehen Sie folgendermaßen vor.

1 Führen Sie das `Export-VMHostImageDb`-Cmdlet aus, um die ESXi-Basisimages erneut zu exportieren. Weitere Informationen finden Sie in Schritt 5 in Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.

2 Führen Sie das `New-TrustAuthorityVMHostBaseImage`-Cmdlet aus, um das neue Basisimage erneut in den vCenter Server des Trust Authority-Clusters zu importieren. Weitere Informationen finden Sie in Schritt 8 in Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.

3 Wenn Sie die älteren Versionen von ESXi nicht mehr bestätigen müssen (alle vertrauenswürdigen Hosts wurden aktualisiert), führen Sie das `Remove-TrustAuthorityVMHostBaseImage`-Cmdlet aus, um die Versionen zu entfernen. Beispiel:

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
$baseImages = Get-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
Remove-TrustAuthorityVMHostBaseImage -VMHostBaseImage $baseImages
```

Sichern der vSphere Trust Authority-Konfiguration

Da die meisten vSphere Trust Authority-Konfigurationsinformationen auf den ESXi-Hosts gespeichert werden, erfolgt keine vCenter Server-Sicherung dieser vSphere Trust Authority-Informationen. Weitere Informationen hierzu finden Sie unter Sichern der vSphere Trust Authority-Konfiguration.

Konfigurieren von vSphere Trust Authority

vSphere Trust Authority ist standardmäßig nicht aktiviert. Sie müssen Ihre Umgebung für vSphere Trust Authority konfigurieren, bevor Sie diese nutzen können.

Sie aktivieren die vSphere Trust Authority-Dienste auf einem dedizierten vCenter Server-Cluster, der als vSphere Trust Authority-Cluster bezeichnet wird. Der Trust Authority-Cluster fungiert als eine zentralisierte, sichere Managementplattform. Anschließend aktivieren Sie einen vCenter Server-Cluster als vertrauenswürdigen Cluster. Der vertrauenswürdige Cluster enthält die vertrauenswürdigen ESXi-Hosts.

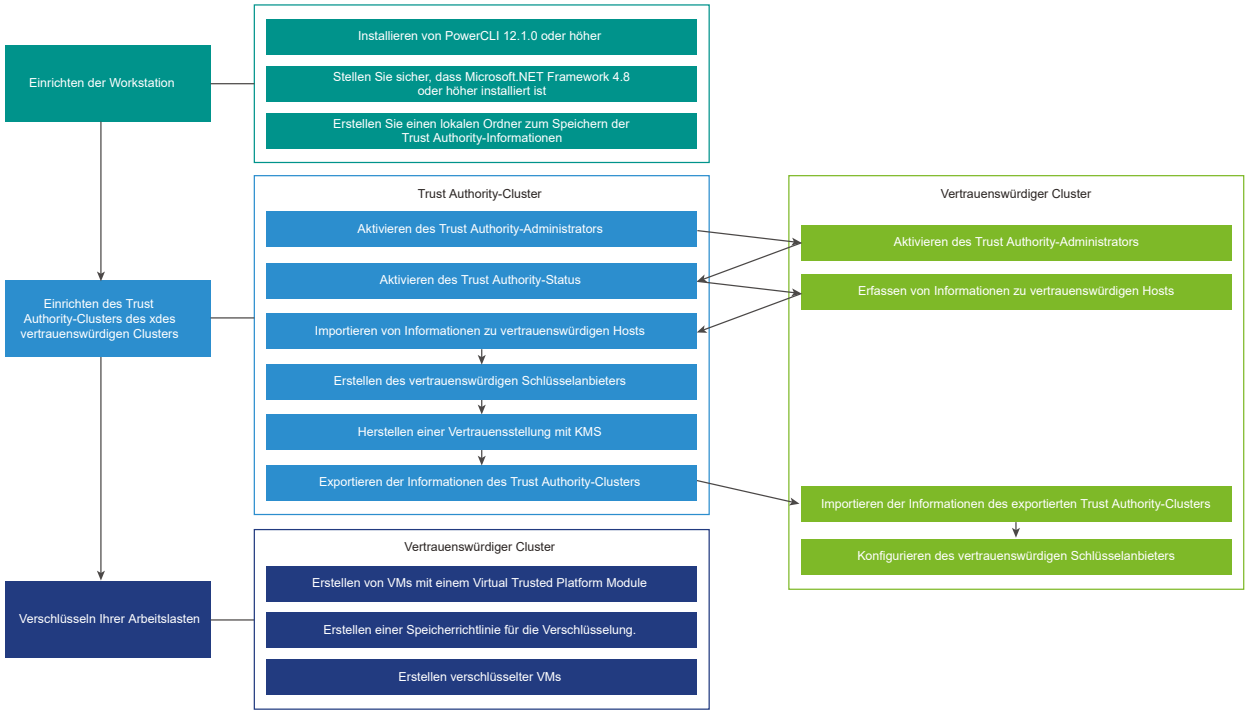
Der Trust Authority-Cluster testet die ESXi-Hosts im vertrauenswürdigen Cluster remote. Der Trust Authority-Cluster gibt Verschlüsselungsschlüssel nur an nachgewiesene ESXi-Hosts im vertrauenswürdigen Cluster frei, um virtuelle Maschinen und virtuelle Festplatten mithilfe vertrauenswürdiger Schlüsselanbieter zu verschlüsseln.

Bevor Sie mit der Konfiguration von vSphere Trust Authority beginnen, finden Sie Informationen zur erforderlichen Einrichtung von vCenter Server-Systemen und ESXi-Hosts unter Voraussetzungen und notwendige Berechtigungen für vSphere Trust Authority.

Sie können verschiedene Aspekte von vSphere Trust Authority auf folgende Arten verwalten.

- Konfigurieren Sie die vSphere Trust Authority-Dienste und vertrauenswürdige Verbindungen mithilfe von PowerCLI-Cmdlets oder vSphere-APIs. Weitere Informationen finden Sie in der *Referenz für VMware PowerCLI-Cmdlets* und im *Programmierhandbuch zu den vSphere Automation SDKs*.
- Verwalten Sie die Konfiguration vertrauenswürdiger Schlüsselanbieter mithilfe der PowerCLI-Cmdlets oder über den vSphere Client.
- Führen Sie Verschlüsselungs-Workflows wie in früheren vSphere-Versionen mit vSphere Client und APIs durch.

Abbildung 9-4. vSphere Trust Authority-Workflow



Zum Konfigurieren und Verwalten von vSphere Trust Authority verwenden Sie VMware PowerCLI, obwohl bestimmte Funktionen im vSphere Client verfügbar sind.

Wenn Sie vSphere Trust Authority konfigurieren, müssen Sie die Einrichtungsaufgaben sowohl für den Trust Authority-Cluster als auch für den vertrauenswürdigen Cluster abschließen. Bei einigen dieser Aufgaben muss eine bestimmte Reihenfolge eingehalten werden. Verwenden Sie die in diesem Handbuch beschriebene Aufgabensequenz.

Hinweis Beim Hinzufügen weiterer ESXi-Hosts zum vertrauenswürdigen Cluster, nachdem Sie die anfängliche vSphere Trust Authority-Einrichtung abgeschlossen haben, müssen Sie möglicherweise die Informationen zum vertrauenswürdigen Host erneut exportieren und importieren. Das heißt, wenn sich die neuen ESXi-Hosts von den ursprünglichen Hosts unterscheiden, müssen Sie die Informationen des neuen ESXi-Hosts zusammenstellen und in den Trust Authority-Cluster importieren. Weitere Informationen hierzu finden Sie unter Hinzufügen und Entfernen von vSphere Trust Authority-Hosts.

Weitere Themen zum Lesen

Verfahren

1 Einrichten Ihrer Workstation zum Konfigurieren von vSphere Trust Authority

   Um eine vSphere Trust Authority-Bereitstellung zu konfigurieren, müssen Sie zur Vorbereitung zunächst die erforderliche Software auf einer Workstation installieren und diese einrichten.

2 Aktivieren des Trust Authority-Administrators

   Zum Aktivieren von vSphere Trust Authority müssen Sie einen Benutzer zur TrustedAdmins-Gruppe in vSphere hinzufügen. Dieser Benutzer übernimmt die Funktion des Trust Authority-Administrators. Sie verwenden den Trust Authority-Administrator für die meisten vSphere Trust Authority-Konfigurationsaufgaben.

3 Aktivieren des Trust Authority-Status

   Durch Umwandeln eines vCenter Server-Clusters in einen vSphere Trust Authority-Cluster (auch bezeichnet als Aktivieren des Trust Authority-Status) werden die notwendigen Trust Authority-Dienste auf den ESXi-Hosts im Cluster gestartet.

4 Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server

   Zum Aufbau einer Vertrauensstellung benötigt der vSphere Trust Authority-Cluster Informationen über die ESXi-Hosts und den vCenter Server des vertrauenswürdigen Clusters. Sie exportieren diese Informationen als Dateien, die in den Trust Authority-Cluster importiert werden. Sie müssen sicherstellen, dass diese Dateien vertraulich behandelt und sicher übertragen werden.

5 Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster

   Sie importieren den exportierten ESXi-Host und die vCenter Server-Informationen in den vSphere Trust Authority-Cluster, um den Trust Authority-Cluster über die zu bestätigenden Hosts zu informieren.

6 Erstellen des Schlüsselanbieters im Trust Authority-Cluster

Damit der Schlüsselanbieterdienst eine Verbindung mit einem Schlüsselanbieter herstellen kann, müssen Sie einen vertrauenswürdigen Schlüsselanbieter erstellen und dann eine vertrauenswürdige Verbindung zwischen dem vSphere Trust Authority-Cluster und dem Schlüsselserver (KMS) konfigurieren. Für die meisten KMIP-kompatiblen Schlüsselserver beinhaltet diese Konfiguration die Einrichtung von Client- und Serverzertifikaten.

7 Exportieren der Informationen des Trust Authority-Clusters

Damit der vertrauenswürdige Cluster eine Verbindung mit dem vSphere Trust Authority-Cluster herstellen kann, müssen Sie die Dienstinformationen des Trust Authority-Clusters in Form einer Datei exportieren und diese Datei dann in den vertrauenswürdigen Cluster importieren. Sie müssen sicherstellen, dass diese Datei vertraulich behandelt und sicher übertragen wird.

8 Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts

Nachdem Sie die Informationen des vSphere Trust Authority-Clusters in den vertrauenswürdigen Cluster importiert haben, starten die vertrauenswürdigen Hosts den Bestätigungsvorgang mit dem Trust Authority-Cluster.

9 Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe des vSphere Client

Sie können den vertrauenswürdigen Schlüsselanbieter mithilfe des vSphere Client konfigurieren.

10 Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe der Befehlszeile

Sie können vertrauenswürdige Schlüsselanbieter über die Befehlszeile konfigurieren. Sie können den vertrauenswürdigen Standardschlüsselanbieter für den vCenter Server oder auf Cluster- oder Ordnerebene in der vCenter-Objekthierarchie konfigurieren.

Einrichten Ihrer Workstation zum Konfigurieren von vSphere Trust Authority

Um eine vSphere Trust Authority-Bereitstellung zu konfigurieren, müssen Sie zur Vorbereitung zunächst die erforderliche Software auf einer Workstation installieren und diese einrichten.

Führen Sie auf einer Workstation mit Zugriff auf Ihre vSphere Trust Authority-Umgebung die folgenden Schritte aus.

Verfahren

1 Installieren Sie PowerCLI 12.1.0 oder höher. Weitere Informationen finden Sie im *PowerCLI-Benutzerhandbuch*.

2 Stellen Sie sicher, dass Microsoft .NET Framework 4.8 oder höher installiert ist.

3 Erstellen Sie einen lokalen Ordner, in dem die Trust Authority-Informationen, die Sie als Dateien exportieren, gespeichert werden.

Nächste Schritte

Fahren Sie mit Aktivieren des Trust Authority-Administrators fort.

Aktivieren des Trust Authority-Administrators

Zum Aktivieren von vSphere Trust Authority müssen Sie einen Benutzer zur TrustedAdmins-Gruppe in vSphere hinzufügen. Dieser Benutzer übernimmt die Funktion des Trust Authority-Administrators. Sie verwenden den Trust Authority-Administrator für die meisten vSphere Trust Authority-Konfigurationsaufgaben.

Verwenden Sie einen anderen Benutzer als den vCenter Server-Administrator als Trust Authority-Administrator. Durch Verwendung eines anderen Benutzers wird die Sicherheit Ihrer Umgebung verbessert. Sie müssen einen Trust Authority-Administrator dem Trust Authority-Cluster und dem vertrauenswürdigen Cluster hinzufügen.

Voraussetzungen

Erstellen Sie entweder einen Benutzer oder identifizieren Sie einen vorhandenen Benutzer als Trust Authority-Administrator.

Verfahren

1. Stellen Sie eine Verbindung zum vSphere Client des Trust Authority-Clusters her, indem Sie den vCenter Server verwenden.
2. Melden Sie sich als Administrator an.
3. Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
4. Klicken Sie unter **Single Sign-On** auf **Benutzer und Gruppen**.
5. Klicken Sie auf **Gruppen** und dann auf die Gruppe **TrustedAdmins**.

   Wenn die Gruppe TrustedAdmins zunächst nicht angezeigt wird, verwenden Sie das **Filter**-Symbol, um nach ihr zu filtern, oder navigieren Sie durch die Gruppen, indem Sie auf den Rechtspfeil am unteren Rand des Fensterspeichers klicken.
6. Klicken Sie im Bereich **Gruppenmitglieder** auf **Mitglieder hinzufügen**.

   Stellen Sie sicher, dass die lokale Identitätsquelle ausgewählt ist („vsphere.local“ ist die Standardeinstellung, aber Sie haben während der Installation möglicherweise eine andere Domäne ausgewählt) und suchen Sie nach dem Mitglied (Benutzer), das Sie der Gruppe als Trust Authority Administrator hinzufügen möchten.
7. Wählen Sie das Mitglied aus.
8. Klicken Sie auf **Speichern**.
9. Wiederholen Sie die Schritte 1 bis 8 für den vCenter Server des vertrauenswürdigen Clusters.

Nächste Schritte

Fahren Sie mit Aktivieren des Trust Authority-Status fort.

Aktivieren des Trust Authority-Status

Durch Umwandeln eines vCenter Server-Clusters in einen vSphere Trust Authority-Cluster (auch bezeichnet als Aktivieren des Trust Authority-Status) werden die notwendigen Trust Authority-Dienste auf den ESXi-Hosts im Cluster gestartet.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.

Verfahren

1. In einer PowerCLI-Sitzung führen Sie das `Connect-VIServer`-Cmdlet aus, um als Administrator der Trust Authority mit dem vCenter Server des Trust Authority-Clusters zu verbinden.

   ```
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
   -Password 'password'
   ```

2. Führen Sie das `Get-TrustAuthorityCluster`-Cmdlet aus, um den aktuellen Status des Clusters zu überprüfen.

   Dieser Befehl zeigt z. B. den Cluster, `vTA Cluster` und dessen Status „deaktiviert“ an.

   ```
   Get-TrustAuthorityCluster

   Name                 State                Id
   ----                 -----                --
   vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8
   ```

   Die Ausgabe zeigt für jeden gefundenen Cluster entweder „Deaktiviert“ oder „Aktiviert“ in der Spalte „Status“ an. „Deaktiviert“ bedeutet, dass die Trust Authority-Dienste nicht ausgeführt werden.

3. Führen Sie das `Set-TrustAuthorityCluster`-Cmdlet zum Aktivieren des Trust Authority-Clusters aus.

   Mit diesem Befehl wird beispielsweise das Cluster `vTA Cluster` aktiviert.

   ```
   Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -State Enabled
   ```

   Das System antwortet mit einer Bestätigungsaufforderung.

   ```
   Confirmation
   Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to
   proceed?
   [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
   ```

4 Drücken Sie an der Bestätigungsaufforderung die Eingabetaste. (Der Standardwert lautet `Y`.)

Die Ausgabe zeigt den Status des Clusters an. Folgendes zeigt beispielsweise, dass Cluster `vTA Cluster` aktiviert wurde:

```
Name                State               Id
----                -----               --
vTA Cluster         Enabled             TrustAuthorityCluster-domain-c8
```

Ergebnisse

Zwei Dienste werden auf den ESXi-Hosts im Trust Authority-Cluster gestartet: der Bestätigungsdienst und der Schlüsselanbieterdienst.

Beispiel: Aktivieren des vertrauenswürdigen Status im Trust Authority-Cluster

In diesem Beispiel wird die Verwendung der PowerCLI zum Aktivieren von Diensten im Trust Authority-Cluster veranschaulicht. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-4. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
vCenter Server für Trust Authority-Cluster	192.168.210.22
Name des Trust Authority-Clusters	vTA-Cluster
Trust Authority-Administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA
Cluster' -State Enabled

Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8
```

Nächste Schritte

Fahren Sie mit Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server fort.

Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server

Zum Aufbau einer Vertrauensstellung benötigt der vSphere Trust Authority-Cluster Informationen über die ESXi-Hosts und den vCenter Server des vertrauenswürdigen Clusters. Sie exportieren diese Informationen als Dateien, die in den Trust Authority-Cluster importiert werden. Sie müssen sicherstellen, dass diese Dateien vertraulich behandelt und sicher übertragen werden.

Mithilfe von vSphere Trust Authority PowerCLI-Cmdlets exportieren Sie die folgenden Informationen als Dateien aus den ESXi-Hosts im vertrauenswürdigen Cluster, damit der Trust Authority-Cluster die vertrauenswürdige Software und Hardware erkennt.

- ESXi-Version
- TPM-Hersteller (CA-Zertifikat)
- (Optional) Einzelnes TPM (EK-Zertifikat)

Hinweis Speichern Sie diese exportierten Dateien an einem sicheren Ort für den Fall, dass Sie die vSphere Trust Authority-Konfiguration wiederherstellen müssen.

Wenn Sie über Hosts desselben Typs und Anbieters verfügen und diese im selben Zeitraum und am selben Ort hergestellt wurden, können Sie unter Umständen alle TPMs als vertrauenswürdig einstufen, indem Sie das CA-Zertifikat nur eines der TPMs abrufen. Um einem einzelnen TPM als vertrauenswürdig einzustufen, rufen Sie das EK-Zertifikat des TPM ab.

Sie müssen auch die Prinzipalinformationen aus dem vCenter Server des vertrauenswürdigen Clusters abrufen. Die Prinzipalinformationen enthalten den Lösungsbenutzer „vpxd“ sowie dessen Zertifikatskette. Mithilfe der Prinzipalinformationen kann der vCenter Server des vertrauenswürdigen Clusters die verfügbaren vertrauenswürdigen Schlüsselanbieter ermitteln, die im Trust Authority-Cluster konfiguriert sind.

Für die erstmalige Konfiguration von vSphere Trust Authority müssen Sie die ESXi-Version und die TPM-Informationen erfassen. Sie müssen auch die ESXi-Version bei jeder Bereitstellung einer neuen Version von ESXi erfassen, so auch beim Upgraden oder Anwenden eines Patches.

Sie erfassen die Informationen des vCenter Server-Prinzipals nur einmal pro vCenter Server-System.

Voraussetzungen

- Geben Sie die ESXi-Versionen und TPM-Hardwaretypen an, die sich im vertrauenswürdigen Cluster befinden, und legen Sie fest, ob Sie alle TPM-Hardwaretypen, nur bestimmte oder einzelne Hosts als vertrauenswürdig einstufen möchten.

- Erstellen Sie auf der Maschine, von der aus Sie die PowerCLI ausführen, einen lokalen Ordner, in dem die Informationen, die Sie als Dateien exportieren, gespeichert werden sollen.
- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.

Verfahren

1 Führen Sie in einer PowerCLI-Sitzung die folgenden Befehle aus, um alle bestehenden Verbindungen zu trennen und als Root-Benutzer eine Verbindung zu einem der ESXi-Hosts im vertrauenswürdigen Cluster herzustellen.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

2 Starten Sie das `Get-VMHost`-Cmdlet, um den ESXi-Host zu bestätigen.

```
Get-VMHost
```

Die Hostinformationen werden angezeigt.

3 Weisen Sie `Get-VMHost` einer Variable zu.

Beispiel:

```
$vmhost = Get-VMHost
```

4 Führen Sie das `Export-Tpm2CACertificate`-Cmdlet aus, um das CA-Zertifikat eines bestimmten TPM-Herstellers zu exportieren.

a Weisen Sie `Get-Tpm2EndorsementKey -VMHost $vmhost` einer Variable zu.

Mit diesem Befehl wird beispielsweise `Get-Tpm2EndorsementKey -VMHost $vmhost` der Variable `$tpm2` zugewiesen.

```
$tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
```

b Führen Sie das `Export-Tpm2CACertificate`-cmdlet aus.

Mit diesem Befehl wird beispielsweise das TPM-Zertifikat in die Datei `cacert.zip` exportiert. Stellen Sie vor dem Ausführen des Befehls sicher, dass das Zielverzeichnis bereits vorhanden ist.

```
Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip
```

Die Datei wird erstellt.

c Wiederholen Sie den Vorgang für jeden TPM-Hardwaretyp im Cluster, den Sie als vertrauenswürdig einstufen möchten. Verwenden Sie einen anderen Dateinamen für jeden TMP-Hardwaretyp, sodass Sie eine zuvor exportierte Datei nicht überschreiben.

5 Führen Sie das `Export-VMHostImageDb`-Cmdlet aus, um die Beschreibung der Software des ESXi-Hosts (das ESXi-Image) zu exportieren.

Mit diesem Befehl werden beispielsweise die Informationen in die Datei `image.tgz` exportiert. Stellen Sie vor dem Ausführen des Befehls sicher, dass das Zielverzeichnis bereits vorhanden ist.

```
Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz
```

Hinweis Das `Export-VMHostImageDb`-Cmdlet funktioniert auch, wenn Sie sich beim vCenter Server des vertrauenswürdigen Clusters anmelden möchten.

Die Datei wird erstellt.

Wiederholen Sie diese Schritte für jede ESXi-Version im Cluster, den Sie als vertrauenswürdig einstufen möchten. Verwenden Sie für jede Version einen anderen Dateinamen, damit Sie eine zuvor exportierte Datei nicht überschreiben.

6 Exportieren Sie die vCenter Server-Prinzipalinformationen des vertrauenswürdigen Clusters.

a Trennen Sie die Verbindung zum ESXi-Host.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Stellen Sie mithilfe des Trust Authority-Administrators eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters her. (Alternativ können Sie einen Benutzer verwenden, der über **Administrator**-Rechte verfügt.)

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

c Um die vCenter Server-Prinzipalinformationen des vertrauenswürdigen Clusters zu exportieren, führen Sie das `Export-TrustedPrincipal`-Cmdlet aus.

Mit diesem Befehl werden beispielsweise die Informationen in die Datei `principal.json` exportiert. Stellen Sie vor dem Ausführen des Befehls sicher, dass das Zielverzeichnis bereits vorhanden ist.

```
Export-TrustedPrincipal -FilePath C:\vta\principal.json
```

Die Datei wird erstellt.

7 (Optional) Wenn Sie einen einzelnen Host als vertrauenswürdig einstufen möchten, müssen Sie das TPM-Zertifikat des öffentlichen EK-Schlüssels exportieren.

Weitere Informationen hierzu finden Sie unter Exportieren und Importieren eines TPM Endorsement Key-Zertifikats.

Ergebnisse

Die folgenden Dateien werden erstellt:

- CA-Zertifikatsdatei des TPM (Dateierweiterung „zip“)
- ESXi-Image-Datei (Dateierweiterung „tgz“)
- vCenter Server-Prinzipaldatei (Dateierweiterung „json“)

Beispiel: Erfassen von Informationen zu ESXi-Hosts und zum vertrauenswürdigen vCenter Server

In diesem Beispiel wird die Verwendung der PowerCLI zum Exportieren der ESXi-Hostinformationen und der vCenter Server-Prinzipalinformationen erläutert. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-5. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
ESXi-Host im vertrauenswürdigen Cluster	192.168.110.51
vCenter Server für vertrauenswürdigen Cluster	192.168.110.22
Variable `$vmhost`	`Get-VMHost`
Variable `$tpm2`	`Get-Tpm2EndorsementKey -VMHost $vmhost`
Trust Authority-Administrator	trustedadmin@vsphere.local
Lokales Verzeichnis zum Speichern von Ausgabedateien	`C:\vta`

```
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                  443  root

PS C:\Users\Administrator.CORP> Get-VMHost

Name               ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz MemoryUsageGB
MemoryTotalGB Version
----               --------------- ---------- ------ ----------- ----------- -------------
------------- -------
192.168.110.51     Connected       PoweredOn       4         200        9576
1.614         7.999   7.0.0

PS C:\Users\Administrator.CORP> $vmhost = Get-VMHost
PS C:\Users\Administrator.CORP> $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
PS C:\> Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/8/2019   6:55 PM           1004 cacert.zip
```

```
PS C:\Users\Administrator.CORP> Export-VMHostImageDb -VMHost $vmhost -FilePath
C:\vta\image.tgz

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/8/2019  11:02 PM           2391 image.tgz

PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Export-TrustedPrincipal -FilePath C:\vta\principal.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/8/2019  11:14 PM           1873 principal.json
```

Nächste Schritte

Fahren Sie mit Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster fort.

Exportieren und Importieren eines TPM Endorsement Key-Zertifikats

Sie können ein TPM Endorsement Key (EK)-Zertifikat von einem ESXi-Host exportieren und in den vSphere Trust Authority-Cluster importieren. Führen Sie den Vorgang aus, wenn Sie einem einzelnen ESXi-Host im vertrauenswürdigen Cluster vertrauen möchten.

Um ein TPM EK-Zertifikat in den Trust Authority-Cluster zu importieren, müssen Sie den standardmäßigen Nachweistyp des Trust Authority-Clusters ändern, damit dieser die Zertifikate akzeptiert. Der standardmäßige Nachweistyp akzeptiert Zertifikate der TPM-Zertifizierungsstelle (Certificate Authority, CA). Bestimmte TPMs enthalten keine EK-Zertifikate. Wenn Sie einzelne ESXi-Hosts als vertrauenswürdig einstufen möchten, muss das TPM ein EK-Zertifikat enthalten.

Hinweis Speichern Sie die exportierten EK-Zertifikatsdateien an einem sicheren Ort für den Fall, dass Sie die vSphere Trust Authority-Konfiguration wiederherstellen müssen.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.

Verfahren

1 Stellen Sie sicher, dass Sie als Trust Authority-Administrator mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.

2 (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 So ändern Sie den Nachweistyp des Trust Authority-Clusters:

   a Führen Sie das `Get-TrustAuthorityCluster`-Cmdlet aus, um die von diesem vCenter Server verwalteten Cluster anzuzeigen.

```
Get-TrustAuthorityCluster
```

   Die Cluster werden angezeigt.

   b Weisen Sie die `Get-TrustAuthorityCluster`-Informationen einer Variable zu.

   Beispiel: Dieser Befehl weist dem Cluster mit dem Namen `vTA Cluster` der Variable `$vTA` zu.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

   c Weisen Sie die `Get-TrustAuthorityTpm2AttestationSettings`-Informationen einer Variable zu.

   Beispiel: Dieser Befehl weist die Informationen der Variable `$tpm2Settings` zu.

```
$tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA
```

d Starten Sie das `Set-TrustAuthorityTpm2AttestationSettings`-Cmdlet, indem Sie `RequireEndorsementKey` oder `RequireCertificateValidation` oder beides angeben.

Beispiel: Dieser Befehl gibt `RequireEndorsementKey` an.

```
Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings $tpm2Settings
-RequireEndorsementKey
```

Das System antwortet mit einer Bestätigungseingabeaufforderung ähnlich der folgenden.

```
Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-
c8' with the following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

e Drücken Sie an der Bestätigungsaufforderung die Eingabetaste. (Der Standardwert lautet **`Y`**.)

Die Ausgabe zeigt den Status „true“ für die angegebene Einstellung an. Beispiel: Dieser Status zeigt „true“ für „Endorsement Key anfordern“ und „false“ für „Zertifikatvalidierung anfordern“ an.

```
Name                                    RequireEndorsementKey
RequireCertificateValidation   Health
----                                    ---------------------
----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok
```

4 So exportieren Sie das TPM EK-Zertifikat:

a Trennen Sie die Verbindung mit dem vCenter Server des Trust Authority-Clusters.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Führen Sie das `Connect-VIServer`-Cmdlet aus, um als Root-Benutzer eine Verbindung zu einem der ESXi-Hosts im vertrauenswürdigen Cluster herzustellen.

```
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

c Starten Sie das `Get-VMHost`-Cmdlet, um den ESXi-Host zu bestätigen.

```
Get-VMHost
```

Die Hostinformationen werden angezeigt.

d Weisen Sie `Get-VMHost` einer Variable zu.

Beispiel:

```
$vmhost = Get-VMHost
```

e Führen Sie das `Export-Tpm2EndorsementKey`-Cmdlet zum Exportieren des EK-Zertifikats des ESXi-Hosts aus.

Beispiel: Mit diesem Befehl wird das EK-Zertifikat in die Datei `tpm2ek.json` exportiert.

```
Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath C:\vta\tpm2ek.json
```

Die Datei wird erstellt.

5 So importieren Sie das TPM EK:

a Trennen Sie die Verbindung mit dem ESXi-Host im vertrauenswürdigen Cluster.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Stellen Sie mithilfe des Trust Authority-Administrators eine Verbindung zum vCenter Server des Trust Authority-Clusters her.

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

c Führen Sie das `Get-TrustAuthorityCluster`-cmdlet aus.

```
Get-TrustAuthorityCluster
```

Die Cluster im Trust Authority-Cluster werden angezeigt.

d Weisen Sie die *Cluster*-Informationen von `Get-TrustAuthorityCluster` einer Variable zu.

Beispiel: Dieser Befehl weist die Informationen für Cluster `vTA Cluster` der Variable `$vTA` zu.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

e Führen Sie das `New-TrustAuthorityTpm2EndorsementKey`-cmdlet aus.

Beispiel: Dieser Befehl verwendet die `tpm2ek`-Datei, die zuvor in Schritt 4 exportiert wurde.

```
New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA -FilePath
C:\vta\tpm2ek.json
```

Die importierten Endorsement Key-Informationen werden angezeigt.

Ergebnisse

Der Nachweistyp des Trust Authority-Clusters wird geändert, um die EK-Zertifikate zu akzeptieren. Das EK-Zertifikat wird aus dem vertrauenswürdigen Cluster exportiert und in den Trust Authority-Cluster importiert.

Beispiel: Exportieren und Importieren eines TPM EK-Zertifikats

Dieses Beispiel zeigt, wie Sie PowerCLI verwenden können, um den standardmäßigen Nachweistyp des Trust Authority-Clusters zu ändern, um EK-Zertifikate zu akzeptieren, das TPM EK-Zertifikat vom ESXi-Host im vertrauenswürdigen Cluster zu exportieren und es in den Trust Authority-Cluster zu importieren. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-6. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
vCenter Server für Trust Authority-Cluster	192.168.210.22
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
Variable `$tpm2Settings`	`Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA`
Variable `$vmhost`	`Get-VMHost`
ESXi-Host im vertrauenswürdigen Cluster	192.168.110.51
Trust Authority-Administrator	trustedadmin@vsphere.local
Lokales Verzeichnis zum Speichern von Ausgabedateien	`C:\vta`

```
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State               Id
----                 -----               --
vTA Cluster          Enabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'

PS C:\Users\Administrator> $tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings
-TrustAuthorityCluster $vTA

PS C:\Users\Administrator> Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings
$tpm2Settings -RequireEndorsementKey

Confirmation
```

```
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-c8' with
the following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                                    RequireEndorsementKey
RequireCertificateValidation   Health
----                                    ---------------------
----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                 443   root

PS C:\Users\Administrator> Get-VMHost

Name                 ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz
MemoryUsageGB   MemoryTotalGB Version
----                 --------------- ---------- ------ ----------- -----------
-------------   ------------- -------
192.168.110.51       Connected       PoweredOn       4          55        9576
1.230           7.999   7.0.0

PS C:\Users\Administrator> $vmhost = Get-VMHost
PS C:\Users\Administrator> Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath
C:\vta\tpm2ek.json

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        12/3/2019  10:16 PM           2391 tpm2ek.json

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State               Id
----                 -----               --
vTA Cluster          Enabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster ‘vTA Cluster’
PS C:\Users\Administrator> New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA
-FilePath C:\vta\tpm2ek.json
```

```
TrustAuthorityClusterId                  Name                                    Health
-----------------------                  ----                                    ------
TrustAuthorityCluster-domain-c8          1a520e42-4db8-1cbb-6dd7-f493fd921ccb    Ok
```

Nächste Schritte

Fahren Sie mit Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster fort.

Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster

Sie importieren den exportierten ESXi-Host und die vCenter Server-Informationen in den vSphere Trust Authority-Cluster, um den Trust Authority-Cluster über die zu bestätigenden Hosts zu informieren.

Während Sie diese Aufgaben in der angegebenen Reihenfolge ausführen, bleiben Sie weiterhin mit dem vCenter Server des Trust Authority-Clusters verbunden.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.

Verfahren

1. Stellen Sie sicher, dass Sie als Trust Authority-Administrator mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.

2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
   -Password 'password'
   ```

3. Führen Sie zur Anzeige der von diesem vCenter Server verwalteten Cluster das Cmdlet `Get-TrustAuthorityCluster` aus.

   ```
   Get-TrustAuthorityCluster
   ```

   Die Cluster werden angezeigt.

4 Weisen Sie die *Cluster*-Informationen von `Get-TrustAuthorityCluster` einer Variable zu.

Beispiel: Dieser Befehl weist die Informationen für Cluster `vTA Cluster` der Variable `$vTA` zu.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

5 Führen Sie zum Importieren der vCenter Server-Prinzipalinformationen des vertrauenswürdigen Clusters in den Trust Authority-Cluster das `New-TrustAuthorityPrincipal`-Cmdlet aus.

Mit dem folgenden Befehl wird beispielsweise die Datei `principal.json` importiert, die zuvor in Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server exportiert wurde.

```
New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA -FilePath C:\vta\principal.json
```

Die Trust Authority-Prinzipalinformationen werden angezeigt.

6 Führen Sie das `Get-TrustAuthorityPrincipal`-Cmdlet aus, um den Import zu überprüfen.

Beispiel:

```
Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
```

Die importierten Trust Authority-Prinzipalinformationen werden angezeigt.

7 Um die Informationen über das TPM-CA-Zertifikat (Trusted Platform Module, Vertrauenswürdiges Plattformmodul) zu importieren, führen Sie das `New-TrustAuthorityTpm2CACertificate`-Cmdlet aus.

Beispiel: Mit dem folgenden Befehl werden die TPM-CA-Zertifikatsinformationen aus der Datei `cacert.zip` importiert, die zuvor nach Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server exportiert wurde.

```
New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster $vTA -FilePath
C:\vta\cacert.zip
```

Die importierten Zertifikatinformationen werden angezeigt.

8 Um die Basisimage-Informationen des ESXi-Hosts zu importieren, führen Sie das `New-TrustAuthorityVMHostBaseImage`-Cmdlet aus.

Beispiel: Mit dem folgenden Befehl werden die Image-Informationen aus der Datei `image.tgz` importiert, die zuvor nach Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server exportiert wurde.

```
New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA -FilePath C:\vta\image.tgz
```

Die importierten Bildinformationen werden angezeigt.

Ergebnisse

Der Trust Authority-Cluster kennt die ESXi-Hosts, die er remote bestätigen und denen er somit vertrauen kann.

Beispiel: Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster

Dieses Beispiel zeigt, wie Sie PowerCLI verwenden können, um die vCenter Server-Prinzipalinformationen über den vertrauenswürdigen Cluster sowie die Informationsdateien über den vertrauenswürdigen Host in den Trust Authority-Cluster zu importieren. Es wird davon ausgegangen, dass Sie als Trust Authority-Administrator mit dem vCenter Server des Trust Authority-Clusters verbunden sind. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-7. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster1'`
vCenter Server für Trust Authority-Cluster	192.168.210.22
Namen der Trust Authority-Cluster	vTA-Cluster1 (Aktiviert) vTA-Cluster2 (Deaktiviert)
Datei mit Prinzipalinformationen	`C:\vta\principal.json`
TPM-Zertifikatsdatei	`C:\vta\cacert.cer`
ESXi-Basisimage-Datei des Hosts	`C:\vta\image.tgz`
Trust Authority-Administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster1         Enabled              TrustAuthorityCluster-domain-c8
vTA Cluster2         Disabled             TrustAuthorityCluster-domain-c26

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster1'

PS C:\Users\Administrator.CORP> New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
-FilePath C:\vta\principal.json

Name                                          Domain          Type
```

```
TrustAuthorityClusterId
----                                        ------          ----
-----------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f    vsphere.local   STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA

Name                                        Domain          Type
TrustAuthorityClusterId
----                                        ------          ----
-----------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f    vsphere.local   STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster
$vTA -FilePath C:\vta\cacert.cer

TrustAuthorityClusterId                 Name                                    Health
-----------------------                 ----                                    ------
TrustAuthorityCluster-domain-c8         52BDB7B4B2F55C925C047257DED4588A7767D961 Ok

PS C:\Users\Administrator.CORP> New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
-FilePath C:\vta\image.tgz

TrustAuthorityClusterId                 VMHostVersion                           Health
-----------------------                 -------------                           ------
TrustAuthorityCluster-domain-c8         ESXi 7.0.0-0.0.14828939                 Ok
```

Nächste Schritte

Fahren Sie mit Erstellen des Schlüsselanbieters im Trust Authority-Cluster fort.

Erstellen des Schlüsselanbieters im Trust Authority-Cluster

Damit der Schlüsselanbieterdienst eine Verbindung mit einem Schlüsselanbieter herstellen kann, müssen Sie einen vertrauenswürdigen Schlüsselanbieter erstellen und dann eine vertrauenswürdige Verbindung zwischen dem vSphere Trust Authority-Cluster und dem Schlüsselserver (KMS) konfigurieren. Für die meisten KMIP-kompatiblen Schlüsselserver beinhaltet diese Konfiguration die Einrichtung von Client- und Serverzertifikaten.

Was zuvor in vSphere 6.7 als KMS-Cluster bezeichnet wurde, heißt in vSphere 7.0 und höher nun Schlüsselanbieter. Weitere Informationen zu Speicheranbietern finden Sie unter Was ist der vSphere Trust Authority-Schlüsselanbieterdienst?.

In einer Produktionsumgebung können Sie mehrere Schlüsselanbieter erstellen. Indem Sie mehrere Schlüsselanbieter erstellen, können Sie festlegen, wie Ihre Bereitstellung basierend auf Unternehmensorganisation, verschiedenen Geschäftsbereichen oder Kunden usw. verwaltet werden soll.

Wenn Sie diese Aufgaben nacheinander ausführen, sind Sie weiterhin mit dem vCenter Server des vSphere Trust Authority-Clusters verbunden.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen und aktivieren Sie einen Schlüssel auf dem Schlüsselserver, der der primäre Schlüssel für den vertrauenswürdigen Schlüsselanbieter sein soll. Dieser Schlüssel umhüllt andere Schlüssel und Geheimnisse, die von diesem vertrauenswürdigen Schlüsselanbieter verwendet werden. Weitere Informationen zum Erstellen von Schlüsseln finden Sie in der Dokumentation des Schlüsselserverherstellers.

Verfahren

1. Stellen Sie sicher, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.
2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
   -Password 'password'
   ```

3. Um einen vertrauenswürdigen Schlüsselanbieter zu erstellen, führen Sie das `New-TrustAuthorityKeyProvider`-Cmdlet aus.

   Dieser Befehl verwendet beispielsweise `1` für die PrimaryKeyID und den Namen `clkp`. Wenn Sie diese Aufgaben nacheinander ausführen, haben Sie die `Get-TrustAuthorityCluster`-Informationen zuvor einer Variable zugewiesen (z. B. `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

   ```
   New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA -PrimaryKeyId 1 -Name clkp
   -KmipServerAddress ip_address
   ```

   Die PrimaryKeyID ist in der Regel eine Schlüssel-ID, die in Form einer UUID aus dem Schlüsselserver stammt. Verwenden Sie für PrimaryKeyID nicht den Schlüsselnamen. Der PrimaryKeyID-Wert ist vom Anbieter abhängig. Informationen finden Sie in der Dokumentation des Schlüsselservers. Das `New-TrustAuthorityKeyProvider`-Cmdlet kann andere Optionen wie z. B. `KmipServerPort`, `ProxyAddress` und `ProxyPort` nutzen. Weitere Informationen finden Sie im `New-TrustAuthorityKeyProvider`-Hilfesystem.

   Jeder logische Schlüsselanbieter muss unabhängig von seinem Typ (Standard-, vertrauenswürdiger und nativer Schlüsselanbieter) über einen eindeutigen Namen in allen vCenter Server-Systemen verfügen.

Weitere Informationen finden Sie unter Benennung des Schlüsselanbieters.

Hinweis Um dem Schlüsselanbieter mehrere Schlüsselserver hinzuzufügen, verwenden Sie das `Add-TrustAuthorityKeyProviderServer`-Cmdlet.

Informationen zum Schlüsselanbieter werden angezeigt.

4 Stellen Sie die vertrauenswürdige Verbindung sicher, sodass der Schlüsselserver dem vertrauenswürdigen Schlüsselanbieter vertraut. Der genaue Prozess hängt von den Zertifikaten, die vom Schlüsselserver akzeptiert werden, sowie von der Unternehmensrichtlinie ab. Wählen Sie die entsprechende Option für den Server aus und schließen Sie die Schritte ab.

Option	Informationen hierzu finden Sie unter
Clientzertifikat hochladen	Hochladen des Clientzertifikats zum Herstellen einer vertrauenswürdigen Verbindung des vertrauenswürdigen Schlüsselanbieters.
KMS-Zertifikat und privaten Schlüssel hochladen	Zertifikat und privaten Schlüssel zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters hochladen.
Neue Zertifikatssignieranforderung	Eine Zertifikatssignieranforderung zum Herstellen einer vertrauenswürdigen Schlüsselanbieter-Verbindung erstellen.

5 Schließen Sie das Trust-Setup ab, indem Sie ein Schlüsselserverzertifikat hochladen, damit der vertrauenswürdige Schlüsselanbieter dem Schlüsselserver vertraut.

a Weisen Sie die `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA-` Informationen einer Variable zu.

Beispiel:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Diese Variable erhält die vertrauenswürdigen Schlüsselanbieter im Trust Authority-Cluster, in diesem Fall `$vTA`.

Hinweis Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, verwenden Sie Befehle ähnlich den folgenden, um den gewünschten Anbieter auszuwählen:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Mit `Select-Object -Last 1` wird der letzte vertrauenswürdige Schlüsselanbieter in der Liste angezeigt.

b Führen Sie den Befehl `Get-TrustAuthorityKeyProviderServerCertificate` aus, um das Serverzertifikat des Schlüsselservers abzurufen.

Beispiel:

```
Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
```

Die Serverzertifikatinformationen werden angezeigt. Anfänglich ist das Zertifikat nicht als vertrauenswürdig eingestuft, d. h., der vertrauenswürdige Zustand lautet „False“. Wenn Sie mehr als einen Schlüsselserver konfiguriert haben, wird eine Zertifikatsliste zurückgegeben. Überprüfen Sie jedes Zertifikat und fügen Sie jedes davon hinzu, indem Sie die folgenden Anweisungen befolgen.

c Bevor Sie dem Zertifikat vertrauen, weisen Sie die Informationen aus `Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers` einer Variablen zu (z. B. `cert`), führen Sie den Befehl `$cert.Certificate.ToString()` aus und überprüfen Sie die Ausgabe.

Beispiel:

```
$cert = Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
$cert.Certificate.ToString()
```

Die Zertifikatsinformationen werden angezeigt, einschließlich Thema, Aussteller und sonstiger Informationen.

d Um dem vertrauenswürdigen Schlüsselanbieter das KMIP-Serverzertifikat hinzuzufügen, führen Sie `Add-TrustAuthorityKeyProviderServerCertificate` aus.

Beispiel:

```
Add-TrustAuthorityKeyProviderServerCertificate -ServerCertificate $cert
```

Die Zertifikatsinformationen werden angezeigt und der vertrauenswürdige Zustand lautet nun „True“.

6 Überprüfen Sie den Status des Schlüsselanbieters.

a Um den Schlüsselanbieterstatus zu aktualisieren, weisen Sie die `$kp`-Variable neu zu.

Beispiel:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Hinweis Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, verwenden Sie Befehle ähnlich den folgenden, um den gewünschten Anbieter auszuwählen:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Mit `Select-Object -Last 1` wird der letzte vertrauenswürdige Schlüsselanbieter in der Liste angezeigt.

b Führen Sie den Befehl `$kp.Status` aus, um den Schlüsselanbieterstatus anzuzeigen.

Beispiel:

```
$kp.Status
```

Hinweis Die Statusaktualisierung kann einige Minuten dauern. Um den Status anzuzeigen, weisen Sie die Variable `$kp` erneut zu und führen Sie den Befehl `$kp.Status` erneut aus.

Ein Systemzustand von „OK“ weist darauf hin, dass der Schlüsselanbieter ordnungsgemäß ausgeführt wird.

Ergebnisse

Der vertrauenswürdige Schlüsselanbieter wurde erstellt und hat eine vertrauenswürdige Verbindung mit dem Schlüsselserver hergestellt.

Beispiel: Erstellen des Schlüsselanbieters im Trust Authority-Cluster

Dieses Beispiel zeigt, wie Sie den vertrauenswürdigen Schlüsselanbieter mithilfe der PowerCLI im Trust Authority-Cluster erstellen können. Es wird davon ausgegangen, dass Sie als Trust Authority-Administrator mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Zudem wird ein Zertifikat verwendet, das vom Schlüsselserveranbieter signiert wurde, nachdem eine CSR an den Anbieter übermittelt wurde.

In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-8. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
Variable `$kp`	`Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`
Variable `$cert`	`Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers`
vCenter Server für Trust Authority-Cluster	192.168.210.22
KMIP-kompatibler Schlüsselserver	192.168.110.91
KMIP-konformer Schlüsselserverbenutzer	vcqekmip
Name des Trust Authority-Clusters	vTA-Cluster
Trust Authority-Administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
-PrimaryKeyId 8 -Name clkp -KmipServerAddress 192.168.110.91
Name                 PrimaryKeyId         Type       TrustAuthorityClusterId
----                 ------------         ----       -----------------------
clkp                 8                    KMIP       TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProviderClientCertificate -KeyProvider
$kp
<Export the client certificate when you need to use it.>
PS C:\Users\Administrator.CORP> Export-TrustAuthorityKeyProviderClientCertificate
-KeyProvider $kp -FilePath clientcert.pem

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers

Certificate                              Trusted    KeyProviderServerId       KeyProviderId
-----------                              -------    -------------------       -------------
[Subject]...                             False      domain-c8-clkp:192.16.... domain-c8-clkp

PS C:\WINDOWS\system32> $cert.Certificate.ToString()
[Subject]
  E=<domain>, CN=<IP address>, OU=VMware Engineering, O=VMware, L=Palo Alto, S=California,
C=US

[Issuer]
  O=<host>.eng.vmware.com, C=US, DC=local, DC=vsphere, CN=CA

[Serial Number]
```

```
  00CEF192BBF9D80C9F

[Not Before]
  8/10/2015 4:16:12 PM

[Not After]
  8/9/2020 4:16:12 PM

[Thumbprint]
  C44068C124C057A3D07F51DCF18720E963604B70

PS C:\Users\Administrator.CORP> $cert = Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers
PS C:\Users\Administrator.CORP> Add-TrustAuthorityKeyProviderServerCertificate
-ServerCertificate $cert

Certificate                              Trusted    KeyProviderServerId       KeyProviderId
-----------                              -------    -------------------       -------------
[Subject]...                             True                                 domain-c8-clkp

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> $kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {192.168.210.22}
```

Nächste Schritte

Fahren Sie mit Exportieren der Informationen des Trust Authority-Clusters fort.

Hochladen des Clientzertifikats zum Herstellen einer vertrauenswürdigen Verbindung des vertrauenswürdigen Schlüsselanbieters

Bestimmte Schlüsselserver-Anbieter (KMS) fordern, dass Sie das Clientzertifikat des vertrauenswürdigen Schlüsselanbieters auf den Schlüsselserver hochladen. Nach dem Upload akzeptiert der Schlüsselserver den Datenverkehr, der von dem vertrauenswürdigen Schlüsselanbieter stammt.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.

Verfahren

1 Stellen Sie sicher, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.

2 (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 Weisen Sie die `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`-Informationen einer Variable zu.

Beispiel:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Wenn Sie diese Aufgaben nacheinander ausführen, haben Sie die `Get-TrustAuthorityCluster`-Informationen zuvor einer Variable zugewiesen (z. B. `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

Diese Variable erhält die vertrauenswürdigen Schlüsselanbieter im Trust Authority-Cluster, in diesem Fall `$vTA`.

Hinweis Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, verwenden Sie Befehle ähnlich den folgenden, um den gewünschten Anbieter auszuwählen:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Mit `Select-Object -Last 1` wird der letzte vertrauenswürdige Schlüsselanbieter in der Liste angezeigt.

4 Um das Clientzertifikat des vertrauenswürdigen Schlüsselanbieters zu erstellen, führen Sie das `New-TrustAuthorityKeyProviderClientCertificate`-Cmdlet aus.

Beispiel:

```
New-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp
```

Der Fingerabdruck wird angezeigt.

5 Um das Clientzertifikat des Schlüsselanbieters zu exportieren, führen Sie das `Export-TrustAuthorityKeyProviderClientCertificate`-Cmdlet aus.

Beispiel:

```
Export-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -FilePath clientcert.pem
```

Das Zertifikat wird in eine Datei exportiert.

6 Laden Sie die Zertifikatsdatei auf den Schlüsselserver hoch.

Weitere Informationen finden Sie in der Dokumentation zum Schlüsselserver.

Ergebnisse

Der vertrauenswürdige Schlüsselanbieter hat eine Vertrauensstellung mit dem Schlüsselserver hergestellt.

Zertifikat und privaten Schlüssel zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters hochladen

Einige Anbieter von Schlüsselservern (KMS) fordern, dass Sie den vertrauenswürdigen Schlüsselanbieter mit dem Clientzertifikat und dem vom Schlüsselserver bereitgestellten privaten Schlüssel konfigurieren. Nach der Konfiguration des vertrauenswürdigen Schlüsselanbieters akzeptiert der Schlüsselserver den Datenverkehr vom vertrauenswürdigen Schlüsselanbieter.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.
- Fordern Sie ein Zertifikat und einen privaten Schlüssel im PEM-Format vom Schlüsselserver-Anbieter an. Wenn das Zertifikat in einem anderen Format als PEM zurückgegeben wird, konvertieren Sie es in PEM. Wenn der private Schlüssel mit einem Kennwort geschützt ist, erstellen Sie eine PEM-Datei mit entferntem Kennwort. Sie können den Befehl `openssl` für beide Vorgänge verwenden. Beispiel:
  - So konvertieren Sie ein Zertifikat vom CRT- in das PEM-Format:

    ```
    openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
    ```

  - So konvertieren Sie ein Zertifikat vom DER- in das PEM-Format:

    ```
    openssl x509 -inform DER -in clientcert.der -out clientcert.pem
    ```

- So entfernen Sie das Kennwort aus einem privaten Schlüssel:

```
openssl rsa -in key.pem -out keynopassword.pem
Enter pass phrase for key.pem:
writing RSA key
```

Verfahren

1. Stellen Sie sicher, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.
2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3. Weisen Sie die `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`-Informationen einer Variable zu.

   Beispiel:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

   Wenn Sie diese Aufgaben nacheinander ausführen, haben Sie die `Get-TrustAuthorityCluster`-Informationen zuvor einer Variable zugewiesen (z. B. `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

   Die `$kp`-Variable erhält die vertrauenswürdigen Schlüsselanbieter im Trust Authority-Cluster, in diesem Fall `$vTA`.

   Hinweis Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, verwenden Sie Befehle ähnlich den folgenden, um den gewünschten Anbieter auszuwählen:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

   Mit `Select-Object -Last 1` wird der letzte vertrauenswürdige Schlüsselanbieter in der Liste angezeigt.

4. Laden Sie das Zertifikat und den privaten Schlüssel mithilfe des Befehls `Set-TrustAuthorityKeyProviderClientCertificate` hoch.

   Beispiel:

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/to/certfile.pem> -PrivateKeyFilePath <path/to/privatekey.pem>
```

Ergebnisse

Der vertrauenswürdige Schlüsselanbieter hat eine Vertrauensstellung mit dem Schlüsselserver hergestellt.

Eine Zertifikatssignieranforderung zum Herstellen einer vertrauenswürdigen Schlüsselanbieter-Verbindung erstellen

Bestimmte Schlüsselserveranbieter (KMS) verlangen, dass eine Zertifikatssignieranforderung (Certificate Signing Request, CSR) generiert und an den Schlüsselserveranbieter übermittelt wird. Der Schlüsselserveranbieter signiert die Zertifikatssignieranforderung und sendet das signierte Zertifikat zurück. Nachdem Sie dieses signierte Zertifikat als Clientzertifikat des vertrauenswürdigen Schlüsselanbieters konfiguriert haben, akzeptiert der Schlüsselserveranbieter den Datenverkehr, der vom vertrauenswürdigen Schlüsselanbieter stammt.

Bei dieser Aufgabe handelt es sich um einen zweistufigen Prozess. Zuerst generieren Sie die Zertifikatssignieranforderung und senden diese an den Schlüsselserveranbieter. Anschließend laden Sie das signierte Zertifikat hoch, das Sie vom Schlüsselserveranbieter erhalten haben.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.

Verfahren

1. Stellen Sie sicher, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.
2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
   -Password 'password'
   ```

3. Weisen Sie die `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA-` Informationen einer Variable zu.

   Beispiel:

   ```
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   ```

Wenn Sie diese Aufgaben nacheinander ausführen, haben Sie die `Get-TrustAuthorityCluster`-Informationen zuvor einer Variable zugewiesen (z. B. `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

Diese Variable erhält die vertrauenswürdigen Schlüsselanbieter im Trust Authority-Cluster, in diesem Fall `$vTA`.

Hinweis Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, verwenden Sie Befehle ähnlich den folgenden, um den gewünschten Anbieter auszuwählen:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Mit `Select-Object -Last 1` wird der letzte vertrauenswürdige Schlüsselanbieter in der Liste angezeigt.

4 Verwenden Sie zum Generieren einer CSR das `New-TrustAuthorityKeyProviderClientCertificateCSR`-Cmdlet.

Beispiel:

```
New-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp
```

Die CSR wird angezeigt. Sie können auch das `Get-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp`-Cmdlet verwenden, um die CSR zu erhalten.

5 Um ein signiertes Zertifikat zu erhalten, übermitteln Sie die CSR an Ihren Schlüsselserveranbieter.

Das Zertifikat muss im PEM-Format sein. Wenn das Zertifikat in einem anderen Format als PEM zurückgegeben wird, konvertieren Sie es mithilfe des Befehls `openssl` in PEM. Beispiel:

- So konvertieren Sie ein Zertifikat vom CRT- in das PEM-Format:

  ```
  openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
  ```

- So konvertieren Sie ein Zertifikat vom DER- in das PEM-Format:

  ```
  openssl x509 -inform DER -in clientcert.der -out clientcert.pem
  ```

6 Wenn Sie das signierte Zertifikat vom Schlüsselserveranbieter erhalten, laden Sie das Zertifikat mithilfe des `Set-TrustAuthorityKeyProviderClientCertificate`-Cmdlet auf den Schlüsselserver hoch.

Beispiel:

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/tp/certfile.pem>
```

Ergebnisse

Der vertrauenswürdige Schlüsselanbieter hat eine Vertrauensstellung mit dem Schlüsselserver hergestellt.

Exportieren der Informationen des Trust Authority-Clusters

Damit der vertrauenswürdige Cluster eine Verbindung mit dem vSphere Trust Authority-Cluster herstellen kann, müssen Sie die Dienstinformationen des Trust Authority-Clusters in Form einer Datei exportieren und diese Datei dann in den vertrauenswürdigen Cluster importieren. Sie müssen sicherstellen, dass diese Datei vertraulich behandelt und sicher übertragen wird.

Während Sie diese Aufgaben in der angegebenen Reihenfolge ausführen, bleiben Sie weiterhin mit dem vCenter Server des Trust Authority-Clusters verbunden.

Hinweis Speichern Sie die exportierte Datei mit den Dienstinformationen an einem sicheren Ort für den Fall, dass Sie die vSphere Trust Authority-Konfiguration wiederherstellen müssen.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.

Verfahren

1. Stellen Sie sicher, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.
2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 Führen Sie das `Export-TrustAuthorityServicesInfo`-Cmdlet aus, um die im Trust Authority-Cluster enthaltenen Informationen des Bestätigungs- und Schlüsselanbieterdiensts zu exportieren.

   Mit diesem Befehl werden die Dienstinformationen beispielsweise in die Datei `clsettings.json` exportiert. Wenn Sie diese Aufgaben nacheinander ausführen, haben Sie die `Get-TrustAuthorityCluster`-Information zuvor einer Variable zugewiesen (z. B. `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

```
Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA -FilePath
C:\vta\clsettings.json
```

   Die Datei wird erstellt.

Ergebnisse

Eine Datei mit Informationen zum Trust Authority-Cluster wird erstellt.

Beispiel: Exportieren der Informationen des Trust Authority-Clusters

In diesem Beispiel wird die Verwendung der PowerCLI zum Exportieren der Dienstinformationen des Trust Authority-Clusters erläutert. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-9. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
vCenter Server für Trust Authority-Cluster	192.168.210.22
Trust Authority-Administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA
-FilePath C:\vta\clsettings.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----       10/16/2019   9:59 PM           8177 clsettings.json
```

Nächste Schritte

Fahren Sie mit Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts fort.

Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts

Nachdem Sie die Informationen des vSphere Trust Authority-Clusters in den vertrauenswürdigen Cluster importiert haben, starten die vertrauenswürdigen Hosts den Bestätigungsvorgang mit dem Trust Authority-Cluster.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.
- Exportieren der Informationen des Trust Authority-Clusters.

Verfahren

1. Stellen Sie sicher, dass Sie als Trust Authority-Administrator mit dem vCenter Server des vertrauenswürdigen Clusters verbunden sind.

   Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.

2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des vertrauenswürdigen Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
   'password'
   ```

   Hinweis Alternativ können Sie eine weitere PowerCLI-Sitzung starten, um eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters herzustellen.

3. Stellen Sie sicher, dass der Status des vertrauenswürdigen Clusters auf „Deaktiviert“ gesetzt ist.

   ```
   Get-TrustedCluster
   ```

   Der Status wird als „Deaktiviert“ angezeigt.

4. Weisen Sie die `Get-TrustedCluster`-Informationen einer Variable zu.

   Beispielsweise weist dieser Befehl Informationen für den Cluster `Trusted Cluster` der Variable `$TC` zu.

   ```
   $TC = Get-TrustedCluster -Name 'Trusted Cluster'
   ```

5 Bestätigen Sie den Wert der Variable durch erneute Eingabe.

Beispiel:

```
$TC
```

Die `Get-TrustedCluster`-Informationen werden angezeigt.

6 Um die Informationen zum Trust Authority-Cluster in den vCenter Server zu exportieren, führen Sie das `Import-TrustAuthorityServicesInfo`-Cmdlet aus.

Beispiel: Mit diesem Befehl werden die Dienstinformationen aus der Datei `clsettings.json` importiert, die zuvor in Exportieren der Informationen des Trust Authority-Clusters exportiert wurde.

```
Import-TrustAuthorityServicesInfo -FilePath C:\vta\clsettings.json
```

Das System antwortet mit einer Bestätigungsaufforderung.

```
Confirmation
Importing the TrustAuthorityServicesInfo into Server 'ip_address'. Do you want to proceed?

[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

7 Drücken Sie an der Bestätigungsaufforderung die Eingabetaste. (Der Standardwert lautet **Y**.)

Die Dienstinformationen für die Hosts im Trust Authority-Cluster werden angezeigt.

8 Um den vertrauenswürdigen Cluster zu aktivieren, führen Sie das `Set-TrustedCluster`-Cmdlet aus.

Beispiel:

```
Set-TrustedCluster -TrustedCluster $TC -State Enabled
```

Das System antwortet mit einer Bestätigungsaufforderung.

```
Confirmation
Setting TrustedCluster 'cluster' with new TrustedState 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

Wenn sich der vertrauenswürdige Cluster nicht in einem fehlerfreien Zustand befindet, wird die folgende Warnmeldung vor der Bestätigungsmeldung angezeigt:

```
WARNING: The TrustedCluster 'cluster' is not healthy in its TrustedClusterAppliedStatus.
This cmdlet will automatically remediate the TrustedCluster.
```

9 Drücken Sie an der Bestätigungsaufforderung die Eingabetaste. (Der Standardwert lautet `Y`.)

Der vertrauenswürdige Cluster ist aktiviert.

Hinweis Sie können den vertrauenswürdigen Cluster auch aktivieren, indem Sie den Bestätigungsdienst und den Schlüsselanbieterdienst einzeln aktivieren. Verwenden Sie die folgenden Befehle: `Add-TrustedClusterAttestationServiceInfo` und `Add-TrustedClusterKeyProviderServiceInfo`. Beispielsweise können die folgenden Befehle die Dienste einzeln für den Cluster `Trusted Cluster` aktivieren, der über zwei Schlüsselanbieter- und zwei Nachweisdienste verfügt.

```
Add-TrustedClusterAttestationServiceInfo -TrustedCluster 'Trusted Cluster'
-AttestationServiceInfo (Get-AttestationServiceInfo | Select-Object -index 0,1)
Add-TrustedClusterKeyProviderServiceInfo  -TrustedCluster 'Trusted Cluster'
-KeyProviderServiceInfo (Get-KeyProviderServiceInfo | Select-Object -index 0,1)
```

10 Stellen Sie sicher, dass der Nachweis- und Schlüsselanbieterdienst im vertrauenswürdigen Cluster konfiguriert sind.

a Weisen Sie die `Get-TrustedCluster`-Informationen einer Variable zu.

Beispielsweise weist dieser Befehl Informationen für den Cluster `Trusted Cluster` der Variable `$TC` zu.

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

b Stellen Sie sicher, dass der Bestätigungsdienst konfiguriert ist.

```
$tc.AttestationServiceInfo
```

Die Informationen des Bestätigungsdiensts werden angezeigt.

c Stellen Sie sicher, dass der Schlüsselanbieterserver konfiguriert ist.

```
$tc.KeyProviderServiceInfo
```

Die Informationen des Schlüsselanbieterdiensts werden angezeigt.

Ergebnisse

Die vertrauenswürdigen ESXi-Hosts im vertrauenswürdigen Cluster starten den Bestätigungsvorgang mit dem Trust Authority-Cluster.

Beispiel: Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts

Dieses Beispiel zeigt, wie die Dienstinformationen des Trust Authority-Clusters in den vertrauenswürdigen Cluster importiert werden. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-10. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
vCenter Server des vertrauenswürdigen Clusters	192.168.110.22
Trust Authority-Administrator	trustedadmin@vsphere.local
Name des vertrauenswürdigen Clusters	Vertrauenswürdiger Cluster
ESXi-Hosts im Trust Authority-Cluster	192.168.210.51 und 192.168.210.52
Variable `$TC`	`Get-TrustedCluster -Name 'Trusted Cluster'`

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustedCluster

Name                  State             Id
----                  -----             --
Trusted Cluster       Disabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $TC

Name                  State             Id
----                  -----             --
Trusted Cluster       Disabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> Import-TrustAuthorityServicesInfo -FilePath
C:\vta\clsettings.json

Confirmation
Importing the TrustAuthorityServicesInfo into Server '192.168.110.22'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

ServiceAddress                 ServicePort          ServiceGroup
--------------                 -----------          ------------
192.168.210.51                 443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                 443                  host-16:86f7ab6c-ad6f-4606-...
192.168.210.51                 443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                 443                  host-16:86f7ab6c-ad6f-4606-...

PS C:\Users\Administrator.CORP> Set-TrustedCluster -TrustedCluster $TC -State Enabled

Confirmation
Setting TrustedCluster 'Trusted Cluster' with new TrustedState 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

```
Name                  State             Id
----                  -----             --
Trusted Cluster       Enabled           TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $tc.AttestationServiceInfo

ServiceAddress                ServicePort          ServiceGroup
--------------                -----------          ------------
192.168.210.51                443                  host-13:dc825986-73d2-463c-...
192.168.210.52                443                  host-16:dc825986-73d2-463c-...

PS C:\Users\Administrator.CORP> $tc.KeyProviderServiceInfo

ServiceAddress                ServicePort          ServiceGroup
--------------                -----------          ------------
192.168.210.51                443                  host-13:dc825986-73d2-463c-...
192.168.210.52                443                  host-16:dc825986-73d2-463c-...
```

Nächste Schritte

Fahren Sie mit Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe des vSphere Client oder Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe der Befehlszeile fort.

Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe des vSphere Client

Sie können den vertrauenswürdigen Schlüsselanbieter mithilfe des vSphere Client konfigurieren.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.
- Exportieren der Informationen des Trust Authority-Clusters.
- Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts.

Verfahren

1. Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her.
2. Melden Sie sich als vCenter Server-Administrator oder als Administrator an, der über die Berechtigung **Kryptografievorgänge.Schlüsselserver verwalten** verfügt.

3 Wählen Sie den vCenter Server und dann **Konfigurieren** aus.

4 Wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

5 Wählen Sie **Vertrauenswürdige Schlüsselanbieter hinzufügen** aus.

Die verfügbaren vertrauenswürdigen Schlüsselanbieter werden mit dem Status „Verbunden“ angezeigt.

6 Wählen Sie einen vertrauenswürdigen Schlüsselanbieter aus und klicken Sie auf **Schlüsselanbieter hinzufügen**.

Der vertrauenswürdige Schlüsselanbieter wird als „Vertrauenswürdig“ und „Verbunden“ angezeigt. Wenn dies der erste vertrauenswürdige Schlüsselanbieter ist, den Sie hinzufügen, wird er als Standard gekennzeichnet.

Hinweis Es dauert eine gewisse Zeit, bis alle Hosts den Schlüsselanbieter abrufen können und der vCenter Server den zugehörigen Cache aktualisieren kann. Aufgrund der Art und Weise der Informationsweiterleitung müssen Sie unter Umständen einige Minuten warten, bis Sie den Schlüsselanbieter für wichtige Vorgänge auf bestimmten Hosts verwenden können.

Ergebnisse

ESXi Vertrauenswürdige Hosts können nun Kryptografievorgänge durchführen, wie z. B. das Erstellen verschlüsselter virtueller Maschinen.

Nächste Schritte

Das Verschlüsseln einer virtuellen Maschine mit einem vertrauenswürdigen Schlüsselanbieter entspricht der Benutzererfahrung bei der VM-Verschlüsselung, die erstmals in vSphere 6.5 bereitgestellt wurde. Weitere Informationen finden Sie unter Kapitel 10 Verwenden der Verschlüsselung in Ihrer vSphere-Umgebung.

Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe der Befehlszeile

Sie können vertrauenswürdige Schlüsselanbieter über die Befehlszeile konfigurieren. Sie können den vertrauenswürdigen Standardschlüsselanbieter für den vCenter Server oder auf Cluster- oder Ordnerebene in der vCenter-Objekthierarchie konfigurieren.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.
- Exportieren der Informationen des Trust Authority-Clusters.

- Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts.

Auf dem vertrauenswürdigen Cluster müssen Sie über eine Rolle verfügen, die das **Verschlüsselungsvorgänge.KMS verwalten**-Recht enthält.

Verfahren

1 Stellen Sie sicher, dass Sie als Administrator mit dem vCenter Server des vertrauenswürdigen Clusters verbunden sind.

   Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.

2 (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des vertrauenswürdigen Clusters verbunden sind.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustedCluster_VC_ip_address -User admin_user -Password 'password'
```

3 Rufen Sie den vertrauenswürdigen Schlüsselanbieter ab.

```
Get-KeyProvider
```

   Sie können die Option `-Name` *keyprovider* verwenden, um einen einzelnen vertrauenswürdigen Schlüsselanbieter anzugeben.

4 Weisen Sie die Informationen über den vertrauenswürdigen `Get-KeyProvider`-Schlüsselanbieter einer Variable zu.

   Beispiel: Dieser Befehl weist die Informationen der Variable `$workload_kp` zu.

```
$workload_kp = Get-KeyProvider
```

   Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, können Sie `Select-Object` verwenden, um einen davon auszuwählen.

```
$workload_kp = Get-KeyProvider | Select-Object -Index 0
```

5 Registrieren Sie den vertrauenswürdigen Schlüsselanbieter.

```
Register-KeyProvider -KeyProvider $workload_kp
```

   Um weitere vertrauenswürdige Schlüsselanbieter zu registrieren, wiederholen Sie die Schritte 4 und 5.

Hinweis Es dauert eine gewisse Zeit, bis alle Hosts den Schlüsselanbieter abrufen können und der vCenter Server den zugehörigen Cache aktualisieren kann. Aufgrund der Art und Weise der Informationsweiterleitung müssen Sie unter Umständen einige Minuten warten, bis Sie den Schlüsselanbieter für wichtige Vorgänge auf bestimmten Hosts verwenden können.

6 Legen Sie den zu verwendenden vertrauenswürdigen Standardschlüsselanbieter fest.

a Führen Sie folgenden Befehl aus, um den Standardschlüsselanbieter auf der vCenter Server-Ebene festzulegen.

```
Set-KeyProvider -KeyProvider $workload_kp -DefaultForSystem
```

b Führen Sie folgenden Befehl aus, um den Schlüsselanbieter auf Clusterebene festzulegen.

Dieser Befehl legt beispielsweise den Schlüsselanbieter für den `Trusted Cluster`-Cluster fest.

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'Trusted Cluster'
```

c Führen Sie folgenden Befehl aus, um den Schlüsselanbieter auf Clusterordnerebene festzulegen.

Dieser Befehl beispielsweise legt den Schlüsselanbieter für den Clusterordner `TC Folder` fest, der auf dem `workLoad`-Datencenter erstellt wurde.

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'TC Folder'
```

Nächste Schritte

Das Verschlüsseln einer virtuellen Maschine mit einem vertrauenswürdigen Schlüsselanbieter entspricht der Benutzererfahrung bei der VM-Verschlüsselung, die erstmals in vSphere 6.5 bereitgestellt wurde. Weitere Informationen finden Sie unter Kapitel 10 Verwenden der Verschlüsselung in Ihrer vSphere-Umgebung.

Verwalten vSphere Trust Authority in Ihrer vSphere-Umgebung

Nach dem Konfigurieren von vSphere Trust Authority können Sie zusätzliche Vorgänge durchführen, wie z. B. Starten und Anhalten der Dienste, Hinzufügen von Hosts zu Clustern und Anzeigen des Status des Trust Authority-Clusters.

Sie können Aufgaben mithilfe des vSphere Client, der API und der PowerCLI-Cmdlets ausführen. Weitere Informationen finden Sie im *Programmierhandbuch zum vSphere Web Services SDK*, in der *VMware PowerCLI*-Dokumentation und in der *Referenz zu VMware PowerCLI-Cmdlets*.

Starten, Stoppen und Neustarten von vSphere Trust Authority-Diensten

Sie können vSphere Trust Authority-Dienste mithilfe des vSphere Client starten, beenden und neu starten.

Die Dienste, aus denen sich vSphere Trust Authority zusammensetzt, sind der Bestätigungsdienst (attestd) und der Schlüsselanbieterdienst (kmxd).

Verfahren

1 Stellen Sie eine Verbindung zum vCenter Server des vSphere Trust Authority-Clusters her, indem Sie den vSphere Client verwenden.

2 Melden Sie sich als Administrator an.

3 Navigieren Sie zu einem ESXi-Host im Trust Authority-Cluster.

4 Klicken Sie auf **Konfigurieren** und dann unter **System** auf **Dienste**.

5 Suchen Sie nach dem attestd- und dem kmxd-Dienst.

6 Wählen Sie je nach Bedarf die Option **Neustarten**, **Starten** oder **Beenden** aus.

Anzeigen der Trust Authority-Hosts

Sie können die für einen vertrauenswürdigen Cluster konfigurierten vSphere Trust Authority-Hosts mithilfe des vSphere Client anzeigen.

Verfahren

1 Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her.

2 Melden Sie sich als Administrator an.

3 Wählen Sie die vCenter Server-Instanz aus.

4 Klicken Sie auf die Registerkarte **Konfigurieren** und wählen Sie **Trust Authority** unter **Sicherheit** aus.

   Die für den vertrauenswürdigen Cluster konfigurierten ESXi-Hosts im Trust Authority-Cluster werden angezeigt.

Anzeigen des Status des vSphere Trust Authority-Clusters

Sie können den Status des vSphere Trust Authority-Clusters mithilfe des vSphere Client anzeigen. Der Status lautet entweder „Aktiviert“ oder „Deaktiviert“.

Wenn der Status des Trust Authority-Clusters „Aktiviert“ ist, können die vertrauenswürdigen Hosts im vertrauenswürdigen Cluster mit dem Bestätigungs- und dem Schlüsselanbieterdienst kommunizieren.

Verfahren

1 Stellen Sie eine Verbindung zum vSphere Client des Trust Authority-Clusters her, indem Sie den vCenter Server verwenden.

2 Melden Sie sich als Administrator an.

3 Wählen Sie den Trust Authority-Cluster in der Objekthierarchie aus.

4 Klicken Sie auf die Registerkarte **Konfigurieren** und wählen Sie **Trust Authority-Cluster** unter **Trust Authority** aus.

   Der Status wird als „Aktiviert“ oder „Deaktiviert“ angezeigt.

Neustarten des Diensts für vertrauenswürdige Hosts

Sie können den Dienst, der auf Ihren vertrauenswürdigen Hosts ausgeführt wird, neu starten.

Der kmxa-Dienst wird auf den vertrauenswürdigen ESXi-Hosts ausgeführt.

Voraussetzungen

Zugriff auf die ESXi Shell muss aktiviert sein. Weitere Informationen hierzu finden Sie unter Aktivieren des Zugriffs auf ESXi Shell mithilfe des vSphere Client.

Verfahren

1 Verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung auf dem vertrauenswürdigen ESXi-Host zu starten.

2 Melden Sie sich als „root“ an.

3 Führen Sie den folgenden Befehl aus.

```
/etc/init.d/kmxa restart
```

Hinzufügen und Entfernen von vSphere Trust Authority-Hosts

Sie fügen ESXi-Hosts einem vSphere Trust Authority-Cluster hinzu und entfernen sie mithilfe von Skripts, die seitens VMware bereitgestellt werden.

In vSphere 7.0 fügen Sie ESXi-Hosts einem vorhandenen vSphere Trust Authority-Cluster oder einem vertrauenswürdigen Cluster hinzu und entfernen sie mithilfe von Skripts, die seitens VMware bereitgestellt werden. In vSphere 7.0 Update 1 und höher verwenden Sie die Standardisierungsfunktion, um ESXi-Hosts zu einem vorhandenen vertrauenswürdigen Cluster hinzuzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mit dem vSphere Client und Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mithilfe der Befehlszeile.

In vSphere 7.0 Update 1 und höher müssen Sie weiterhin Skripts verwenden, um ESXi-Hosts zu einem vorhandenen Trust Authority-Cluster hinzuzufügen. Weitere Informationen finden Sie in den VMware-Knowledgebase-Artikeln unter https://kb.vmware.com/s/article/77234 und https://kb.vmware.com/s/article/77146.

Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mit dem vSphere Client

Sie können ESXi-Hosts mithilfe des vSphere Client einem vorhandenen vertrauenswürdigen Cluster hinzufügen.

Nachdem Sie zunächst einen vertrauenswürdigen Cluster konfiguriert haben, möchten Sie unter Umständen weitere ESXi-Hosts hinzufügen. Wenn Sie den Host jedoch einem vertrauenswürdigen Cluster hinzufügen, müssen Sie in einem zusätzlichen Schritt eine Standardisierung durchführen. Stellen Sie beim Standardisieren des vertrauenswürdigen Clusters sicher, dass der gewünschte Konfigurationszustand mit der angewendeten Konfiguration übereinstimmt.

In der ersten in vSphere 7.0 veröffentlichten Version von vSphere Trust Authority können Sie Skripts zum Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster ausführen. In vSphere 7.0 Update 1 und höher verwenden Sie die Standardisierungsfunktion, um einen Host zu einem vertrauenswürdigen Cluster hinzuzufügen. In vSphere 7.0 Update 1 und höher müssen Sie weiterhin Skripts verwenden, um einen Host zu einem vorhandenen Trust Authority-Cluster hinzuzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen und Entfernen von vSphere Trust Authority-Hosts.

Voraussetzungen

Auf dem vCenter Server für den vertrauenswürdigen Cluster muss vSphere 7.0 Update 1 oder höher ausgeführt werden.

Wenn Sie einen ESXi-Host mit einer anderen ESXi-Version oder einem anderen TPM-Hardwaretyp als dem anfänglich für den vertrauenswürdigen Cluster konfigurierten Typ hinzufügen, sind weitere Schritte notwendig. Sie müssen diese Informationen in den vSphere Trust Authority-Cluster importieren oder daraus exportieren. Siehe Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server und Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.

Notwendige Berechtigungen: Weitere Informationen finden Sie in den Aufgaben zum Hinzufügen von Hosts unter Erforderliche vCenter Server-Rechte für allgemeine Aufgaben

Verfahren

1. Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her.
2. Melden Sie sich als Trust Authority-Administrator an.
3. Navigieren Sie zu einem vertrauenswürdigen Cluster.
4. Wählen Sie auf der Registerkarte **Konfigurieren** die Option **Konfiguration > Schnellstart** aus.
5. Klicken Sie auf der Karte **Hosts hinzufügen** auf **Hinzufügen**.
6. Führen Sie die angezeigten Anweisungen aus.
7. Klicken Sie auf der Registerkarte **Trust Authority** auf **Standardisieren**.
8. Um sicherzustellen, dass der vertrauenswürdige Cluster fehlerfrei ist, klicken Sie auf **Integrität überprüfen**.

Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mithilfe der Befehlszeile

Sie können ESXi-Hosts mithilfe der Befehlszeile einem vorhandenen vertrauenswürdigen Cluster hinzufügen.

Nachdem Sie zunächst einen vertrauenswürdigen Cluster konfiguriert haben, möchten Sie unter Umständen weitere ESXi-Hosts hinzufügen. Wenn Sie den Host jedoch einem vertrauenswürdigen Cluster hinzufügen, müssen Sie in einem zusätzlichen Schritt eine Standardisierung durchführen. Stellen Sie beim Standardisieren des vertrauenswürdigen Clusters sicher, dass der gewünschte Konfigurationszustand mit der angewendeten Konfiguration übereinstimmt.

In der ersten in vSphere 7.0 veröffentlichten Version von vSphere Trust Authority können Sie Skripts zum Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster ausführen. In vSphere 7.0 Update 1 und höher verwenden Sie die Standardisierungsfunktion, um einen vertrauenswürdigen Host hinzuzufügen. In vSphere 7.0 Update 1 und höher müssen Sie weiterhin Skripts verwenden, um einen Host zu einem vorhandenen Trust Authority-Cluster hinzuzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen und Entfernen von vSphere Trust Authority-Hosts.

Voraussetzungen

- Auf dem vCenter Server für den vertrauenswürdigen Cluster muss vSphere 7.0 Update 1 oder höher ausgeführt werden.
- PowerCLI 12.1.0 oder höher ist notwendig.
- Notwendige Berechtigungen: Weitere Informationen finden Sie in den Aufgaben zum Hinzufügen von Hosts unter Erforderliche vCenter Server-Rechte für allgemeine Aufgaben

Verfahren

1. Führen Sie alle üblichen Schritte aus, um den ESXi-Host zum vertrauenswürdigen Cluster hinzuzufügen.
2. In einer PowerCLI-Sitzung führen Sie das Cmdlet `Connect-VIServer` aus, um als Trust Authority-Administrator eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters herzustellen.

   ```
   Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
   'password'
   ```

3. Führen Sie zum Überprüfen des Status des vertrauenswürdigen Clusters das PowerCLI-cmdlet `Get-TrustedClusterAppliedStatus` aus.

   ```
   Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
   ```

4 Wenn der vertrauenswürdige Cluster fehlerhaft ist, sollten Sie das Cmdlet `Set-TrustedCluster` mit dem Parameter `-Remediate` ausführen.

```
Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate
```

5 Um sicherzustellen, dass der vertrauenswürdige Cluster fehlerfrei ist, führen Sie das Cmdlet `Get-TrustedClusterAppliedStatus` erneut aus.

```
Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
```

Stilllegen vertrauenswürdiger Hosts in einem vertrauenswürdigen Cluster

Sie können vertrauenswürdige Hosts aus einem vertrauenswürdigen Cluster entfernen oder stilllegen. Sie können je nach Szenario einen oder alle vertrauenswürdigen Hosts in einem vertrauenswürdigen Cluster stilllegen.

Wenn Sie einen vertrauenswürdigen Host stilllegen, legt die Standardisierungsfunktion den gewünschten Status des vertrauenswürdigen Hosts auf den des nicht vertrauenswürdigen Clusters fest, auf den der Host verschoben wird. Der stillgelegte vertrauenswürdige Host wird zu einem regulären Host. Der vertrauenswürdige Cluster (aus dem der vertrauenswürdige Host verschoben wurde) verfügt weiterhin über die gewünschte Statuskonfiguration und fungiert auch weiterhin als vertrauenswürdiger Cluster.

Wenn Sie alle vertrauenswürdigen Hosts aus einem vertrauenswürdigen Cluster entfernen, legen Sie den vertrauenswürdigen Cluster still. Sie entfernen sowohl die gewünschte Statuskonfiguration als auch die angewendete Konfiguration aus den vertrauenswürdigen Hosts und dem vertrauenswürdigen Cluster und verschieben dann alle vertrauenswürdigen Hosts in einen nicht vertrauenswürdigen Cluster.

Sie können stillgelegte vertrauenswürdige Hosts in Ihrer Umgebung wiederverwenden. Beispielsweise können Sie die Hosts in einer nicht vertrauenswürdigen Infrastrukturkapazität oder als vSphere Trust Authority-Hosts wiederverwenden. Sie können die stillgelegten Hosts im selben vCenter Server oder einem anderen vCenter Server verwenden.

Weitere Informationen zur Konfiguration und Integrität des vertrauenswürdigen Clusters finden Sie unter Prüfen und Standardisieren der Integrität eines vertrauenswürdigen Clusters.

Voraussetzungen

- Auf dem vCenter Server für den vertrauenswürdigen Cluster muss vSphere 7.0 Update 1 oder höher ausgeführt werden.
- Bei Verwendung von PowerCLI wird Version 12.1.0 oder höher benötigt.

Verfahren

1 Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her.

2 Melden Sie sich als Trust Authority-Administrator an.

3 Navigieren Sie zu einem vertrauenswürdigen Cluster.

4 Legen Sie fest, wie die vertrauenswürdigen Hosts im vertrauenswürdigen Cluster stillgelegt werden sollen.

Aufgabe	Schritte
Beibehalten des gewünschten Konfigurationsstatus des vertrauenswürdigen Clusters und der verbleibenden vertrauenswürdigen Hosts	a Versetzen Sie die Hosts in den Wartungsmodus und verschieben Sie sie in einen neuen, leeren Cluster (d. h., der Cluster enthält keine Hosts). b Beenden Sie den Wartungsmodus auf den Hosts. c Klicken Sie für den neuen, leeren Cluster (nicht den vertrauenswürdigen Cluster) auf der Registerkarte **Trust Authority** auf **Standardisieren**. Bei der Standardisierung wird die vertrauenswürdige Konfiguration aus den verschobenen Hosts entfernt. Der vertrauenswürdige Cluster behält seine gewünschte Statuskonfiguration bei.

Entfernen des gewünschten und des angewendeten Konfigurationsstatus aller vertrauenswürdigen Hosts	a In einer PowerCLI-Sitzung führen Sie das Cmdlet `Connect-VIServer` aus, um als Trust Authority-Administrator eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters herzustellen.
	`Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`
	b Führen Sie das Cmdlet `Set-TrustedCluster` aus. Beispiel:
	`Set-TrustedCluster -TrustedCluster 'TrustedCluster' -State Disabled`
	Die Konfiguration der vertrauenswürdigen Infrastruktur wird aus allen vertrauenswürdigen Hosts entfernt. Außerdem wird die gewünschte Statuskonfiguration des vertrauenswürdigen Clusters entfernt.
	c Versetzen Sie alle Hosts in den Wartungsmodus und verschieben Sie sie in einen anderen Cluster.
	d Beenden Sie den Wartungsmodus auf den Hosts.

5 Um sicherzustellen, dass es sich um einen fehlerfreien vertrauenswürdigen Cluster handelt, klicken Sie auf **Integrität prüfen** auf der Registerkarte **Trust Authority** für den vertrauenswürdigen Cluster.

Nächste Schritte

Wenn Sie die spezifischen Versionen von ESXi oder die TPM-Hardware aus den stillgelegten ESXi-Hosts nicht mehr bestätigen möchten, aktualisieren Sie die Konfiguration des Trust Authority-Clusters, um optimale Sicherheit zu gewährleisten. Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/77146.

Sichern der vSphere Trust Authority-Konfiguration

Verwenden Sie die Dateien, die Sie beim Konfigurieren von vSphere Trust Authority als Trust Authority-Sicherung exportiert haben. Sie können diese Dateien zum Wiederherstellen einer

Trust Authority-Bereitstellung verwenden. Behandeln Sie die Konfigurationsdateien vertraulich und sorgen Sie für eine sichere Übertragung.

Die meisten vSphere Trust Authority-Konfigurations- und -Statusinformationen werden auf den ESXi-Hosts in der ConfigStore-Datenbank gespeichert. Die vCenter Server-Verwaltungsschnittstelle, die Sie zum Sichern einer vCenter Server-Instanz verwenden, führt keine Sicherung der Konfigurationsinformationen für vSphere Trust Authority durch. Wenn Sie die Konfigurationsdateien, die Sie beim Einrichten Ihrer vSphere Trust Authority-Umgebung exportiert haben, sicher speichern, verfügen Sie über die notwendigen Informationen zum Wiederherstellen einer vSphere Trust Authority-Konfiguration. Weitere Informationen für den Fall, dass Sie diese Informationen erzeugen müssen, finden Sie unter Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.

Ändern des primären Schlüssels eines vertrauenswürdigen Schlüsselanbieters

Sie können den primären Schlüssel eines vertrauenswürdigen Schlüsselanbieters ändern, wenn Sie z. B. den verwendeten primären Schlüssel im Turnus wechseln möchten.

Weitere Informationen zu Schlüssellebenszyklen finden Sie unter Virtuelle Maschine – Empfohlene Vorgehensweisen für die Verschlüsselung.

Voraussetzungen

Erstellen und aktivieren Sie einen Schlüssel auf dem Schlüsselserver (KMS), der als neuer primärer Schlüssel für den vertrauenswürdigen Schlüsselanbieter verwendet wird. Dieser Schlüssel umhüllt andere Schlüssel und Geheimnisse, die von diesem vertrauenswürdigen Schlüsselanbieter verwendet werden. Weitere Informationen zum Erstellen von Schlüsseln finden Sie in der Dokumentation Ihres KMS-Anbieters.

Verfahren

1 Führen Sie den Befehl `Set-TrustAuthorityKeyProvider` aus.

Beispiel:

```
Set-TrustAuthorityKeyProvider -MasterKeyId Key-ID
```

2 Überprüfen Sie den Status des Schlüsselanbieters.

a Weisen Sie `Get-TrustAuthorityCluster`-Informationen einer Variable zu.

Beispiel:

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

b Weisen Sie die `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`-Informationen einer Variable zu.

Beispiel:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

c Überprüfen Sie den Status des Schlüsselanbieters, indem Sie `$kp.Status` ausführen.

Beispiel:

```
$kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {IP_address}
```

Ein Systemzustand von „OK“ weist darauf hin, dass der Schlüsselanbieter ordnungsgemäß ausgeführt wird.

Ergebnisse

Der neue primäre Schlüssel wird für alle neuen Verschlüsselungsvorgänge verwendet. Daten, die mit dem alten primären Schlüssel verschlüsselt wurden, werden nach wie vor mit dem alten Schlüssel entschlüsselt.

Nachweisberichte für vertrauenswürdige Hosts

In vSphere Trust Authority überprüft vCenter Server den Nachweisstatus eines vertrauenswürdigen Hosts und meldet diesen. Sie können den vSphere Client verwenden, um den Nachweisstatus von vertrauenswürdigen Hosts anzuzeigen.

Was sind vSphere Trust Authority-Nachweisberichte?

vSphere Trust Authority verwendet Remotebestätigungen für vertrauenswürdige Hosts, um die Echtheit der gestarteten Software zu bestätigen. Mithilfe von Nachweisen wird sichergestellt, dass auf den vertrauenswürdigen Hosts echte VMware-Software oder von VMware signierte Partnersoftware verwendet wird. Der vCenter Server des vertrauenswürdigen Clusters kommuniziert mit dem vertrauenswürdigen Host, um einen internen Nachweisbericht zu erhalten. Der Nachweisbericht gibt an, ob der vertrauenswürdige Host über den auf dem Trust Authority-

Cluster ausgeführten Nachweisdienst bestätigt wurde oder nicht. Wenn der vertrauenswürdige Host nicht bestätigt wurde, enthält der Nachweisbericht auch eine Fehlermeldung. Der vSphere Client zeigt den Nachweisstatus eines vertrauenswürdigen Hosts an, und wenn vSphere Trust Authority oder vCenter Server den Host bestätigt haben.

Nachweisstatus „Bestanden“

Der Status „Bestanden“ gibt an, dass der vertrauenswürdige Host mit einem vSphere Trust Authority-Nachweisdienst bestätigt wurde und der interne Nachweisbericht vCenter Server zur Verfügung steht.

Nachweisstatus „Fehlgeschlagen“

Der Status „Fehlgeschlagen“ weist darauf hin, dass der vertrauenswürdige Host keinen vSphere Trust Authority-Nachweisdienst bestätigen konnte. Der interne vCenter Server-Nachweisbericht enthält den Fehler, der vom Nachweisdienst gemeldet wurde, bei dem die Bestätigung des vertrauenswürdigen Hosts versucht wurde.

Umgang mit nicht bestätigten vertrauenswürdigen Hosts

Wenn ein vertrauenswürdiger Host nicht bestätigt ist, sind virtuelle Maschinen, einschließlich verschlüsselter virtueller Maschinen, die auf dem vertrauenswürdigen Host ausgeführt werden, weiterhin zugänglich. Virtuelle Maschinen können auf einem nicht bestätigten vertrauenswürdigen Host nicht eingeschaltet werden. Sie können jedoch weiterhin unverschlüsselte virtuelle Maschinen hinzufügen. Wenn ein vertrauenswürdiger Host nicht bestätigt ist, ergreifen Sie die Schritte, um das Nachweisproblem zu beheben. Weitere Informationen finden Sie unter Beheben von Problemen beim Nachweis des vertrauenswürdigen Hosts.

Mehrere Trust Authority-Hosts und Nachweisberichte

Wenn Sie mehrere Trust Authority-Hosts konfiguriert haben, sind potenziell mehrere Nachweisberichte von jedem Host verfügbar. Wenn Status gemeldet werden, zeigt der vSphere Client den Status des ersten gefundenen „Bestätigt“-Berichts. Wenn keine „Bestätigt“-Berichte vorliegen, zeigt der vSphere Client den Fehler des ersten „Nicht bestätigt“-Bericht, den er findet.

Selbst wenn Sie mehrere vertrauenswürdige Trust Authority-Hosts konfiguriert haben, zeigt der vSphere Client den Status und potenziell eine Fehlermeldung aus nur einem Nachweisbericht an.

Anzeigen des Nachweisstatus des vertrauenswürdigen Clusters

Sie können den Nachweisstatus eines vertrauenswürdigen Hosts mithilfe des vSphere Client anzeigen.

Voraussetzungen

- Sowohl die vertrauenswürdigen Hosts als auch die vSphere Trust Authority-Hosts müssen ESXi Version 7.0 Update 1 oder höher ausführen.

- Die vCenter Server-Hosts für die entsprechenden Cluster müssen vSphere 7.0 Update 1 oder höher ausführen.

Verfahren

1. Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her.
2. Melden Sie sich als Administrator an.

   Sie können sich als Trust Authority-Administrator oder als vSphere-Administrator anmelden.
3. Navigieren Sie zu einem Datencenter und klicken Sie auf die Registerkarte **Überwachen**.
4. Klicken Sie auf **Sicherheit**.
5. Überprüfen Sie den Status des vertrauenswürdigen Hosts in der Spalte „Integritätsnachweis“ und lesen Sie die begleitende Nachricht in der Spalte „Nachricht“.

Nächste Schritte

Wenn Fehler auftreten, finden Sie weitere Informationen unter Beheben von Problemen beim Nachweis des vertrauenswürdigen Hosts.

Beheben von Problemen beim Nachweis des vertrauenswürdigen Hosts

Die vSphere Trust Authority-Nachweisberichte bieten einen Ansatzpunkt für die Fehlerbehebung bei der Behebung von Nachweisfehlern für vertrauenswürdige Hosts.

Verfahren

1. Anzeigen des Nachweisstatus des vertrauenswürdigen Clusters.
2. Verwenden Sie die folgende Tabelle, um Fehler zu ermitteln und zu beheben.

Error	Ursache und Lösung
Die Nachweisdienste sind nicht konfiguriert.	Es wurden keine Nachweisdienste konfiguriert. Konfigurieren Sie den vertrauenswürdigen Host für die Verwendung von Nachweisdiensten, indem Sie die Standardisierungsaktion verwenden. Weitere Informationen hierzu finden Sie unter Standardisieren eines vertrauenswürdigen Clusters.
Kein TPM2-Gerät verfügbar.	Installieren und konfigurieren Sie den vertrauenswürdigen Host für die Verwendung eines Trusted Platform Module (TPM). Informationen finden Sie in der Dokumentation des Anbieters.
Öffentlicher TPM2 Endorsement Key oder Zertifikat konnte nicht abgerufen werden.	Stellen Sie sicher, dass das TPM unterstützt wird und dass es über einen gültigen Endorsement Key verfügt. Möglicherweise müssen Sie sich an den VMware Support wenden.
Der Nachweisbericht ist nicht verfügbar.	Es ist möglich, dass der vertrauenswürdige Host den Nachweis noch nicht abgeschlossen hat. Warten Sie einige Minuten, und überprüfen Sie den Nachweisstatus erneut.
Die Nachweisdienstversion ist nicht mit der Anforderung kompatibel.	Aktualisieren Sie den Host der Trust Authority, auf dem der Nachweisdienst ausgeführt wird, auf vSphere 7.0 Update 1 oder höher.

Error	Ursache und Lösung
Der Nachweis ist fehlgeschlagen, da der sichere Start nicht aktiviert ist.	Überprüfen Sie, ob der vertrauenswürdige Host für die Verwendung von Secure Boot konfiguriert ist. Weitere Informationen hierzu finden Sie unter UEFI Secure Boot für ESXi-Hosts.
Die Remotesoftwareversion konnte durch den Nachweis nicht ermittelt werden.	Importieren Sie die Basisimage-Informationen des vertrauenswürdigen Hosts in den Nachweisdienst. Weitere Informationen hierzu finden Sie unter Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
Der Nachweis ist fehlgeschlagen, da ein TPM-Zertifikat erforderlich ist.	Stellen Sie sicher, dass das TPM unterstützt wird. Führen Sie alternativ das folgende PowerCLI-Cmdlet zur Änderung von com.vmware.esx.attestation.tpm2.settings aus, um `requireCertificateValidation` auf `false` festzulegen. `Set-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster TrustedCluster -RequireCertificateValidation:$false -RequireEndorsementKey:$true`
Der Nachweis ist aufgrund eines unbekannten TPM fehlgeschlagen.	Importieren Sie den TPM Endorsement Key in die Nachweisdienste. Weitere Informationen hierzu finden Sie unter Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
Fehler: vapi.send.failed.	Der kmxa-Dienst wird möglicherweise auf dem vertrauenswürdigen Host nicht ausgeführt oder der kmxa-Dienst kann den Nachweisdienst nicht kontaktieren. Stellen Sie sicher, dass der kmxa-Dienst gestartet wurde. Stellen Sie außerdem sicher, dass der Nachweisdienst ausgeführt wird. Weitere Informationen hierzu finden Sie unter Neustarten des Diensts für vertrauenswürdige Hosts.

Prüfen und Standardisieren der Integrität eines vertrauenswürdigen Clusters

Sie können die Integrität eines vertrauenswürdigen Clusters überprüfen und validieren. Wenn die Konfiguration eines vertrauenswürdigen Clusters nicht fehlerfrei ist, müssen Sie die Konfigurationsinkonsistenzen beheben. Hierzu standardisieren Sie den vertrauenswürdigen Cluster. Wenn Sie einen vertrauenswürdigen Cluster standardisieren, stellen Sie sicher, dass alle vertrauenswürdigen Hosts im vertrauenswürdigen Cluster dieselbe vertrauenswürdige Konfiguration aufweisen.

Ein vertrauenswürdiger Cluster besteht aus einem vCenter Server-Cluster mit vertrauenswürdigen ESXi-Hosts, die remote vom Trust Authority-Cluster bestätigt wurden. Wenn Sie vSphere Trust Authority erstmals konfigurieren, müssen Sie die Informationen zu Trust Authority Services aus dem Trust Authority-Cluster in den vertrauenswürdigen Cluster importieren. Der vertrauenswürdige Cluster verwendet diese Konfiguration von Komponenten für die Kontaktaufnahme mit dem Schlüsselanbieterdienst und dem auf dem Trust Authority-Cluster ausgeführten Nachweisdienst. Weitere Informationen zu diesem Aspekt der Konfiguration eines vertrauenswürdigen Clusters finden Sie unter Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts. Nachdem Sie einen vertrauenswürdigen Cluster konfiguriert haben, können Sie seine Integrität überprüfen und ihn standardisieren.

Überprüfen der Integrität des vertrauenswürdigen Clusters

Die Überprüfung der Integrität eines vertrauenswürdigen Clusters hängt von den folgenden Umständen ab.

Gewünschte Zustandskonfiguration

Die gewünschte Zustandskonfiguration basiert auf den Informationen der Trust Authority Services, die Sie in den vertrauenswürdigen Cluster importieren. Die gewünschte Zustandskonfiguration ist die „Wahrheitsquelle“ des vertrauenswürdigen Clusters. Betrachten Sie die gewünschte Zustandskonfiguration als die Konfiguration, die bei der ersten Einrichtung des vertrauenswürdigen Clusters erstellt wurde.

Angewendete Konfiguration

Bei der angewendeten Konfiguration handelt es sich um die Registrierung der spezifischen Nachweisdienste und Schlüsselanbieterdienste, für die Sie den vertrauenswürdigen Cluster konfiguriert haben. Die angewendete Konfiguration ist das, was der vertrauenswürdige Cluster momentan ausführt. Betrachten Sie die angewendete Konfiguration als „Laufzeitkonfiguration“. Die gewünschte Zustandskonfiguration sollte mit der angewendeten Konfiguration übereinstimmen. Wenn die angewendete Konfiguration jedoch nicht mit der gewünschten Zustandskonfiguration übereinstimmt, wird der vertrauenswürdige Cluster als „nicht fehlerfrei“ eingestuft. Ein vertrauenswürdiger Cluster, der nicht fehlerfrei ist, kann eine verminderte Leistung aufweisen oder gar nicht funktionieren.

Diese Integritätsprüfung ist kein Indikator für den allgemeinen Systemzustand für einen vertrauenswürdigen Cluster oder die vSphere Trust Authority-Infrastruktur. Die Integritätsprüfung vergleicht nur die gewünschte Zustandskonfiguration des vertrauenswürdigen Clusters mit der angewendeten Konfiguration.

Standardisieren des vertrauenswürdigen Clusters

Die Standardisierung ist der Prozess, bei dem vSphere Trust Authority eine inkonsistente Konfiguration eines vertrauenswürdigen Clusters behebt. Die Konfiguration eines vertrauenswürdigen Clusters kann im Laufe der Zeit oder aufgrund anderer Betriebsfehler inkonsistent werden.

Verwenden Sie die Standardisierung wie folgt:

- Überprüfen Sie die Integrität des vertrauenswürdigen Clusters.
- Wenn der vertrauenswürdige Cluster nicht fehlerfrei ist, standardisieren Sie ihn.

Sie können entweder den vSphere Client oder die CLI verwenden, um die Integrität des vertrauenswürdigen Clusters zu prüfen. Siehe Überprüfen der Integrität des vertrauenswürdigen Clusters. Sie können den vSphere Client oder die CLI auch verwenden, um einen vertrauenswürdigen Cluster zu standardisieren. Weitere Informationen hierzu finden Sie unter Standardisieren eines vertrauenswürdigen Clusters.

Hinweis Die Standardisierung eignet sich auch zum Hinzufügen eines Hosts zu einem vorhandenen vertrauenswürdigen Cluster. Siehe Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mit dem vSphere Client und Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mithilfe der Befehlszeile.

Überprüfen der Integrität des vertrauenswürdigen Clusters

Sie können den Integritätsstatus eines vertrauenswürdigen Clusters überprüfen, indem Sie entweder den vSphere Client oder die Befehlszeile verwenden.

Voraussetzungen

- Auf dem vCenter Server für den vertrauenswürdigen Cluster muss vSphere 7.0 Update 1 oder höher ausgeführt werden.
- Bei Verwendung von PowerCLI wird Version 12.1.0 oder höher benötigt.

Verfahren

1 Überprüfen Sie die Integrität des vertrauenswürdigen Clusters.

Tool	Schritte
vSphere Client	a Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her. b Melden Sie sich als Trust Authority-Administrator an. c Navigieren Sie zu einem vertrauenswürdigen Cluster, wählen Sie **Konfigurieren** und anschließend **Trust Authority** aus. d Klicken Sie auf **Integrität überprüfen**.

Befehlszeilenschnittstelle	a In einer PowerCLI-Sitzung führen Sie das Cmdlet `Connect-VIServer` aus, um als Trust Authority-Administrator eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters herzustellen.
	`Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`
	b Führen Sie das Cmdlet `Get-TrustedClusterAppliedStatus` aus. Beispiel:
	`Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'`

2 Wenn Fehler auftreten, finden Sie weitere Informationen unter Standardisieren eines vertrauenswürdigen Clusters.

Standardisieren eines vertrauenswürdigen Clusters

Sie können die Konfiguration eines vertrauenswürdigen Clusters mithilfe des vSphere Client oder der Befehlszeile standardisieren.

Voraussetzungen

Auf dem vCenter Server für den vertrauenswürdigen Cluster muss vSphere 7.0 Update 1 oder höher ausgeführt werden.

Verfahren

1 Stellen Sie eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters her.

Tool	Schritte
vSphere Client	a Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her. b Melden Sie sich als Trust Authority-Administrator an.
Befehlszeilenschnittstelle	In einer PowerCLI-Sitzung führen Sie das Cmdlet `Connect-VIServer` aus, um als Trust Authority-Administrator eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters herzustellen. `Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`

2 Standardisieren Sie den vertrauenswürdigen Cluster und überprüfen Sie dann die Integrität des vertrauenswürdigen Clusters erneut.

Tool	Schritte
vSphere Client	a Navigieren Sie zu einem vertrauenswürdigen Cluster. b Wählen Sie **Konfigurieren** und wählen Sie dann **Trust Authority**. c Klicken Sie auf **Standardisieren**. d Klicken Sie auf **Integrität überprüfen**.

Befehlszeilenschnittstelle	a Führen Sie das `Set-TrustedCluster`-Cmdlet mit dem Parameter `-Remediate` aus, wie z. B.:
	`Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate`
	b Führen Sie das Cmdlet `Get-TrustedClusterAppliedStatus` aus. Beispiel:
	`Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'`

Verwenden der Verschlüsselung in Ihrer vSphere-Umgebung

10

Die Verwendung von Verschlüsselung in Ihrer vSphere-Umgebung muss vorbereitet werden. Dabei spielt es keine Rolle, ob Sie einen Standardschlüsselanbieter, einen vertrauenswürdigen Schlüsselanbieter oder einen vSphere Native Key Provider verwenden.

Weitere Informationen zum Einrichten Ihrer Umgebung für die Verwendung eines Schlüsselanbieters finden Sie unter:

- Kapitel 7 Konfigurieren und Verwalten eines Standardschlüsselanbieters
- Kapitel 8 Konfigurieren und Verwalten eines vSphere Native Key Providers
- Konfigurieren von vSphere Trust Authority

Wenn Sie Ihre Umgebung eingerichtet haben, können Sie mithilfe des vSphere Client verschlüsselte virtuelle Maschinen und virtuelle Festplatten erstellen und vorhandene virtuelle Maschinen und Festplatten verschlüsseln.

Unter Verwendung der API und der `crypto-util`-Befehlszeile können Sie zusätzliche Aufgaben ausführen. Die API-Dokumentation finden Sie im *Programmierhandbuch zum vSphere Web Services SDK*. Informationen zu diesem Tool finden Sie der `crypto-util`-Befehlszeilenhilfe.

Lesen Sie als Nächstes die folgenden Themen:

- Erstellen einer Speicherrichtlinie für die Verschlüsselung.
- Explizites Aktivieren des Hostverschlüsselungsmodus
- Deaktivieren des Hostverschlüsselungsmodus mithilfe der API
- Erstellen einer verschlüsselten virtuellen Maschine
- Klonen einer verschlüsselten virtuellen Maschine
- Verschlüsseln einer bestehenden virtuellen Maschine oder virtuellen Festplatte
- Entschlüsseln einer verschlüsselten virtuellen Maschine oder virtuellen Festplatte
- Ändern der Verschlüsselungsrichtlinie für virtuelle Festplatten
- Beheben von Problemen in Bezug auf fehlende Verschlüsselungsschlüssel
- Entsperren von gesperrten virtuellen Maschinen
- Beheben von Problemen im Zusammenhang mit dem Verschlüsselungsmodus des ESXi-Hosts

- Erneutes Aktivieren des ESXi-Hostverschlüsselungsmodus
- Festlegen des Schwellenwerts für den Ablauf von Schlüsselserverzertifikaten
- vSphere VM-Verschlüsselung und Core-Dumps
- Aktivieren und Deaktivieren von Schlüsselpersistenz auf einem ESXi-Host
- Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe des vSphere Client
- Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe der CLI
- Festlegen des Standardschlüsselanbieters mithilfe des vSphere Client
- Festlegen des Standardschlüsselanbieters über die Befehlszeile

Erstellen einer Speicherrichtlinie für die Verschlüsselung.

Bevor Sie verschlüsselte virtuelle Maschinen erstellen können, müssen Sie eine Speicherrichtlinie für die Verschlüsselung erstellen. Die Speicherrichtlinie wird nur einmal erstellt und immer dann zugewiesen, wenn eine virtuelle Maschine oder eine virtuelle Festplatte verschlüsselt wird.

Wenn Sie VM-Verschlüsselung mit anderen I/O-Filtern oder den Assistenten **VM-Speicherrichtlinie erstellen** im vSphere Client verwenden möchten, finden Sie weitere Informationen in der Dokumentation *vSphere-Speicher*.

Voraussetzungen

- Richten Sie die Verbindung zu einem Schlüsselanbieter ein.

  Obwohl eine Speicherrichtlinie für die VM-Verschlüsselung auch ohne Verbindung zum Schlüsselanbieter erstellt werden kann, können Sie Verschlüsselungsaufgaben erst durchführen, nachdem die vertrauenswürdige Verbindung mit dem Schlüsselanbieter eingerichtet wurde.
- Erforderliche Rechte: **Verschlüsselungsvorgänge.Verschlüsselungsrichtlinien verwalten**.

Verfahren

1. Melden Sie sich beim vCenter Server mit dem vSphere Client an.
2. Wählen Sie **Home** aus, klicken Sie auf **Richtlinien und Profile** und klicken Sie dann auf **VM-Speicherrichtlinien**.
3. Klicken Sie auf **Erstellen**.
4. Wählen Sie den vCenter Server aus, geben Sie einen Richtliniennamen sowie optional eine Beschreibung ein und klicken Sie dann auf **Weiter**.
5. Aktivieren Sie auf der Seite **Richtlinienstruktur** die Option **Hostbasierte Rollen aktivieren** und klicken Sie dann auf **Weiter**.

6 Wählen Sie auf der Seite **Hostbasierte Dienste** die Option **Speicherrichtlinienkomponente verwenden** aus, wählen Sie im Dropdown-Menü **Standardeigenschaften der Verschlüsselung** aus und klicken Sie dann auf **Weiter**.

7 Behalten Sie auf der Seite **Speicherkompatibilität** die Option **Kompatibel** bei, wählen Sie einen Datenspeicher und klicken Sie dann auf **Weiter**.

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

Ergebnisse

Die VM-Verschlüsselungsspeicherrichtlinie wird zur Liste hinzugefügt und steht für die Verschlüsselung einer virtuellen Maschine bereit.

Explizites Aktivieren des Hostverschlüsselungsmodus

Der Hostverschlüsselungsmodus muss aktiviert sein, wenn Sie Verschlüsselungsaufgaben wie das Erstellen einer verschlüsselten virtuellen Maschine auf einem ESXi-Host durchführen möchten. In den meisten Fällen wird der Hostverschlüsselungsmodus automatisch aktiviert, wenn Sie eine Verschlüsselungsaufgabe durchführen.

In bestimmten Fällen muss der Verschlüsselungsmodus explizit eingeschaltet werden. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für VM-Verschlüsselungsaufgaben.

Voraussetzungen

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

Verfahren

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

2 Navigieren Sie zum ESXi-Host und klicken Sie auf **Konfigurieren**.

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

4 Klicken Sie im Fenster „Hostverschlüsselungsmodus“ auf **Bearbeiten**.

5 Wählen Sie **Aktiviert** aus und klicken Sie auf **OK**.

Deaktivieren des Hostverschlüsselungsmodus mithilfe der API

Der Hostverschlüsselungsmodus wird automatisch aktiviert, wenn ein Benutzer eine Verschlüsselungsaufgabe durchführt, wenn der Benutzer über ausreichende Berechtigungen verfügt. Nachdem der Hostverschlüsselungsmodus aktiviert wurde, werden alle Core-Dumps verschlüsselt, um die Freigabe von vertraulichen Informationen an Supportmitarbeiter zu vermeiden. Falls Sie die Verschlüsselung virtueller Maschinen bei einem ESXi-Host nicht mehr verwenden, können Sie den Verschlüsselungsmodus deaktivieren.

Nach der Aktivierung des Verschlüsselungsmodus für einen ESXi-Host müssen Sie ihn möglicherweise deaktivieren. Beispielsweise müssen Sie möglicherweise den Verschlüsselungsmodus deaktivieren, um ein ESXi-Support-Paket zu generieren (mithilfe des Befehls `vm-support`). Die Umschaltoption „Hostverschlüsselungsmodus“ (**Host > Konfigurieren > Sicherheitsprofil > Hostverschlüsselungsmodus bearbeiten**) funktioniert nicht, wenn Schlüsselmaterial auf dem Host vorhanden ist.

Sie können die API verwenden, um den Hostverschlüsselungsmodus zu deaktivieren, indem Sie die API-Methode „`CryptoManagerHostDisable`“ aufrufen.

Die für einen ESXi-Host definierten Verschlüsselungsmodi bzw. -zustände lauten:

- pendingIncapable: Der Host ist für die Verschlüsselung aktiviert ist, das heißt, der Host kann keine vSphere VM-Verschlüsselungsvorgänge durchführen.
- incapable: Der Host ist für den Empfang vertraulicher Materialien nicht sicher.
- prepared: Der Host ist für den Empfang vertraulicher Materialien vorbereitet, verfügt aber noch nicht über einen festgelegten Hostschlüssel.
- safe: Der Host ist verschlüsselungssicher (aktiviert) und verfügt über einen Hostschlüsselsatz, das heißt, vSphere Virtual Machine Encryption-Vorgänge sind möglich.

Nachdem Sie „`CryptoManagerHostDisable`“ auf einem Host aufgerufen haben, ändert sich der Verschlüsselungsstatus des Hosts wie folgt:

- Wenn der ursprüngliche Host-Verschlüsselungsstatus nicht in der Lage (incapable) oder vorbereitet (prepared) ist, wird der Host-Verschlüsselungsstatus in „incapable“ geändert.
- Wenn der ursprüngliche Host-Verschlüsselungsstatus sicher (safe) ist, wird der Host-Verschlüsselungsstatus in „pendingIncapable“ geändert.
- Wenn der Host-Verschlüsselungsstatus „pendingIncapable“ lautet, ist der Host-Verschlüsselungsstatus weiterhin „pendingIncapable“.

Diese Aufgabe zeigt mithilfe des vCenter Server-MOB (Managed Object Browser) den Hostverschlüsselungsmodus deaktivieren. Weitere Informationen zur Verwendung der API finden Sie in der Dokumentation *vSphere Web Services API* unter https://developer.vmware.com/apis/968/vsphere.

Verfahren

1. Melden Sie sich beim vCenter Server als Administrator an.
2. Heben Sie die Registrierung aller verschlüsselten virtuellen Maschinen auf dem ESXi-Host auf, dessen Verschlüsselungsmodus Sie deaktivieren möchten.
3. Greifen Sie auf den MOB auf dem vCenter Server zu.

```
https://vcenter_server/mob
```

4 Rufen Sie die Methode „`CryptoManagerHostDisable`“ auf einem Host auf.

   a Klicken Sie unter „content name“ auf **content**.

   b Klicken Sie unter „rootFolder“ auf **group-D1 (Datacenters)**.

   c Klicken Sie unter „childEntity“ auf das entsprechende Datencenter.

   d Klicken Sie unter „hostFolder“ auf den entsprechenden Host.

   e Klicken Sie unter „childEntity“ auf den entsprechenden Cluster.

   f Klicken Sie unter „host“ auf den entsprechenden Host.

   g Klicken Sie unter „configManager“ auf **configManager**.

   h Klicken Sie unter „cryptoManager“ auf **CryptoManagerHost-***Zahl*.

   i Klicken Sie auf **CryptoManagerHostDisable**.

   Der Host-Verschlüsselungsstatus wird je nach ursprünglichem Verschlüsselungsstatus in „pendingIncapable“ oder „incapable“ geändert.

5 Wiederholen Sie Schritt 4 für andere Hosts, auf denen Sie den Verschlüsselungsmodus deaktivieren möchten.

6 Starten Sie die Hosts neu.

Ergebnisse

Sobald der Hostverschlüsselungsmodus deaktiviert ist, können Sie keine Verschlüsselungsvorgänge wie das Hinzufügen verschlüsselter virtueller Maschinen durchführen, es sei denn, Sie aktivieren den Hostverschlüsselungsmodus erneut.

Hinweis Nachdem Sie einen ESXi-Host neu gestartet haben, auf dem Sie den Verschlüsselungsmodus deaktiviert haben, ist der Hostverschlüsselungsstatus weiterhin „pendingIncapable“, wenn der Hostverschlüsselungsstatus ursprünglich „pendingIncapable“ lautete. Um den Hostverschlüsselungsmodus erneut zu aktivieren, greifen Sie erneut auf den vCenter Server-MOB zu und rufen Sie die API-Methode `ConfigureCryptoKey` auf. Verwenden Sie beim erneuten Aktivieren des Hostverschlüsselungsmodus die ursprüngliche Hostschlüssel-ID, wenn der Hostverschlüsselungsstatus „pendingIncapable“ lautet.

Erstellen einer verschlüsselten virtuellen Maschine

Sie können den vSphere Client verwenden, um verschlüsselte virtuelle Maschinen zu erstellen.

Der vSphere Client filtert nach Speicherrichtlinien für die VM-Verschlüsselung und vereinfacht somit die Erstellung verschlüsselter virtueller Maschinen.

Hinweis Das Erstellen einer verschlüsselten virtuellen Maschine geht schneller und beansprucht weniger Speicherressourcen als das Verschlüsseln einer vorhandenen virtuellen Maschine. Falls möglich, verschlüsseln Sie virtuelle Maschinen während des Erstellungsvorgangs.

Voraussetzungen

- Konfigurieren Sie einen Schlüsselanbieter und legen Sie ihn als Standard fest.
- Erstellen Sie eine Speicherrichtlinie für die Verschlüsselung oder verwenden Sie das im Lieferumfang enthaltene Beispiel für eine VM-Verschlüsselungsrichtlinie.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- Stellen Sie sicher, dass Sie über die erforderlichen Rechte verfügen:
  - **Verschlüsselungsvorgänge.Neue verschlüsseln**
  - Wenn der Hostverschlüsselungsmodus nicht auf „Aktiviert“ festgelegt ist, benötigen Sie außerdem **Verschlüsselungsvorgänge.Host registrieren**.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.
3. Klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie **Neue virtuelle Maschine** aus.
4. Folgen Sie den Anweisungen, um eine verschlüsselte virtuelle Maschine zu erstellen.

Option	Aktion
Erstellungstyp auswählen	Erstellen Sie eine neue virtuelle Maschine.
Namen und Ordner auswählen	Geben Sie einen eindeutigen Namen und einen Zielspeicherort für die virtuelle Maschine an.
Computing-Ressource auswählen	Geben Sie ein Objekt an, für das Sie über Berechtigungen zum Erstellen von verschlüsselten virtuellen Maschinen verfügen. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für VM-Verschlüsselungsaufgaben.
Speicher auswählen	Aktivieren Sie das Kontrollkästchen **Diese virtuelle Maschine verschlüsseln**. VM-Speicherrichtlinien mit Verschlüsselung werden angezeigt. Wählen Sie eine VM-Speicherrichtlinie (das mitgelieferte Beispiel lautet „VM-Verschlüsselungsrichtlinie“) und einen kompatiblen Datenspeicher aus.
Kompatibilität auswählen	Wählen Sie die Kompatibilität aus. Sie können eine verschlüsselte virtuelle Maschine nur zu Hosts migrieren, die mit ESXi 6.5 oder höher kompatibel sind.
Gastbetriebssystem auswählen	Wählen Sie ein Gastbetriebssystem aus, das Sie später auf der virtuellen Maschine installieren möchten.

Option	Aktion
Hardware anpassen	Passen Sie die Hardware an, indem Sie z. B. die Festplattengröße oder die CPU ändern. (Optional) Wählen Sie die Registerkarte **VM-Optionen** aus und erweitern Sie **Verschlüsselung**. Wählen Sie die Festplatten aus, die nicht verschlüsselt werden sollen. Wenn Sie die Auswahl einer Festplatte aufheben, werden nur VM-Home und etwaige andere ausgewählte Festplatten verschlüsselt. Jede neue Festplatte, die Sie hinzufügen, wird verschlüsselt. Sie können die Speicherrichtlinie für einzelne Festplatten später ändern.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

Klonen einer verschlüsselten virtuellen Maschine

Eine geklonte, verschlüsselte virtuelle Maschine wird mit denselben Schlüsseln verschlüsselt, es sei denn, Sie ändern sie. Um Schlüssel zu ändern, können Sie vSphere Client, PowerCLI oder die API verwenden. Wenn Sie die PowerCLI oder die API verwenden, können Sie die verschlüsselte virtuelle Maschine klonen und die Schlüssel in einem Schritt ändern.

Während des Klonens können Sie die folgenden Vorgänge ausführen.

- Erstellen Sie eine verschlüsselte virtuelle Maschine anhand einer nicht verschlüsselten oder Vorlagen-VM.
- Erstellen Sie eine entschlüsselte virtuelle Maschine anhand einer verschlüsselten oder Vorlagen-VM.
- Verschlüsseln Sie die virtuelle Zielmaschine erneut mit Schlüsseln, die sich von denen der virtuellen Quellmaschine unterscheiden.
- In vSphere 8.0 und höher beginnt der Vorgang bei Auswahl der Option **Ersetzen** für eine virtuelle Maschine mit einem vTPM mit einem neuen, leeren vTPM, das seine eigenen geheimen Schlüssel und seine eigene Identität erhält.

Hinweis vSphere 8.0 und höher enthält die erweiterte Einstellung `vpxd.clone.tpmProvisionPolicy`, um das standardmäßige Klonverhalten für vTPMs als „ersetzen“ festzulegen.

Sie können eine Instant Clone-VM anhand einer verschlüsselten virtuellen Maschine unter der Voraussetzung erstellen, dass der Instant Clone denselben Schlüssel wie die virtuelle Quellmaschine verwendet. Sie können Schlüssel weder auf der Quell- noch auf der Instant Clone-VM erneut verschlüsseln.

Informationen zur Verwendung der API zum Klonen verschlüsselter Maschinen finden Sie unter *Programmierhandbuch zum vSphere Web Services SDK*.

Voraussetzungen

- Ein Schlüsselanbieter muss konfiguriert und aktiviert sein.

- Erstellen Sie eine Speicherrichtlinie für die Verschlüsselung oder verwenden Sie das im Lieferumfang enthaltene Beispiel für eine VM-Verschlüsselungsrichtlinie.
- Erforderliche Rechte (gilt für alle Schlüsselanbieter):
  - **Verschlüsselungsvorgänge.Klonen**
  - **Verschlüsselungsvorgänge.Verschlüsseln**
  - **Verschlüsselungsvorgänge.Entschlüsseln**
  - **Verschlüsselungsvorgänge.Erneut verschlüsseln**
  - Wenn der Hostverschlüsselungsmodus nicht auf „Aktiviert“ festgelegt ist, benötigen Sie außerdem **Verschlüsselungsvorgänge.Host registrieren**-Rechte.

Verfahren

1 Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.

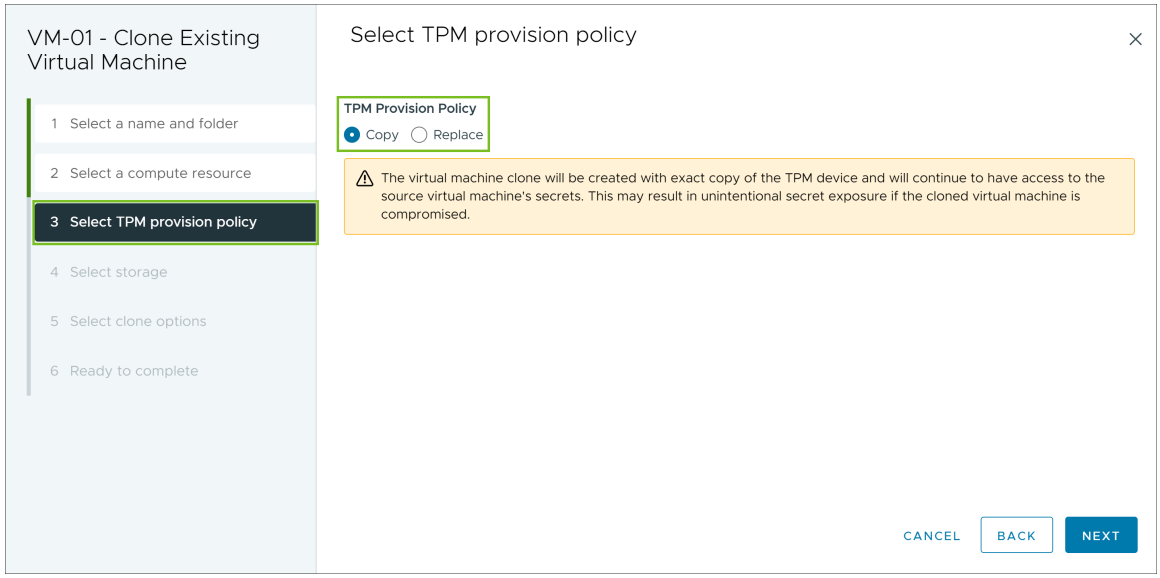
2 Um einen Klon einer verschlüsselten Maschine zu erstellen, klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, wählen Sie **Klonen > In virtueller Maschine klonen** und folgen Sie den Anweisungen.

   a Geben Sie auf der Seite **Namen und Ordner auswählen** einen Namen und den Zielspeicherort für den Klon an.

   b Geben Sie auf der Seite **Computing-Ressource auswählen** ein Objekt an, für das Sie über Rechte verfügen.

c (Optional) Ändern Sie die Schlüssel für die geklonte vTPM.

Abbildung 10-1. TPM-Bereitstellungsrichtlinie auswählen



Durch das Klonen einer virtuellen Maschine wird die gesamte virtuelle Maschine dupliziert, einschließlich des vTPM und der jeweiligen geheimen Schlüssel, die zur Ermittlung der Identität eines Systems verwendet werden können. Zum Ändern geheimer Schlüssel auf einem vTPM wählen Sie **Erstellen** für **TPM-Bereitstellungsrichtlinie** aus.

Hinweis Wenn Sie die geheimen Schlüssel eines vTPM ersetzen, werden alle Schlüssel, einschließlich arbeitslastbezogener Schlüssel, ersetzt. Stellen Sie als Best Practice sicher, dass Ihre Arbeitslasten kein vTPM mehr verwenden, bevor Sie die Schlüssel ersetzen. Andernfalls funktionieren die Arbeitslasten in der geklonten virtuellen Maschine möglicherweise nicht ordnungsgemäß.

d Konfigurieren Sie den Datenspeicher auf der Seite **Speicher auswählen**. Sie können die Speicherrichtlinie im Rahmen des Klonvorgangs ändern. Wenn Sie beispielsweise statt einer Verschlüsselungsrichtlinie eine Nicht-Verschlüsselungsrichtlinie verwenden, werden die Festplatten entschlüsselt.

e Wählen Sie auf der Seite **Klonoptionen auswählen** die Klonoptionen aus, wie in der Dokumentation zu *vSphere-Administratorhandbuch für virtuelle Maschinen* beschrieben.

f Überprüfen Sie auf der Seite **Bereit zum Abschließen** die dort angezeigten Informationen und klicken Sie auf **Beenden**.

3 (Optional) Ändern Sie die Schlüssel für die geklonte virtuelle Maschine.

Die geklonte virtuelle Maschine wird standardmäßig mit denselben Schlüsseln erstellt wie die übergeordnete virtuelle Maschine. Es wird empfohlen, die Schlüssel der geklonten virtuellen Maschine zu ändern, um sicherzustellen, dass mehrere virtuelle Maschinen nicht über dieselben Schlüssel verfügen.

a Entscheiden Sie sich für eine flache oder tiefe Neuverschlüsselung.

Wenn Sie einen anderen Daten-Verschlüsselungsschlüssel (Data Encryption Key, DEK) und einen anderen Schlüssel-Verschlüsselungsschlüssel (Key Encryption Key, KEK) verwenden möchten, führen Sie eine tiefe Neuverschlüsselung der geklonten virtuellen Maschine durch. Wenn Sie einen anderen KEK verwenden möchten, führen Sie eine flache Neuverschlüsselung der geklonten virtuellen Maschine durch. Bei einer tiefen Neuverschlüsselung müssen Sie die virtuelle Maschine ausschalten. Sie können eine flache Neuverschlüsselung bei eingeschalteter virtueller Maschine durchführen, sofern auf der virtuellen Maschine Snapshots vorhanden sind. Die flache Neuverschlüsselung einer verschlüsselten virtuellen Maschine mit Snapshots ist nur in einem einzelnen Snapshot-Zweig (Festplattenkette) zulässig. Mehrere Snapshot-Zweige werden nicht unterstützt. Wenn die flache Neuverschlüsselung fehlschlägt, bevor alle Verknüpfungen in der Kette mit dem neuen KEK aktualisiert werden, können Sie weiterhin auf die verschlüsselte virtuelle Maschine zugreifen, vorausgesetzt, Sie verfügen über die alten und neuen KEKs.

b Verschlüsseln Sie den Klon erneut über die API. Siehe *Programmierhandbuch zum vSphere Web Services SDK*.

Verschlüsseln einer bestehenden virtuellen Maschine oder virtuellen Festplatte

Sie können eine bestehende virtuelle Maschine oder virtuelle Festplatte verschlüsseln, in dem sie ihre Speicherrichtlinie ändern. Sie können virtuelle Festplatten nur für verschlüsselte virtuelle Maschinen verschlüsseln.

Voraussetzungen

- Konfigurieren Sie einen Schlüsselanbieter und legen Sie ihn als Standard fest.
- Erstellen Sie eine Speicherrichtlinie für die Verschlüsselung oder verwenden Sie das im Lieferumfang enthaltene Beispiel für eine VM-Verschlüsselungsrichtlinie.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- Stellen Sie sicher, dass Sie über die erforderlichen Rechte verfügen:
  - **Verschlüsselungsvorgänge.Neue verschlüsseln**
  - Wenn der Hostverschlüsselungsmodus nicht auf „Aktiviert“ festgelegt ist, benötigen Sie außerdem **Verschlüsselungsvorgänge.Host registrieren**.

Verfahren

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

2 Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine und wählen Sie **VM-Richtlinien > VM-Speicherrichtlinien bearbeiten**.

   Sie können die Speicherrichtlinie für die Dateien der virtuellen Maschine, dargestellt von VM-Home, und die Speicherrichtlinie für virtuelle Festplatten festlegen.

3 Wählen Sie die Speicherrichtlinie aus.

   - Um die virtuelle Maschine und deren Festplatten zu verschlüsseln, wählen Sie eine Speicherrichtlinie für die Verschlüsselung aus und klicken Sie auf **OK**.
   - Um die virtuelle Maschine, jedoch nicht deren virtuelle Festplatten zu verschlüsseln, aktivieren Sie **Pro Datenträger konfigurieren**, wählen Sie die Speicherrichtlinie für die Verschlüsselung für VM-Home und andere Speicherrichtlinien für die virtuellen Festplatten aus und klicken Sie auf **OK**.

   Die virtuelle Festplatte einer nicht verschlüsselten virtuellen Maschine kann nicht verschlüsselt werden. Wenn Sie jedoch den vSphere Client verwenden, um die VM-Home-Dateien zu verschlüsseln, können Sie die unverschlüsselte virtuelle Maschine mit der verschlüsselten Festplatte neu konfigurieren.

4 Auf Wunsch können Sie die virtuelle Maschine – oder die virtuelle Maschine und die Festplatten – über das Menü **Einstellungen bearbeiten** im vSphere Client verschlüsseln.

   a Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

   b Wählen Sie die Registerkarte **VM-Optionen** aus und öffnen Sie **Verschlüsselung**. Wählen Sie eine Verschlüsselungsrichtlinie aus. Wenn Sie alle Festplatten deaktivieren, wird nur VM-Home verschlüsselt.

   c Klicken Sie auf **OK**.

Entschlüsseln einer verschlüsselten virtuellen Maschine oder virtuellen Festplatte

Sie können eine virtuelle Maschine, deren Festplatten oder beides entschlüsseln, indem Sie die Speicherrichtlinie ändern.

In dieser Aufgabe wird beschrieben, wie Sie eine verschlüsselte virtuelle Maschine mit vSphere Client entschlüsseln.

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

In dieser Aufgabe wird erläutert, wie Sie anhand von Speicherrichtlinien entschlüsseln. Für virtuelle Festplatten können Sie für die Entschlüsselung auch das Menü **Einstellungen bearbeiten** verwenden.

Hinweis Im Bereich „Details der virtuellen Maschine“ zeigt eine vTPM-fähige virtuelle Maschine sowohl ein Sperrsymbol als auch die Meldung „Verschlüsselt mit *key_provider*“ an. Informationen zum Entfernen eines vTPM aus einer virtuellen Maschine finden Sie unter Entfernen eines virtuellen Trusted Platform Module von einer virtuellen Maschine.

Voraussetzungen

- Die virtuelle Maschine muss verschlüsselt sein.
- Die virtuelle Maschine muss ausgeschaltet sein oder sich im Wartungsmodus befinden.
- Erforderliche Berechtigungen: **Verschlüsselungsvorgänge.Entschlüsseln**

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine und wählen Sie **VM-Richtlinien > VM-Speicherrichtlinien bearbeiten**.

   Sie können die Speicherrichtlinie für die Dateien der virtuellen Maschine, dargestellt von VM-Home, und die Speicherrichtlinie für virtuelle Festplatten festlegen.
3. Wählen Sie eine Speicherrichtlinie aus.
   - Um die virtuelle Maschine und deren Festplatten zu entschlüsseln, deaktivieren Sie **Pro Datenträger konfigurieren**, wählen Sie im Dropdown-Menü eine Speicherrichtlinie aus und klicken Sie auf **OK**.
   - Um die virtuelle Festplatte, jedoch nicht die virtuelle Maschine zu entschlüsseln, aktivieren Sie **Pro Datenträger konfigurieren**, wählen Sie die Speicherrichtlinie für die Verschlüsselung für VM-Home und andere Speicherrichtlinien für die virtuellen Festplatten aus und klicken Sie auf **OK**.

   Es ist nicht möglich, die virtuelle Maschine zu entschlüsseln und die Festplatte verschlüsselt zu lassen.
4. Auf Wunsch können Sie die virtuelle Maschine und die Festplatten mit vSphere Client über das Menü **Einstellungen bearbeiten** entschlüsseln.
   a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
   b. Wählen Sie die Registerkarte **VM-Optionen** aus und erweitern Sie **Verschlüsselung**.
   c. Um die virtuelle Maschine und deren Festplatten zu entschlüsseln, wählen Sie im Dropdown-Menü **VM verschlüsseln** die Option **Keine** aus.

d Um eine virtuelle Festplatte, jedoch nicht die virtuelle Maschine zu entschlüsseln, heben Sie die Auswahl der Festplatte auf.

e Klicken Sie auf **OK**.

5 (Optional) Sie können die Einstellung für verschlüsseltes vMotion ändern.

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

b Klicken Sie auf **VM-Optionen** und öffnen Sie **Verschlüsselung**.

c Legen Sie den Wert für **Verschlüsseltes vMotion** fest.

Ändern der Verschlüsselungsrichtlinie für virtuelle Festplatten

Beim Erstellen einer verschlüsselten virtuellen Maschine über den vSphere Client können Sie festlegen, welche virtuellen Festplatten, die Sie während der Erstellung der virtuellen Maschine hinzufügen, verschlüsselt werden. Sie können verschlüsselte virtuelle Festplatten mithilfe der Option **VM-Speicherrichtlinie bearbeiten** entschlüsseln.

Hinweis Eine verschlüsselte virtuelle Maschine kann nicht verschlüsselte virtuelle Festplatten enthalten. Eine nicht verschlüsselte virtuelle Maschine kann jedoch keine verschlüsselten virtuellen Festplatten enthalten.

Weitere Informationen hierzu finden Sie unter Verschlüsseln von virtuellen Festplatten.

In dieser Aufgabe wird beschrieben, wie Sie die Verschlüsselungsrichtlinie anhand von Speicherrichtlinien ändern. Sie können auch das Menü **Einstellungen bearbeiten** verwenden, um diese Änderung vorzunehmen.

Voraussetzungen

- Sie benötigen die Berechtigung **Verschlüsselungsvorgänge.Verschlüsselungsrichtlinien verwalten**.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

Verfahren

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

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **VM-Richtlinien > VM-Speicherrichtlinien bearbeiten** aus.

3 Ändern Sie die Speicherrichtlinie.

- Um die Speicherrichtlinie für die virtuelle Maschine und deren Festplatten zu ändern, wählen Sie eine Speicherrichtlinie für die Verschlüsselung aus und klicken Sie auf **OK**.

- Um die virtuelle Maschine, jedoch nicht deren virtuelle Festplatten zu verschlüsseln, aktivieren Sie **Pro Datenträger konfigurieren**, wählen Sie die Speicherrichtlinie für die Verschlüsselung für VM-Home und andere Speicherrichtlinien für die virtuellen Festplatten aus und klicken Sie auf **OK**.

Die virtuelle Festplatte einer nicht verschlüsselten virtuellen Maschine kann nicht verschlüsselt werden.

4 Auf Wunsch können Sie die Speicherrichtlinie im Menü **Einstellungen bearbeiten** ändern.

a Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

b Wählen Sie die Registerkarte **Virtuelle Hardware** aus, erweitern Sie eine Festplatte und wählen Sie im Dropdown-Menü eine Verschlüsselungsrichtlinie aus.

c Klicken Sie auf **OK**.

Beheben von Problemen in Bezug auf fehlende Verschlüsselungsschlüssel

Wenn der ESXi-Host den Schlüssel (KEK) für eine verschlüsselte virtuelle Maschine oder eine verschlüsselte virtuelle Festplatte nicht vom vCenter Server abrufen kann, wird die verschlüsselte virtuelle Maschine gesperrt. Nachdem Sie die Schlüssel auf dem Schlüsselserverr (KMS) verfügbar gemacht haben, können Sie eine gesperrte verschlüsselte virtuelle Maschine entsperren.

Unter bestimmten Umständen kann bei Verwendung eines Standardschlüsselanbieters der ESXi-Host den Schlüsselverschlüsselungsschlüssel (Key Encryption Key, KEK) für eine verschlüsselte virtuelle Maschine oder eine verschlüsselte virtuelle Festplatte nicht vom vCenter Server abrufen. In diesem Fall können Sie dennoch die Registrierung der virtuellen Maschine aufheben oder diese neu laden. Sie können jedoch keine anderen VM-Vorgänge durchführen, wie z. B. Einschalten der virtuellen Maschine. Nachdem Sie die nötigen Schritte ausgeführt haben, um die erforderlichen Schlüssel auf dem Schlüsselserver verfügbar zu machen, können Sie eine gesperrte verschlüsselte virtuelle Maschine mithilfe des vSphere Client entsperren.

Wenn der Schlüssel der virtuellen Maschine nicht verfügbar ist, werden Sie durch einen vCenter Server-Alarm benachrichtigt, und der Status der virtuellen Maschine wird als ungültig angezeigt. Die virtuelle Maschine kann nicht eingeschaltet werden. Wenn der Schlüssel der virtuellen Maschine verfügbar ist, aber kein Schlüssel für eine verschlüsselte Festplatte verfügbar ist, wird der Status für die virtuelle Maschine nicht als ungültig angezeigt. Die virtuelle Maschine kann jedoch nicht eingeschaltet werden, und es kommt zu folgendem Fehler:

```
The disk [/path/to/the/disk.vmdk] is encrypted and a required key was not found.
```

Hinweis In folgendem Verfahren werden die Situationen geschildert, die zur Sperrung einer virtuellen Maschine führen können, sowie neben den zugehörigen Alarmen und Ereignisprotokollen die Vorgehensweisen im jeweiligen Fall.

Verfahren

1 Falls die Verbindung zwischen dem vCenter Server-System und dem Schlüsselserver das Problem ist, generiert der vCenter Server einen VM-Alarm. Außerdem wird eine Fehlermeldung im Ereignisprotokoll angezeigt.

   Stellen Sie die Verbindung zum Schlüsselserver wieder her. Wenn der Schlüsselserver und die Schlüssel zur Verfügung stehen, entsperren Sie die gesperrten virtuellen Maschinen. Weitere Informationen hierzu finden Sie unter Entsperren von gesperrten virtuellen Maschinen. Sie können den Host auch neu starten und die virtuelle Maschine erneut registrieren, um sie nach der Wiederherstellung der Verbindung zu entsperren.

   Bei einer Unterbrechung der Verbindung zum Schlüsselserver wird die virtuelle Maschine nicht automatisch gesperrt. Die virtuelle Maschine wechselt nur dann in einen gesperrten Zustand, wenn die folgenden Bedingungen erfüllt sind:

   - Der Schlüssel ist nicht auf dem ESXi-Host verfügbar.
   - vCenter Server kann keine Schlüssel vom Schlüsselserver abrufen.

   Nach jedem Neustart von ESXi ist es wünschenswert, wenn auch nicht erforderlich, dass vCenter Server zuerst gestartet wird. vCenter Server fordert den Schlüssel mit der entsprechenden ID vom Schlüsselserver an und stellt ihn auf ESXi zur Verfügung.

   Hinweis In vSphere 7.0 Update 2 und höher können Sie Verschlüsselungsschlüssel auch bei mehreren ESXi-Neustarts beibehalten. Weitere Informationen finden Sie unter vSphere-Schlüsselpersistenz auf ESXi-Hosts.

   Wenn die virtuelle Maschine nach dem Wiederherstellen der Verbindung zum Schlüsselanbieter weiterhin gesperrt ist, erhalten Sie weitere Informationen unter Entsperren von gesperrten virtuellen Maschinen.

2 Wenn die Verbindung wiederhergestellt wurde, registrieren Sie die virtuelle Maschine. Falls ein Fehler auftritt oder der Vorgang erfolgreich verläuft, die virtuelle Maschine jedoch gesperrt ist, stellen Sie sicher, dass Sie über das Recht **Cryptographic operations.RegisterVM** für das vCenter Server-System verfügen.

   Diese Berechtigung ist für das Einschalten einer verschlüsselten virtuellen Maschine nicht erforderlich, wenn der Schlüssel verfügbar ist. Diese Berechtigung ist für die Registrierung der virtuellen Maschine erforderlich, wenn der Schlüssel abgerufen werden muss.

3 Wenn der Schlüssel auf dem Schlüsselserver nicht mehr verfügbar ist, generiert der vCenter Server einen VM-Alarm. Außerdem wird eine Fehlermeldung im Ereignisprotokoll angezeigt.

   Bitten Sie den Schlüsselserver-Administrator, den Schlüssel wiederherzustellen. Sie können auf einen inaktiven Schlüssel stoßen, wenn Sie eine virtuelle Maschine einschalten, die aus der Bestandsliste entfernt und seit einiger Zeit nicht registriert wurde. Es passiert auch, wenn Sie den ESXi-Host neu starten, wenn der Schlüsselserver nicht verfügbar ist.

   a Rufen Sie die Schlüssel-ID mithilfe des Managed Object Browsers (MOB) oder der vSphere API ab.

     Rufen Sie die `keyId` von der Datei `VirtualMachine.config.keyId.keyId` ab.

   b Bitten Sie den Schlüsselserver-Administrator, den Schlüssel zu reaktivieren, der dieser Schlüssel-ID entspricht.

   c Nach der Wiederherstellung des Schlüssels erhalten Sie weitere Informationen unter Entsperren von gesperrten virtuellen Maschinen.

   Wenn der Schlüssel auf dem Schlüsselserver wiederhergestellt werden kann, ruft vCenter Server ihn ab und leitet ihn an den ESXi-Host weiter, wenn er das nächste Mal benötigt wird.

4 Wenn auf den Schlüsselserver zugegriffen werden kann und der ESXi-Host eingeschaltet ist, das vCenter Server-System jedoch nicht zur Verfügung steht, führen Sie die folgenden Schritte durch, um die virtuellen Maschinen zu entsperren.

   a Stellen Sie das vCenter Server-System wieder her oder richten Sie ein anderes vCenter Server-System ein. Legen Sie anschließend ein Vertrauensverhältnis mit dem Schlüsselserver fest.

     Sie müssen den gleichen Schlüsselanbieternamen verwenden, die IP-Adresse des Schlüsselserver kann sich aber unterscheiden.

   b Registrieren Sie alle gesperrten virtuellen Maschinen neu.

     Die neue vCenter Server-Instanz ruft die Schlüssel vom Schlüsselserver ab, und die virtuellen Maschinen werden entsperrt.

5 Wenn die Schlüssel nur auf dem ESXi-Host fehlen, generiert der vCenter Server einen VM-Alarm, und im Ereignisprotokoll wird die folgende Meldung angezeigt:

   `Die virtuelle Maschine ist gesperrt, weil Schlüssel auf dem Host fehlen.`

   Das vCenter Server-System kann die fehlenden Schlüssel aus dem Schlüsselanbieter abrufen. Ein manuelle Wiederherstellung der Schlüssel ist nicht erforderlich. Weitere Informationen hierzu finden Sie unter Entsperren von gesperrten virtuellen Maschinen.

Entsperren von gesperrten virtuellen Maschinen

Sie werden in einem vCenter Server-Alarm informiert, wenn sich eine verschlüsselte virtuelle Maschine im gesperrten Modus befindet. Sie können eine gesperrte verschlüsselte VM mithilfe des vSphere Client entsperren, nachdem Sie die notwendigen Schritte zur Bereitstellung der erforderlichen Schlüssel auf dem Schlüsselserver durchgeführt haben.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über die erforderlichen Berechtigungen verfügen: **Kryptografievorgänge.RegisterVM**
- Andere Berechtigungen sind unter Umständen für optionale Aufgaben erforderlich, wie z. B. das Aktivieren von Hostverschlüsselung.
- Ermitteln Sie vor dem Entsperren einer gesperrten virtuellen Maschine die Fehlerursache und versuchen Sie, das Problem manuell zu beheben. Weitere Informationen hierzu finden Sie unter Beheben von Problemen in Bezug auf fehlende Verschlüsselungsschlüssel.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Navigieren Sie zur Registerkarte **Übersicht** der virtuellen Maschine.

   Wenn eine virtuelle Maschine gesperrt ist, wird der Alarm „Virtuelle Maschine gesperrt“ angezeigt.
3. Sie können den Alarm bestätigen oder auf „Grün“ zurücksetzen, die virtuelle Maschine zu diesem Zeitpunkt jedoch nicht entsperren.

   Wenn Sie auf **Bestätigen** oder **Auf Grün zurücksetzen** klicken, wird der Alarm ausgeblendet. Die virtuelle Maschine bleibt jedoch solange gesperrt, bis Sie sie entsperren.
4. Navigieren Sie zur Registerkarte **Überwachen** der virtuellen Maschine und klicken Sie auf **Ereignisse**.

   Im Bereich **Ereignisse** werden Informationen darüber angezeigt, warum die virtuelle Maschine gesperrt ist.
5. Führen Sie die vorgeschlagene Fehlerbehebung durch, bevor Sie die virtuelle Maschine entsperren.
6. Navigieren Sie zur Registerkarte **Übersicht** der virtuellen Maschine.

   Ein Alarm wegen einer gesperrten virtuellen Maschine wird angezeigt.
7. Wählen Sie **VM entsperren** aus dem Dropdown-Menü **Aktionen** auf der rechten Seite aus.

Beheben von Problemen im Zusammenhang mit dem Verschlüsselungsmodus des ESXi-Hosts

Unter bestimmten Umständen kann der Verschlüsselungsmodus des ESXi-Hosts deaktiviert werden.

Für einen ESXi-Host muss der Hostverschlüsselungsmodus aktiviert sein, wenn er verschlüsselte virtuelle Maschinen enthält. Wenn der Host erkennt, dass der zugehörige Hostschlüssel fehlt, oder wenn der Schlüsselanbieter nicht verfügbar ist, kann der Host den Verschlüsselungsmodus unter Umständen nicht aktivieren. vCenter Server erzeugt einen Alarm, wenn der Hostverschlüsselungsmodus nicht aktiviert werden kann.

Verfahren

1. Wenn das Problem in der Verbindung zwischen dem vCenter Server-System und dem Schlüsselanbieter besteht, wird ein Alarm erzeugt und eine Fehlermeldung im Ereignisprotokoll angezeigt.

   Sie müssen die Verbindung mit dem Schlüsselanbieter wiederherstellen, der die betreffenden Verschlüsselungsschlüssel enthält.
2. Wenn Schlüssel fehlen, wird ein Alarm erzeugt und eine Fehlermeldung im Ereignisprotokoll angezeigt.

   Sie müssen sicherstellen, dass die Schlüssel im Schlüsselanbieter vorhanden sind. Informationen zum Wiederherstellen aus einer Sicherung finden Sie in der Dokumentation Ihres Schlüsselverwaltungsanbieters.

Nächste Schritte

Wenn der Verschlüsselungsmodus des Hosts nach der Wiederherstellung der Verbindung mit dem Schlüsselanbieter oder der manuellen Wiederherstellung der Schlüssel für den Schlüsselanbieter weiterhin deaktiviert ist, aktivieren Sie den Verschlüsselungsmodus des Hosts erneut. Weitere Informationen hierzu finden Sie unter Erneutes Aktivieren des ESXi-Hostverschlüsselungsmodus.

Erneutes Aktivieren des ESXi-Hostverschlüsselungsmodus

Bei vSphere 6.7 und höher informiert Sie ein vCenter Server-Alarm darüber, wenn der Verschlüsselungsmodus eines ESXi-Hosts deaktiviert wurde. Falls der Hostverschlüsselungsmodus deaktiviert wurde, können Sie ihn erneut aktivieren.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über die erforderlichen Berechtigungen verfügen: **Kryptografievorgänge.Host registrieren**
- Ermitteln Sie vor dem erneuten Aktivieren des Verschlüsselungsmodus die Fehlerursache und versuchen Sie, das Problem manuell zu beheben.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Navigieren Sie zur Registerkarte **Übersicht** für den ESXi-Host.

   Wenn der Verschlüsselungsmodus deaktiviert ist, wird ein Alarm mit dem Hinweis angezeigt, dass der Verschlüsselungsmodus für den Host aktiviert werden muss.
3. Sie können den Alarm bestätigen oder auf „Grün“ zurücksetzen, den Hostverschlüsselungsmodus zu diesem Zeitpunkt jedoch nicht erneut aktivieren.

   Wenn Sie auf **Bestätigen** oder **Auf Grün zurücksetzen** klicken, wird der Alarm ausgeblendet. Der Verschlüsselungsmodus für den Host bleibt deaktiviert, bis Sie ihn wieder aktivieren.

4 Navigieren Sie zur Registerkarte **Überwachen** für den ESXi-Host und klicken Sie auf **Ereignisse**.

   Es werden weitere Informationen darüber angezeigt, warum der Verschlüsselungsmodus deaktiviert ist. Führen Sie die vorgeschlagene Fehlerbehebung durch, bevor Sie den Verschlüsselungsmodus erneut aktivieren.

5 Klicken Sie auf der Registerkarte **Übersicht** auf **Hostverschlüsselungsmodus aktivieren**, um die Hostverschlüsselung erneut zu aktivieren.

   Eine Meldung mit der Warnung, dass Verschlüsselungsschlüsseldaten an den Host übermittelt werden, wird angezeigt.

6 Klicken Sie auf **Ja**.

Festlegen des Schwellenwerts für den Ablauf von Schlüsselserverzertifikaten

Standardmäßig benachrichtigt Sie vCenter Server 30 Tage vor dem Ablauf Ihrer Schlüsselserver-Zertifikate (KMS). Sie können diesen Standardwert ändern.

Schlüsselserverzertifikate haben ein Ablaufdatum. Wenn der Schwellenwert für das Ablaufdatum erreicht ist, werden Sie mittels eines Alarms benachrichtigt.

vCenter Server und Schlüsselserver tauschen zwei Arten von Zertifikaten aus: Server und Client. Im VMware Endpoint Certificate Store (VECS) auf dem vCenter Server-System werden die Serverzertifikate und ein Clientzertifikat pro Schlüsselanbieter gespeichert. Da es zwei Zertifikattypen gibt, gibt es zwei Alarme für die beiden Zertifikattypen (einen für Client- und einen für Serverzertifikate).

Verfahren

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

2 Wählen Sie in der Objekthierarchie das vCenter Server-System aus.

3 Klicken Sie auf **Konfigurieren**.

4 Klicken Sie unter **Einstellungen** auf **Erweiterte Einstellungen** und dann auf **Einstellungen bearbeiten**.

5 Klicken Sie auf das Symbol **Filter** und geben Sie `vpxd.kmscert.threshold` ein oder führen Sie einen Bildlauf zum Konfigurationsparameter durch.

6 Geben Sie den Wert in Tagen ein und klicken Sie auf **Speichern**.

vSphere VM-Verschlüsselung und Core-Dumps

Wenn in Ihrer Umgebung vSphere VM-Verschlüsselung verwendet wird und auf dem ESXi-Host ein Fehler auftritt, wird der dadurch entstandene Core-Dump verschlüsselt, um Kundendaten zu schützen. Auch die Core-Dumps im vm-support-Paket sind verschlüsselt.

Hinweis Core-Dumps können vertrauliche Informationen enthalten. Befolgen Sie beim Umgang mit Core-Dumps die Datensicherheits- und Datenschutzrichtlinien Ihrer Organisation.

Core-Dumps auf ESXi-Hosts

Wenn ein ESXi-Host, eine Benutzer-World oder eine virtuelle Maschine fehlschlägt, wird ein Core-Dump erstellt und der Host neu gestartet. Wenn für den ESXi-Host der Verschlüsselungsmodus aktiviert ist, wird der Core-Dump mit einem Schlüssel verschlüsselt, der sich im ESXi-Schlüssel-Cache befindet. (Abhängig vom verwendeten Schlüsselanbieter stammt der Schlüssel von einem externen Schlüsselserver, dem Schlüsselanbieterdienst oder vCenter Server). Weitere Hintergrundinformationen finden Sie unter Wie vSphere Virtual Machine Encryption Ihre Umgebung schützt.

Wenn ein ESXi-Host aus kryptografischer Sicht „sicher“ ist und ein Core-Dump erzeugt wird, löst dies ein Ereignis aus. Das Ereignis gibt an, dass ein Core-Dump zusammen mit folgenden Informationen durchgeführt wurde: Name der World, Zeitpunkt des Auftretens, keyID des zum Verschlüsseln des Core-Dumps verwendeten Schlüssel sowie der Dateiname des Core-Dumps. Sie können das Ereignis im Ereignis-Viewer unter **Aufgaben und Ereignisse** für den vCenter Server anzeigen.

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

Tabelle 10-1. Core-Dump-Verschlüsselungsschlüssel

Core-Dump-Typ	Verschlüsselungsschlüssel (ESXi 6.5)	Verschlüsselungsschlüssel (ESXi 6.7 und höher)
ESXi-Kernel	Hostschlüssel	Hostschlüssel
Benutzer-World (hostd)	Hostschlüssel	Hostschlüssel
Verschlüsselte virtuelle Maschine (VM)	Hostschlüssel	VM-Schlüssel

Die Vorgehensweise nach dem Neustart eines ESXi-Hosts hängt von mehreren Faktoren ab.

- In den meisten Fällen versucht der Schlüsselanbieter, den Schlüssel nach dem Neustart an den ESXi-Host zu übertragen. Wenn der Vorgang erfolgreich war, können Sie das vm-support-Paket generieren und den Core-Dump entschlüsseln bzw. neu verschlüsseln. Weitere Informationen hierzu finden Sie unter Entschlüsseln oder erneutes Verschlüsseln eines verschlüsselten Core-Dump.

- Wenn vCenter Server keine Verbindung zum ESXi-Host herstellen kann, können Sie den Schlüssel möglicherweise abrufen. Weitere Informationen hierzu finden Sie unter Beheben von Problemen in Bezug auf fehlende Verschlüsselungsschlüssel.
- Wenn der Host einen benutzerdefinierten Schlüssel verwendet hat und es sich bei diesem Schlüssel nicht um den Schlüssel handelt, den vCenter Server an den Host übermittelt, können Sie den Core-Dump nicht verändern. Vermeiden Sie die Verwendung von benutzerdefinierten Schlüsseln.

Core-Dumps und vm-support-Pakete

Wenn Sie sich an den technischen Support von VMware wenden, um einen schwerwiegenden Fehler zu melden, werden Sie in der Regel von dem Support-Mitarbeiter gebeten, ein vm-support-Paket zu generieren. Das Paket enthält Protokolldateien und weitere Informationen, einschließlich Core-Dumps. Wenn die Support-Mitarbeiter mithilfe der Protokolldateien und weiteren Informationen die Probleme nicht beheben können, werden Sie möglicherweise gebeten, die Core-Dumps zu entschlüsseln und relevante Informationen zur Verfügung zu stellen. Befolgen Sie zum Schutz vertraulicher Informationen wie z. B. Schlüssel die Sicherheits- und Datenschutzrichtlinie Ihres Unternehmens. Weitere Informationen hierzu finden Sie unter Erfassen eines vm-support-Pakets für einen ESXi-Host, auf dem Verschlüsselung verwendet wird.

Core-Dumps auf vCenter Server-Systemen

Ein Core-Dump auf einem vCenter Server-System ist nicht verschlüsselt. vCenter Server enthält bereits potenziell vertrauliche Informationen. Stellen Sie mindestens sicher, dass vCenter Server geschützt ist. Weitere Informationen hierzu finden Sie unter Kapitel 4 Sichern von vCenter Server-Systemen. Alternativ können Sie Core-Dumps für das vCenter Server-System deaktivieren. Weitere Informationen in den Protokolldateien können zum Ermitteln der Ursache des Problems dienlich sein.

Erfassen eines vm-support-Pakets für einen ESXi-Host, auf dem Verschlüsselung verwendet wird

Wenn der Hostverschlüsselungsmodus für den ESXi-Host aktiviert ist, werden alle Core-Dumps im `vm-support`-Paket verschlüsselt. Sie können das Paket vom vSphere Client erfassen und ein Kennwort angeben, falls Sie davon ausgehen, dass der Core-Dump zu einem späteren Zeitpunkt entschlüsselt werden muss.

Das `vm-support`-Paket enthält u. a. Protokolldateien und Core-Dump-Dateien.

Voraussetzungen

Informieren Sie den Supportmitarbeiter darüber, dass der Hostverschlüsselungsmodus für den ESXi-Host aktiviert ist. Der Supportmitarbeiter bittet Sie möglicherweise darum, Core-Dumps zu entschlüsseln und relevante Informationen zu extrahieren.

Hinweis Core-Dumps können vertrauliche Informationen enthalten. Beachten Sie die Sicherheits- und Datenschutzrichtlinie Ihres Unternehmens, um den Schutz vertraulicher Daten wie Hostschlüssel zu gewährleisten.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Klicken Sie auf **Hosts und Cluster** und klicken Sie dann mit der rechten Maustaste auf den ESXi-Host.
3. Wählen Sie **Systemprotokolle exportieren** aus.
4. Wählen Sie im Dialogfeld **Kennwort für verschlüsselte Core-Dumps** aus, geben Sie ein Kennwort an und bestätigen Sie es.
5. Behalten Sie die Standardeinstellungen für die anderen Optionen bei oder nehmen Sie Änderungen vor, wenn dies vom technischen Support von VMware gefordert wird, und klicken Sie dann auf **Protokolle exportieren**.

   Wenn Sie Ihren Browser nicht so konfiguriert haben, dass er vor dem Herunterladen fragt, wo die Dateien gespeichert werden sollen, wird der Download gestartet. Wenn Sie Ihren Browser so konfiguriert haben, dass er fragt, wo Dateien gespeichert werden sollen, geben Sie einen Speicherort für die Datei an.
6. Falls der Supportmitarbeiter Sie dazu aufgefordert hat, den Core-Dump im `vm-support`-Paket zu entschlüsseln, melden Sie sich bei einem ESXi-Host an und führen Sie die folgenden Schritte aus.
   a. Melden Sie sich beim ESXi-Host an und stellen Sie eine Verbindung zu dem Verzeichnis her, in dem sich das `vm-support`-Paket befindet.

      Der Dateiname richtet sich nach folgendem Muster: esx.date_and_time.tgz.
   b. Stellen Sie sicher, dass das Verzeichnis ausreichend Speicherplatz für das Paket, das dekomprimierte Paket und das erneut komprimierte Paket enthält, oder verschieben Sie das Paket.
   c. Extrahieren Sie das Paket in das lokale Verzeichnis.

      ```
      vm-support -x *.tgz .
      ```

      Die daraus resultierende Dateihierarchie enthält möglicherweise Core-Dump-Dateien für den ESXi-Host (üblicherweise im Verzeichnis `/var/core`) und mehrere Core-Dump-Dateien für virtuelle Maschinen.

d Entschlüsseln Sie jede verschlüsselte Core-Dump-Datei separat.

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

vm-support-incident-key-file ist die Schlüsseldatei des Vorfalls. Sie befindet sich auf der obersten Ebene im Verzeichnis.

encryptedZdump ist der Name der verschlüsselten Core-Dump-Datei.

decryptedZdump ist der von dem Befehl generierte Name der Datei. Legen Sie einen Namen fest, der *encryptedZdump* ähnelt.

e Geben Sie das Kennwort an, das Sie beim Erstellen des `vm-support`-Pakets angegeben haben.

f Entfernen Sie die verschlüsselten Core-Dumps und komprimieren Sie das Paket erneut.

```
vm-support --reconstruct
```

7 Entfernen Sie alle Dateien, die vertrauliche Informationen enthalten.

Entschlüsseln oder erneutes Verschlüsseln eines verschlüsselten Core-Dump

Ein verschlüsselter Core-Dump auf einem ESXi-Host kann mithilfe der CLI `crypto-util` entschlüsselt oder erneut verschlüsselt werden.

Sie können die Core-Dumps im vm-support-Paket selbst entschlüsseln und untersuchen. Core-Dumps können vertrauliche Informationen enthalten. Beachten Sie die Sicherheits- und Datenschutzrichtlinie Ihres Unternehmens, um den Schutz vertraulicher Daten wie Schlüssel zu gewährleisten.

Nähere Informationen zum erneuten Verschlüsseln eines Core-Dump und weiteren Funktionen von `crypto-util` finden Sie in der Befehlszeilenhilfe.

Hinweis `crypto-util` ist für fortgeschrittene Benutzer vorgesehen.

Voraussetzungen

Der zum Verschlüsseln des Core-Dumps verwendete Schlüssel muss auf dem ESXi-Host verfügbar sein, der den Core-Dump generiert hat.

Verfahren

1 Melden Sie sich direkt beim ESXi-Host an, auf dem der Core-Dump generiert wurde.

Falls sich der ESXi-Host im Sperrmodus befindet, oder wenn der SSH-Zugriff deaktiviert ist, müssen Sie möglicherweise zuerst den Zugriff aktivieren.

2 Ermitteln Sie, ob der Core-Dump verschlüsselt ist.

Option	Beschreibung
Core-Dump überwachen	`crypto-util envelope describe vmmcores.ve`
zdump-Datei	`crypto-util envelope describe --offset 4096 zdumpFile`

3 Entschlüsseln Sie den Core-Dump, je nach Typ.

Option	Beschreibung
Core-Dump überwachen	`crypto-util envelope extract vmmcores.ve vmmcores`
zdump-Datei	`crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted`

Aktivieren und Deaktivieren von Schlüsselpersistenz auf einem ESXi-Host

Sie müssen Schlüsselpersistenz auf einem ESXi-Host aktivieren. Schlüsselpersistenz ist standardmäßig nicht aktiviert.

Konzeptionelle Informationen zur Schlüsselpersistenz finden Sie unter vSphere-Schlüsselpersistenz auf ESXi-Hosts.

Voraussetzungen

Anforderungen zum Aktivieren von Schlüsselpersistenz:

- ESXi 7.0 Update 2 oder höher
- Mit TPM 2.0 installierter ESXi-Host
- Zugriff auf den ESXCLI-Befehlssatz. Sie können ESXCLI-Befehle remote oder in der ESXi Shell ausführen.

Hinweis Die Schlüsselpersistenz ist nicht erforderlich, wenn vSphere Native Key Provider verwendet wird. vSphere Native Key Provider ist sofort einsatzbereit und kann ohne Zugriff auf einen Schlüsselserver ausgeführt werden.

Für zusätzliche Sicherheit kann das TPM auch eine Versiegelungsrichtlinie verwenden, um Manipulationen beim Start des ESXi-Hosts zu verhindern. Weitere Informationen hierzu finden Sie unter Was sind TPM-Versiegelungsrichtlinien?.

Verfahren

1 Starten Sie eine Sitzung auf dem ESXi-Host mithilfe von SSH oder einer anderen Remotekonsolenverbindung.

2 Melden Sie sich als „root“ an.

3 Stellen Sie sicher, dass sich der ESXi-Host im TPM-Modus befindet.

```
esxcli system settings encryption get
```

Wenn als Modus KEINE angezeigt wird, müssen Sie das TPM in der Firmware des Hosts aktivieren und den Modus durch Ausführen des folgenden Befehls festlegen.

```
esxcli system settings encryption set --mode=TPM
```

4 Aktivieren oder deaktivieren Sie Schlüsselpersistenz.

a So aktivieren Sie Schlüsselpersistenz:

```
esxcli system security keypersistence enable
```

b So deaktivieren Sie Persistenz:

```
esxcli system security keypersistence disable --remove-all-stored-keys
```

Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe des vSphere Client

Sie können den vSphere Client verwenden, um eine flache erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine durchzuführen. Aus geschäftlichen oder Konformitätsgründen können Sie eine erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine durchführen.

Eine flache erneute Schlüsselerstellung (auch Neuverschlüsselung genannt) ersetzt nur den Schlüsselverschlüsselungsschlüssel (Key Encryption Key, KEK). Sie müssen die verschlüsselte virtuelle Maschine nicht ausschalten, um eine flache erneute Schlüsselerstellung durchzuführen. Wenn Sie sowohl den Festplattenverschlüsselungsschlüssel (DEK) als auch den KEK ersetzen müssen, müssen Sie eine tiefe erneute Schlüsselerstellung durchführen.

Hinweis Virtuelle Maschinen, die mit IDE-Controllern konfiguriert sind, müssen ausgeschaltet werden, um eine flache erneute Schlüsselerstellung durchzuführen.

Weitere konzeptuelle Informationen finden Sie unter Vorgehensweise zum Neuverschlüsseln (erneute Schlüsselerstellung) einer verschlüsselten virtuellen Maschine.

Voraussetzungen

Erforderliche Berechtigung:**Verschlüsselungsvorgänge.Erneut verschlüsseln**

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die verschlüsselte virtuelle Maschine aus.
3. Klicken Sie mit der rechten Maustaste auf die verschlüsselte virtuelle Maschine und wählen Sie **VM-Richtlinien** aus.
4. Wählen Sie **Erneut verschlüsseln** aus.
5. Klicken Sie auf **Ja**.

   Die verschlüsselte virtuelle Maschine wird mit dem neuen KEK neu verschlüsselt.

   Hinweis Wenn die erneute Schlüsselerstellung fehlschlägt, veröffentlicht das Ereignissubsystem das folgende Ereignis:

   ```
   com.vmware.vc.vm.crypto.RekeyFail
   ```

Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe der CLI

Sie können die CLI verwenden, um eine flache erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine durchzuführen. Aus geschäftlichen oder Konformitätsgründen können Sie eine erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine durchführen.

Ein flacher Schlüssel (auch Neuverschlüsselung genannt) ersetzt nur den Key Encryption Key (KEK). Sie müssen die verschlüsselte virtuelle Maschine nicht ausschalten, um eine flache erneute Schlüsselerstellung durchzuführen. Wenn Sie sowohl den Festplattenverschlüsselungsschlüssel (DEK) als auch den KEK ersetzen müssen, müssen Sie eine tiefe erneute Schlüsselerstellung durchführen.

Diese Aufgabe zeigt, wie Sie eine flache erneute Schlüsselerstellung auf einer verschlüsselten virtuellen Maschine mithilfe des aktuell zugewiesenen Schlüsselanbieters durchführen.

Weitere konzeptuelle Informationen finden Sie unter Vorgehensweise zum Neuverschlüsseln (erneute Schlüsselerstellung) einer verschlüsselten virtuellen Maschine.

Voraussetzungen

Erforderliche Berechtigung:**Verschlüsselungsvorgänge.Erneut verschlüsseln**

Hinweis Virtuelle Maschinen, die mit IDE-Controllern konfiguriert sind, müssen ausgeschaltet werden, um eine flache erneute Schlüsselerstellung durchzuführen.

Verfahren

1. Führen Sie in einer PowerCLI-Sitzung das `Connect-VIServer`-Cmdlet aus, um als Administrator eine Verbindung mit dem vCenter Server-Host herzustellen.

2 Weisen Sie den aktuellen Schlüsselanbieter einer Variablen zu.

```
$kp = Get-KeyProvider keyprovider_name
```

3 Weisen Sie die verschlüsselte virtuelle Maschine einer Variablen zu.

```
$vm = Get-VM encrypted_vm_name
```

4 Überprüfen Sie die Sicherheitsinformationen für die verschlüsselte virtuelle Maschine.

```
Get-SecurityInfo -Entity $vm
```

Beachten Sie die EncryptionKeyId.

5 Führen Sie die flache erneute Schlüsselerstellung der verschlüsselten virtuellen Maschine durch.

```
Set-VM -vm $vm -KeyProvider $kp
```

Geben Sie **Y** ein, um die erneute Schlüsselerstellung zu bestätigen.

6 Um sicherzustellen, dass die EncryptionKeyId geändert wurde, überprüfen Sie die Sicherheitsinformationen für die verschlüsselte virtuelle Maschine.

```
Get-SecurityInfo -Entity $vm
```

Festlegen des Standardschlüsselanbieters mithilfe des vSphere Client

Sie müssen den Standardschlüsselanbieter festlegen, wenn Sie nicht den ersten Schlüsselanbieter als Standardschlüsselanbieter verwenden oder wenn in Ihrer Umgebung mehrere Schlüsselanbieter verwendet werden und der Standardschlüsselanbieter von Ihnen entfernt wird. Sie können den vSphere Client verwenden, um den Standardschlüsselanbieter auf der vCenter Server-Ebene festzulegen.

Voraussetzungen

Als Best Practice stellen Sie sicher, dass der Verbindungsstatus auf der Registerkarte „Schlüsselanbieter“ aktiv und mit einem grünen Häkchen versehen ist.

Verfahren

1 Melden Sie sich mithilfe von vSphere Client an.

2 Navigieren Sie zum vCenter Server.

3 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

4 Wählen Sie den Schlüsselanbieter aus.

5 Klicken Sie auf **Als Standard festlegen**.

Ein Bestätigungsdialogfeld wird angezeigt.

6 Klicken Sie auf **Als Standard festlegen**.

Der Schlüsselanbieter wird als aktueller Standardschlüsselanbieter angezeigt.

Festlegen des Standardschlüsselanbieters über die Befehlszeile

Sie müssen den Standardschlüsselanbieter festlegen, wenn Sie nicht den ersten Schlüsselanbieter als Standardschlüsselanbieter verwenden oder wenn in Ihrer Umgebung mehrere Schlüsselanbieter verwendet werden und der Standardschlüsselanbieter von Ihnen entfernt wird. Sie können PowerCLI verwenden, um den Standardschlüsselanbieter auf vCenter Server-, Cluster- oder Clusterordnerebene festzulegen.

Voraussetzungen

Als Best Practice stellen Sie sicher, dass der Verbindungsstatus auf der Registerkarte „Schlüsselanbieter“ aktiv und mit einem grünen Häkchen versehen ist.

Sie müssen über eine Rolle mit dem **Verschlüsselungsvorgänge.KMS verwalten**-Recht verfügen. In „vSphere Trust Authority“ muss die Rolle auf den vertrauenswürdigen Cluster angewendet werden.

Verfahren

1 Stellen Sie sicher, dass Sie als Administrator mit dem vCenter Server des vertrauenswürdigen Clusters verbunden sind, wenn Sie den Schlüsselanbieter erstellt haben.

Hinweis Stellen Sie in „vSphere Trust Authority“ eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters her.

```
Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
```

2 Rufen Sie den Schlüsselanbieter ab.

```
Get-KeyProvider
```

Sie können die Option `-Name` *keyprovider* verwenden, um einen einzelnen Schlüsselanbieter anzugeben.

3 Weisen Sie die Informationen über den `Get-KeyProvider`-Schlüsselanbieter einer Variable zu.

Beispiel: Dieser Befehl weist die Informationen der Variable `$kp` zu.

```
$kp = Get-KeyProvider
```

Wenn Sie über mehrere Schlüsselanbieter verfügen, können Sie `Select-Object` verwenden, um einen davon auszuwählen.

```
$kp = Get-KeyProvider | Select-Object -Index 0
```

4 Verwenden Sie einen der folgenden PowerCLI-Befehle.

Vorgehensweise zum Festlegen der Standardeinstellung	Befehl
vCenter Server-Ebene	`Set-KeyProvider -KeyProvider $kp -DefaultForSystem`
Clusterebene	Dieser Befehl legt beispielsweise den Schlüsselanbieter für den `CL-01`-Cluster fest. `Add-EntityDefaultKeyProvider -KeyProvider $kp -Entity 'CL-01'`
Clusterordnerebene	Dieser Befehl legt beispielsweise den Schlüsselanbieter für den `Cluster-Folder-01`-Clusterordner fest. `Add-EntityDefaultKeyProvider -KeyProvider $kp -Entity 'Cluster-Folder-01'`

Sichern von virtuellen Maschinen mit Virtual Trusted Platform Module

11

Mithilfe der vTPM-Funktion (Virtual Trusted Platform Module) können Sie einer virtuellen Maschine einen virtuellen TPM 2.0-Kryptoprozessor hinzufügen.

Ein vTPM ist eine softwarebasierte Darstellung eines physischen Trusted Platform Module 2.0-Chips. Ein vTPM verhält sich wie jedes andere virtuelle Gerät. Sie können ein vTPM genauso wie virtuelle CPUs, Arbeitsspeicher, Festplatten- oder Netzwerk-Controller zu einer virtuellen Maschine hinzufügen. Ein vTPM benötigt keinen Trusted Platform Module-Hardware-Chip.

Lesen Sie als Nächstes die folgenden Themen:

- Was ist ein Virtual Trusted Platform Module?
- Erstellen einer virtuellen Maschine mit einem Virtual Trusted Platform Module
- Hinzufügen des virtuellen Trusted Platform Module zu einer vorhandenen virtuellen Maschine
- Entfernen eines virtuellen Trusted Platform Module von einer virtuellen Maschine
- Angeben vTPM-fähiger virtueller Maschinen
- Anzeigen von Zertifikaten des Virtual Trusted Platform Module-Geräts
- Exportieren und Ersetzen von Virtual Trusted Platform Module-Gerätezertifikaten

Was ist ein Virtual Trusted Platform Module?

Ein vTPM (Virtual Trusted Platform Module) ist eine softwarebasierte Darstellung eines physischen Trusted Platform Module 2.0-Chips. Ein vTPM verhält sich wie jedes andere virtuelle Gerät.

vTPMs bieten hardwarebasierte sicherheitsbezogene Funktionen wie zufallsbasierte Zahlengenerierung, Nachweise, Schlüsselgenerierung und vieles mehr. Wenn vTPM zu einer virtuellen Maschine hinzugefügt wird, kann damit das Gastbetriebssystem Schlüssel, die privat sind, aktivieren. Diese Schlüssel werden nicht für das Gastbetriebssystem selbst verfügbar gemacht. Aus diesem Grund sind die Angriffspunkte von virtuellen Maschinen reduziert. In der Regel wirkt sich eine Gefährdung des Gastbetriebssystems auch auf dessen Geheimnisse aus. Die Aktivierung eines vTPM verringert dieses Risiko jedoch deutlich. Diese Schlüssel können nur durch das Gastbetriebssystem für die Verschlüsselung oder Signierung verwendet werden. Mit einem angehängten vTPM kann ein Client die Identität der virtuellen Maschine remote bestätigen und die ausgeführte Software überprüfen.

Ein vTPM benötigt keinen physischen TPM 2.0-Chip (Trusted Platform Module) auf dem ESXi-Host. Wenn Sie jedoch einen Hostnachweis durchführen möchten, benötigen Sie eine externe Entität, z. B. einen physischen TPM 2.0-Chip. Weitere Informationen hierzu finden Sie unter Sichern von ESXi-Hosts mit Trusted Platform Module.

Hinweis Einer mit einem vTPM aktivierten virtuellen Maschine ist standardmäßig keine Speicherrichtlinie zugeordnet. Nur die VM-Dateien (VM-Home) sind verschlüsselt. Sie haben die Möglichkeit, Verschlüsselung für die virtuelle Maschine und die zugehörigen Festplatten explizit hinzuzufügen. Die VM-Dateien wären dann jedoch bereits verschlüsselt.

Vorgehensweise zum Konfigurieren eines vTPM für eine virtuelle Maschine

Aus Sicht der virtuellen Maschine ist ein vTPM ein virtuelles Gerät. Sie können ein vTPM zu einer neuen oder einer vorhandenen virtuellen Maschine hinzufügen. Ein vTPM hängt von der Verschlüsselung virtueller Maschinen ab, um wichtige TPM-Daten zu sichern. Daher müssen Sie einen Schlüsselanbieter konfigurieren. Wenn Sie ein vTPM konfigurieren, werden die Dateien der virtuellen Maschine verschlüsselt, die Festplatten hingegen nicht. Sie haben die Möglichkeit, Verschlüsselung für die virtuelle Maschine und die zugehörigen Festplatten explizit hinzuzufügen.

Wenn Sie eine mit einem vTPM aktivierte virtuelle Maschine sichern, muss die Sicherung alle Daten der virtuellen Maschine umfassen, einschließlich der Datei `*.nvram`. Wenn die Datei `*.nvram` nicht in der Sicherung enthalten ist, können Sie eine virtuelle Maschine nicht mit einem vTPM wiederherstellen. Da die VM-Home-Dateien einer vTPM-fähigen virtuellen Maschine verschlüsselt sind, stellen Sie darüber hinaus sicher, dass die Verschlüsselungsschlüssel zum Zeitpunkt der Wiederherstellung verfügbar sind.

Ab vSphere 8.0 wird beim Klonen einer virtuellen Maschine mit einem vTPM durch Auswahl der Option **Ersetzen** für eine virtuelle Maschine mit einem vTPM ein neues, leeres vTPM erstellt, das seine eigenen geheimen Schlüssel und seine eigene Identität erhält. Wenn Sie die geheimen Schlüssel eines vTPM ersetzen, werden alle Schlüssel, einschließlich arbeitslastbezogener Schlüssel, ersetzt. Stellen Sie als Best Practice sicher, dass Ihre Arbeitslasten kein vTPM mehr verwenden, bevor Sie die Schlüssel ersetzen. Andernfalls funktionieren die Arbeitslasten in der geklonten virtuellen Maschine möglicherweise nicht ordnungsgemäß.

vSphere-Anforderungen für vTPMs

Zur Verwendung eines vTPM muss die vSphere-Umgebung folgende Voraussetzungen erfüllen:

- Anforderungen an virtuelle Maschinen:
  - EFI-Firmware
  - Hardwareversion 14 und höher
- Anforderungen an Komponenten:
  - vCenter Server 6.7 und höher für virtuelle Windows-Maschinen verwenden vCenter Server 7.0 Update 2 und höher für virtuelle Linux-Maschinen.

  - VM-Verschlüsselung (zum Verschlüsseln der Home-Dateien der virtuellen Maschine).
  - Für vCenter Server konfigurierter Schlüsselanbieter. Weitere Informationen hierzu finden Sie unter Vergleich von vSphere-Schlüsselanbietern.
- Unterstützung folgender Gastbetriebssysteme:
  - Linux
  - Windows Server 2008 und höher
  - Windows 7 und höher

Unterschiede zwischen einem Hardware-TPM und einem virtuellem TPM

Sie verwenden ein Hardware-TPM (Trusted Platform Module), um sichere Speicherung von Anmeldeinformationen und Schlüsseln bereitzustellen. Ein vTPM führt dieselben Funktionen wie ein TPM durch, stellt aber kryptografische Koprozessorfunktionen in der Software bereit. Ein vTPM verwendet die `.nvram`-Datei, die mithilfe von VM-Verschlüsselung verschlüsselt wird, als sicheren Speicher.

Ein Hardware-TPM enthält einen vorab geladenen Schlüssel mit der Bezeichnung „Endorsement Key“ (EK). Der EK besitzt einen privaten und öffentlichen Schlüssel. Der EK stellt dem TPM eine eindeutige Identität bereit. Für ein vTPM wird dieser Schlüssel entweder von der VMware Certificate Authority (VMCA) oder einer Drittanbieterzertifizierungsstelle (CA, Certificate Authority) bereitgestellt. Sobald das vTPM einen Schlüssel verwendet, wird der Schlüssel in der Regel nicht geändert, da ansonsten vertrauliche im vTPM gespeicherte Informationen ungültig werden. Das vTPM wendet sich zu keiner Zeit an die Drittanbieter-Zertifizierungsstelle.

Erstellen einer virtuellen Maschine mit einem Virtual Trusted Platform Module

Beim Erstellen einer virtuellen Maschine können Sie ein Virtual Trusted Platform Module (vTPM) hinzufügen, um verbesserte Sicherheitseinstellungen für das Gastbetriebssystem zur Verfügung zu stellen. Vor dem Hinzufügen eines vTPM müssen Sie einen Schlüsselanbieter erstellen.

Das virtuelle TPM von VMware ist mit TPM 2.0 kompatibel und erstellt einen virtuellen Chip mit aktiviertem TPM zur Verwendung durch die virtuelle Maschine und das von ihr gehostete Gastbetriebssystem.

Voraussetzungen

- Stellen Sie sicher, dass Ihre vSphere-Umgebung mit einem Schlüsselanbieter konfiguriert ist. Weitere Informationen hierzu finden Sie unter:
  - Konfigurieren von vSphere Trust Authority
  - Kapitel 7 Konfigurieren und Verwalten eines Standardschlüsselanbieters
  - Kapitel 8 Konfigurieren und Verwalten eines vSphere Native Key Providers

- Als Gastbetriebssystem können Sie Windows Server 2008 und höher, Windows 7 und höher oder Linux verwenden.
- Auf den in Ihrer Umgebung ausgeführten ESXi-Hosts muss ESXi 6.7 oder höher (Windows-Gastbetriebssystem) oder 7.0 Update 2 oder höher (Linux-Gastbetriebssystem) installiert sein.
- Die virtuelle Maschine muss EFI-Firmware nutzen.
- Stellen Sie sicher, dass Sie über die erforderlichen Rechte verfügen:
  - **Verschlüsselungsvorgänge.Klonen**
  - **Verschlüsselungsvorgänge.Verschlüsseln**
  - **Verschlüsselungsvorgänge.Neue verschlüsseln**
  - **Verschlüsselungsvorgänge.Migrieren**
  - **Verschlüsselungsvorgänge.VM registrieren**
  - **Verschlüsselungsvorgänge.Host registrieren**

Hinweis Nach dem Erstellen einer virtuellen Maschine mit einem vTPM ist die Berechtigung **Kryptografievorgänge.Direktzugriff** erforderlich, um eine Konsolensitzung zu öffnen.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.
3. Klicken Sie mit der rechten Maustaste auf das Objekt, wählen Sie **Neue virtuelle Maschine** aus und befolgen Sie die Anweisungen zum Erstellen einer virtuellen Maschine.

Option	Aktion
Erstellungstyp auswählen	Erstellen Sie eine neue virtuelle Maschine.
Namen und Ordner auswählen	Legen Sie einen Namen und einen Zielspeicherort fest.
Computing-Ressource auswählen	Geben Sie ein Objekt an, für das Sie über Berechtigungen zum Erstellen einer virtuellen Maschine verfügen. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für VM-Verschlüsselungsaufgaben.
Speicher auswählen	Wählen Sie einen kompatiblen Datenspeicher aus.
Kompatibilität auswählen	Sie müssen **ESXi 6.7 und höher** für ein Windows-Gastbetriebssystem oder **ESXi 7.0 U2** und höher für ein Linux-Gastbetriebssystem auswählen.
Gastbetriebssystem auswählen	Wählen Sie Windows oder Linux als Gastbetriebssystem aus.

Option	Aktion
Hardware anpassen	Klicken Sie auf **Neues Gerät hinzufügen** und wählen Sie **Trusted Platform Module** aus. Passen Sie die Hardware weiter an, indem Sie beispielsweise die Festplattengröße oder die CPU ändern.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

Ergebnisse

Die vTPM-fähige virtuelle Maschine wird wie angegeben in Ihrem Bestand angezeigt.

Hinzufügen des virtuellen Trusted Platform Module zu einer vorhandenen virtuellen Maschine

Sie können ein virtuelles Trusted Platform Module (vTPM) einer vorhandenen virtuellen Maschine hinzufügen, um verbesserte Sicherheitseinstellungen für das Gastbetriebssystem zur Verfügung zu stellen. Vor dem Hinzufügen eines vTPM müssen Sie einen Schlüsselanbieter erstellen.

VMware Virtual TPM ist mit TPM 2.0 kompatibel und erstellt einen virtuellen Chip mit aktiviertem TPM zur Verwendung durch die virtuelle Maschine und das von ihr gehostete Gastbetriebssystem.

Voraussetzungen

- Stellen Sie sicher, dass Ihre vSphere-Umgebung für einen Schlüsselanbieter konfiguriert ist. Weitere Informationen hierzu finden Sie unter:
  - Konfigurieren von vSphere Trust Authority
  - Kapitel 7 Konfigurieren und Verwalten eines Standardschlüsselanbieters
  - Kapitel 8 Konfigurieren und Verwalten eines vSphere Native Key Providers
- Als Gastbetriebssystem können Sie Windows Server 2008 und höher, Windows 7 und höher oder Linux verwenden.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- Auf den in Ihrer Umgebung ausgeführten ESXi-Hosts muss ESXi 6.7 oder höher (Windows-Gastbetriebssystem) oder 7.0 Update 2 oder höher (Linux-Gastbetriebssystem) installiert sein.
- Die virtuelle Maschine muss EFI-Firmware nutzen.
- Stellen Sie sicher, dass Sie über die erforderlichen Rechte verfügen:
  - **Verschlüsselungsvorgänge.Klonen**
  - **Verschlüsselungsvorgänge.Verschlüsseln**
  - **Verschlüsselungsvorgänge.Neue verschlüsseln**
  - **Verschlüsselungsvorgänge.Migrieren**

- **Verschlüsselungsvorgänge.VM registrieren**
- **Virtuelle Maschine.Konfiguration ändern.Gerät hinzufügen oder entfernen**

Hinweis Nach dem Hinzufügen eines vTPM zu einer virtuellen Maschine ist die Berechtigung **Kryptografievorgänge.Direktzugriff** erforderlich, um eine Konsolensitzung zu öffnen.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.
3. Klicken Sie im Dialogfeld **Einstellungen bearbeiten** auf **Neues Gerät hinzufügen** und wählen Sie **Trusted Platform Module** aus.
4. Klicken Sie auf **OK**.

   Der Bereich **VM-Details** zeigt an, dass die Verschlüsselung auf die virtuelle Maschine angewendet wurde.

Entfernen eines virtuellen Trusted Platform Module von einer virtuellen Maschine

Sie können die virtuelle Trusted Platform Module-Sicherheit (vTPM) von einer virtuellen Maschine entfernen.

Das Entfernen eines vTPM-Geräts führt dazu, dass alle verschlüsselten Informationen auf der virtuellen Maschine nicht mehr wiederherstellbar sind. Bevor Sie ein vTPM von einer virtuellen Maschine entfernen, müssen Sie alle Anwendungen im Gastbetriebssystem deaktivieren, die das vTPM-Gerät verwenden (wie z. B. BitLocker). Wenn Sie dies nicht tun, kann die virtuelle Maschine unter Umständen nicht gestartet werden. Darüber hinaus können Sie ein vTPM-Gerät auch nicht aus einer virtuellen Maschine entfernen, die Snapshots enthält.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- Stellen Sie sicher, dass Sie über die erforderlichen Rechte verfügen: **Virtuelle Maschine.Konfiguration ändern.Gerät hinzufügen oder entfernen** und **Verschlüsselungsvorgänge.Entschlüsseln**

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.
3. Erweitern Sie auf der Registerkarte **Virtuelle Hardware** die Option **Sicherheitsgeräte**.
4. Klicken Sie auf das Auslassungszeichen für Virtuelles TPM.

5 Klicken Sie auf **Gerät entfernen**.

6 Klicken Sie auf **Löschen**, um zu bestätigen, dass Sie das vTPM entfernen möchten.

Das vTPM-Gerät ist zum Entfernen markiert.

7 Klicken Sie auf **OK**.

Angeben vTPM-fähiger virtueller Maschinen

Sie können feststellen, welche Ihrer virtuellen Maschinen für die Verwendung eines Virtual Trusted Platform Module (vTPM) aktiviert sind.

Sie können eine Liste aller virtuellen Maschinen in Ihrer Bestandsliste generieren, in der der Name, das Betriebssystem und der vTPM-Status der virtuellen Maschinen angezeigt werden. Sie können diese Liste zur Verwendung in Konformitätsprüfungen auch in eine CSV-Datei exportieren.

Verfahren

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

2 Wählen Sie eine vCenter Server-Instanz, einen Host oder einen Cluster aus.

3 Klicken Sie auf der Registerkarte **VMs** auf **Virtuelle Maschinen**.

4 Um alle virtuellen Maschinen anzuzeigen, auf denen ein TPM aktiviert ist, klicken Sie auf **Spalten verwalten** und wählen Sie **TPM** aus.

In der TPM-Spalte wird für virtuelle Maschinen, auf denen TPM aktiviert ist, „Vorhanden“ angezeigt. Virtuelle Maschinen ohne TPM werden als „Nicht vorhanden“ aufgeführt.

5 Um den Inhalt einer Bestandslistenansicht in eine CSV-Datei zu exportieren, klicken Sie auf **Exportieren**.

Anzeigen von Zertifikaten des Virtual Trusted Platform Module-Geräts

Im Lieferumfang von vTPM-Geräten (Virtual Trusted Platform Module) sind vorkonfigurierte Standardzertifikate enthalten, die von Ihnen überprüft werden können.

Voraussetzungen

In Ihrer Umgebung muss eine virtuelle Maschine mit aktiviertem vTPM vorhanden sein.

Verfahren

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

2 Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.

3 Um vTPM-fähige virtuelle Maschinen zu identifizieren, klicken Sie auf **VMs** und dann auf **Virtuelle Maschinen**.

   Klicken Sie bei Bedarf auf **Spalten verwalten** und wählen Sie **TPM** aus, um virtuelle Maschinen mit einem TPM „Vorhanden“ anzuzeigen.

4 Wählen Sie die vTPM-fähige VM aus, deren Zertifikatsinformationen angezeigt werden sollen.

5 Klicken Sie auf die Registerkarte **Konfiguration** der virtuellen Maschine.

6 Wählen Sie unter **TPM** die Option **Zertifikate** aus.

7 Wählen Sie das Zertifikat aus und zeigen Sie dessen Informationen an.

8 (Optional) Klicken Sie zum Exportieren der Zertifikatsinformationen auf **Exportieren**.

   Das Zertifikat wird auf der Festplatte gespeichert.

Nächste Schritte

Sie können das Standardzertifikat durch ein von einer Drittanbieter-Zertifizierungsstelle (CA) ausgestelltes Zertifikat ersetzen. Weitere Informationen hierzu finden Sie unter Exportieren und Ersetzen von Virtual Trusted Platform Module-Gerätezertifikaten.

Exportieren und Ersetzen von Virtual Trusted Platform Module-Gerätezertifikaten

Sie können das im Lieferumfang eines vTPM-Geräts (Virtual Trusted Platform Module) enthaltene Standardzertifikat ersetzen.

Voraussetzungen

In Ihrer Umgebung muss eine virtuelle Maschine mit aktiviertem vTPM vorhanden sein.

Verfahren

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

2 Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.

3 Wählen Sie in der Bestandsliste die virtuelle Maschine mit aktiviertem vTPM aus, deren Zertifikatsinformationen Sie ersetzen möchten.

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

5 Wählen Sie unter **TPM** die Option **Signieranforderungen** aus.

6 Wählen Sie ein Zertifikat aus.

7 Um die Zertifikatsinformationen zu exportieren, klicken Sie auf **Exportieren**.

   Das Zertifikat wird auf der Festplatte gespeichert.

8 Rufen Sie für die von Ihnen exportierte Zertifikatsignieranforderung (Certificate Signing Request, CSR) ein von einer Drittanbieter-Zertifizierungsstelle (Certificate Authority, CA) ausgestelltes Zertifikat ab.

   Sie können eine beliebige Zertifizierungsstelle verwenden, die in Ihrer IT-Umgebung möglicherweise verfügbar ist.

9 Wenn Ihnen das neue Zertifikat zur Verfügung steht, ersetzen Sie das vorhandene Zertifikat.

   a Klicken Sie mit der rechten Maustaste in der Bestandsliste auf die virtuelle Maschine, deren Zertifikat Sie ersetzen möchten, und wählen Sie **Einstellungen bearbeiten** aus.

   b Erweitern Sie im Dialogfeld **Einstellungen bearbeiten** die Option **Sicherheitsgeräte** und erweitern Sie dann **Virtuelle TPM**.

      Das Zertifikat wird angezeigt.

   c Klicken Sie für das Zertifikat, das Sie ersetzen möchten, auf **Ersetzen**.

      Das Dialogfeld **Datei-Upload** wird angezeigt.

   d Suchen Sie das neue Zertifikat auf Ihrer lokalen Maschine und laden Sie es hoch.

      Das neue Zertifikat ersetzt das Standardzertifikat, das im Lieferumfang Ihres vTPM-Geräts enthalten war.

   e Die Zertifikatsinformationen werden in der Zertifikateliste aktualisiert.

Sichern von Windows-Gastbetriebssystemen mit virtualisierungsbasierter Sicherheit

12

In vSphere 6.7 und höher können Sie Microsoft VBS (Virtualization-Based Security, Virtualisierungsbasierte Sicherheit) auf unterstützten Windows-Gastbetriebssystemen aktivieren.

Microsoft VBS, eine in Windows 10 und Windows Server 2016 eingeführte Funktion, verwendet Hardware- und Softwarevirtualisierung zur Verbesserung der Systemsicherheit, indem ein isoliertes auf einen Hypervisor beschränktes spezialisiertes Subsystem erstellt wird.

Mit VBS können Sie die folgenden Windows-Sicherheitsfunktionen verwenden, um das System zusätzlich zu sichern und wichtige System- und Benutzergeheimnisse vor Missbrauch zu schützen:

- Credential Guard: Zielt darauf ab, wichtige System- und Benutzergeheimnisse zu isolieren und vor Missbrauch zu schützen.
- Device Guard: Stellt eine Gruppe von Funktionen bereit, mit denen die Ausführung von Malware auf einem Windows-System vermieden werden kann.
- Konfigurierbare Codeintegrität: Stellt sicher, dass nur vertrauenswürdiger Code nach dem Bootloader-Programm ausgeführt wird.

Weitere Informationen finden Sie im Thema zu virtualisierungsbasierter Sicherheit in der Microsoft-Dokumentation.

Nachdem Sie VBS für eine virtuelle Maschine über vCenter Server aktiviert haben, aktivieren Sie VBS innerhalb des Windows-Gastbetriebssystems.

Lesen Sie als Nächstes die folgenden Themen:

- Best Practices für die Sicherheit auf Basis der vSphere-Virtualisierung
- Aktivieren der virtualisierungsbasierten Sicherheit auf einer virtuellen Maschine
- Aktivieren der virtualisierungsbasierten Sicherheit auf einer vorhandenen virtuellen Maschine
- Aktivieren von virtualisierungsbasierter Sicherheit auf dem Gastbetriebssystem
- Deaktivieren von virtualisierungsbasierter Sicherheit
- Identifizieren von VBS-fähigen virtuellen Maschinen

Best Practices für die Sicherheit auf Basis der vSphere-Virtualisierung

Befolgen Sie die empfohlenen Vorgehensweisen für virtualisierungsbasierte Sicherheit (VBS), um Sicherheit und Handhabbarkeit Ihrer Windows-Gastbetriebssystemumgebung zu maximieren.

Vermeiden Sie Probleme, indem Sie diese empfohlenen Vorgehensweisen befolgen.

VBS-Hardwareanforderungen

Verwenden Sie folgende Hardware für VBS:

- Intel
  - Haswell-CPU oder höher. Verwenden Sie für eine optimale Leistung die Skylake-EP-CPU oder höher.
  - Die Ivy-Bridge-CPU ist akzeptabel.
  - Die Sandy-Bridge-CPU kann die Leistung beeinträchtigen.
- AMD
  - CPUs der Zen 2-Serie (Rome) oder höher.
  - Ältere CPUs können die Leistung beeinträchtigen.

Die Risikominderungen für die Schwachstelle „Machine Check Exception on Page Size Change Intel CPU“ können sich negativ auf die Leistung des Gastbetriebssystems auswirken, wenn VBS verwendet wird. Weitere Informationen finden Sie im VMware Knowledge Base-Artikel unter https://kb.vmware.com/kb/76050.

Kompatibilität von VBS und Windows-Gastbetriebssystemen

Auf Intel wird VBS für virtuelle Maschinen unter Windows 10, Windows Server 2016 und höher unterstützt. Für die Windows Server 2016-Versionen 1607 und 1703 sind jedoch Patches erforderlich. In der Microsoft-Dokumentation finden Sie Informationen zur Hardwarekompatibilität der ESXi-Hosts. Die Verwendung von Intel-CPUs für VBS erfordert vSphere 6.7 oder höher und Hardwareversion 14 oder höher.

Auf AMD wird VBS auf virtuellen Maschinen mit Windows 10, Version 1809 und Windows 2019 und höher unterstützt. Die Verwendung von AMD-CPUs für VBS erfordert vSphere 7.0 Update 2 oder höher und Hardwareversion 19 oder höher.

Anfänglich war für Windows 10 erforderlich, dass Sie Hyper-V für VBS aktivieren. Die Aktivierung von Hyper-V ist für Windows 10 nicht erforderlich. Dasselbe gilt für Windows Server 2016 und höher. Weitere Informationen finden Sie in der aktuellen Microsoft-Dokumentation und in den *VMware vSphere-Versionshinweisen* .

Nicht unterstützte VMware-Funktionen auf VBS

Die folgenden Funktionen werden bei aktivierter VBS auf einer virtuellen Maschine nicht unterstützt:

- Fault Tolerance
- PCI-Passthrough
- CPU oder Arbeitsspeicher im laufenden Betrieb hinzufügen

Installations- und Upgrade-Einschränkungen mit VBS

Vor der Konfiguration von VBS müssen Sie sich mit den folgenden Einschränkungen hinsichtlich Installation und Aktualisierung vertraut machen:

- Neue virtuelle Maschinen, die in niedrigeren virtuellen Hardwareversionen als Version 14 für Windows 10 und Windows Server 2016 und höher konfiguriert werden, werden standardmäßig mit dem Legacy-BIOS erstellt. Sie müssen das Gastbetriebssystem neu installieren, nachdem Sie den Firmware-Typ der virtuellen Maschine von Legacy-BIOS in UEFI geändert haben.
- Wenn Sie Ihre virtuellen Maschinen von vorherigen vSphere-Versionen zu vSphere 6.7 oder höher migrieren und VBS auf den virtuellen Maschinen aktivieren möchten, verwenden Sie UEFI, um eine Neuinstallation des Betriebssystems zu vermeiden.

Aktivieren der virtualisierungsbasierten Sicherheit auf einer virtuellen Maschine

Sie können die virtualisierungsbasierte Sicherheit (VBS) von Microsoft für unterstützte Windows-Gastbetriebssysteme während der Erstellung einer virtuellen Maschine aktivieren.

Die Konfiguration von VBS ist ein Prozess, bei dem VBS zuerst in der virtuellen Maschine und anschließend im Windows-Gastbetriebssystem aktiviert wird.

Voraussetzungen

Weitere Informationen zu geeigneten CPUs finden Sie unter Best Practices für die Sicherheit auf Basis der vSphere-Virtualisierung.

Die Verwendung von Intel-CPUs für VBS erfordert vSphere 6.7 oder höher. Erstellen Sie eine virtuelle Maschine, für die Hardwareversion 14 oder höher und eines der folgenden unterstützten Gastbetriebssysteme verwendet wird:

- Windows 10 (64 Bit) oder höhere Versionen
- Windows Server 2016 (64 Bit) oder höhere Versionen

Die Verwendung von AMD-CPUs für VBS erfordert vSphere 7.0 Update 2 oder höher. Erstellen Sie eine virtuelle Maschine, für die Hardwareversion 19 oder höher und eines der folgenden unterstützten Gastbetriebssysteme verwendet wird:

- Windows 10 (64 Bit), Version 1809 oder höhere Versionen
- Windows Server 2019 (64 Bit) oder höhere Versionen

Stellen Sie sicher, dass Sie die neuesten Patches für Windows 10, Version 1809, und Windows Server 2019 installieren, bevor Sie VBS aktivieren.

Weitere Informationen zum Aktivieren von VBS auf virtuellen Maschinen auf AMD-Plattformen finden Sie im VMware KB-Artikel unter https://kb.vmware.com/s/article/89880.

Verfahren

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

2 Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.

3 Klicken Sie mit der rechten Maustaste auf das Objekt, wählen Sie **Neue virtuelle Maschine** aus und befolgen Sie die Anweisungen zum Erstellen einer virtuellen Maschine.

Option	Aktion
Erstellungstyp auswählen	Erstellen Sie eine virtuelle Maschine.
Namen und Ordner auswählen	Legen Sie einen Namen und einen Zielspeicherort fest.
Computing-Ressource auswählen	Geben Sie ein Objekt an, für das Sie über Rechte zum Erstellen von virtuellen Maschinen verfügen.
Speicher auswählen	Wählen Sie in der VM-Speicherrichtlinie die entsprechende Speicherrichtlinie aus. Wählen Sie einen kompatiblen Datenspeicher aus.
Kompatibilität auswählen	Intel-CPU: Stellen Sie sicher, dass **ESXi 6.7 und höher** ausgewählt ist. AMD-CPU: Stellen Sie sicher, dass **ESXi 7.0 U2 und höher** ausgewählt ist.
Gastbetriebssystem auswählen	Wählen Sie die Option „Windows-Gastbetriebssystem“ aus, die der Betriebssystemversion am besten entspricht. Aktivieren Sie das Kontrollkästchen **Virtualisierungsbasierte Sicherheit für Windows aktivieren**.
Hardware anpassen	Passen Sie die Hardware an, indem Sie z. B. die Festplattengröße oder die CPU ändern.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

Ergebnisse

Auf der Kachel „Details zur virtuellen Maschine“ auf der Registerkarte **Übersicht** wird „Virtualisierungsbasierte Sicherheit – Aktivieren“ angezeigt.

Nächste Schritte

Weitere Informationen hierzu finden Sie unter Aktivieren von virtualisierungsbasierter Sicherheit auf dem Gastbetriebssystem.

Aktivieren der virtualisierungsbasierten Sicherheit auf einer vorhandenen virtuellen Maschine

Sie können die virtualisierungsbasierte Sicherheit (VBS) von Microsoft auf vorhandenen virtuellen Maschinen für unterstützte Windows-Gastbetriebssysteme aktivieren.

Die Konfiguration von VBS ist ein Prozess, bei dem VBS zuerst in der virtuellen Maschine und anschließend im Gastbetriebssystem aktiviert wird.

Hinweis Neue virtuelle Maschinen, die in niedrigeren Hardwareversionen als Version 14 für Windows 10, Windows Server 2016 und Windows Server 2019 konfiguriert werden, werden standardmäßig mit dem Legacy-BIOS erstellt. Wenn Sie den Firmwaretyp der virtuellen Maschine von Legacy-BIOS in UEFI ändern, müssen Sie das Gastbetriebssystem neu installieren.

Voraussetzungen

Weitere Informationen zu geeigneten CPUs finden Sie unter Best Practices für die Sicherheit auf Basis der vSphere-Virtualisierung.

Die Verwendung von Intel-CPUs für VBS erfordert vSphere 6.7 oder höher. Die virtuelle Maschine muss mit der Hardwareversion 14 oder höher und einem der folgenden unterstützten Gastbetriebssysteme erstellt worden sein:

- Windows 10 (64 Bit) oder höhere Versionen
- Windows Server 2016 (64 Bit) oder höhere Versionen

Die Verwendung von AMD-CPUs für VBS erfordert vSphere 7.0 Update 2 oder höher. Die virtuelle Maschine muss mit der Hardwareversion 19 oder höher und einem der folgenden unterstützten Gastbetriebssysteme erstellt worden sein:

- Windows 10 (64 Bit), Version 1809 oder höhere Versionen
- Windows Server 2019 (64 Bit) oder höhere Versionen

Stellen Sie sicher, dass Sie die neuesten Patches für Windows 10, Version 1809, und Windows Server 2019 installieren, bevor Sie VBS aktivieren.

Weitere Informationen zum Aktivieren von VBS auf virtuellen Maschinen auf AMD-Plattformen finden Sie im VMware KB-Artikel unter https://kb.vmware.com/s/article/89880.

Verfahren

1. Navigieren Sie im vSphere Client zur virtuellen Maschine.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

3 Klicken Sie auf die Registerkarte **VM-Optionen**.

4 Aktivieren Sie das Kontrollkästchen **Aktivieren** für die virtualisierungsbasierte Sicherheit.

5 Klicken Sie auf **OK**.

Ergebnisse

Auf der Kachel „Details zur virtuellen Maschine“ auf der Registerkarte **Übersicht** wird „Virtualisierungsbasierte Sicherheit – Aktivieren“ angezeigt.

Nächste Schritte

Weitere Informationen hierzu finden Sie unter Aktivieren von virtualisierungsbasierter Sicherheit auf dem Gastbetriebssystem.

Aktivieren von virtualisierungsbasierter Sicherheit auf dem Gastbetriebssystem

Sie können die virtualisierungsbasierte Sicherheit (VBS) von Microsoft für unterstützte Windows-Gastbetriebssysteme aktivieren.

Sie aktivieren VBS innerhalb des Windows-Gastbetriebssystems. Windows konfiguriert und erzwingt VBS über ein Gruppenrichtlinienobjekt (GPO). Mit dem Gruppenrichtlinienobjekt können Sie die verschiedenen von VBS bereitgestellten Dienste aus- und einschalten, beispielsweise sicherer Start, Device Guard und Credential Guard. Bei bestimmten Windows-Versionen müssen Sie einen zusätzlichen Schritt zur Aktivierung der Hyper-V-Plattform durchführen.

In der Microsoft-Dokumentation finden Sie Details zum Bereitstellen von Device Guard, um die virtualisierungsbasierte Sicherheit zu aktivieren.

Voraussetzungen

- Stellen Sie sicher, dass die virtualisierungsbasierte Sicherheit auf der virtuellen Maschine aktiviert wurde.

Verfahren

1 Bearbeiten Sie unter Microsoft Windows die Gruppenrichtlinie, um VBS zu aktivieren, und wählen Sie andere VBS-bezogene Sicherheitsoptionen aus.

2 (Optional) Bei Microsoft Windows-Versionen vor Redstone 4 aktivieren Sie die Hyper-V-Plattform in der Systemsteuerung unter „Windows-Funktionen“.

3 Starten Sie das Gastbetriebssystem neu.

Deaktivieren von virtualisierungsbasierter Sicherheit

Falls Sie die virtualisierungsbasierte Sicherheit (VBS) bei einer virtuellen Maschine nicht mehr verwenden, können Sie sie deaktivieren. Bei der Deaktivierung von VBS für die virtuelle Maschine bleiben die VBS-Optionen von Windows unverändert, sie rufen dann aber möglicherweise

Leistungsprobleme hervor. Deaktivieren Sie VBS-Optionen in Windows, bevor Sie VBS auf der virtuellen Maschine deaktivieren.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

Verfahren

1. Navigieren Sie im vSphere Client zu der virtuellen Maschine, die VBS verwendet.

   Unter Identifizieren von VBS-fähigen virtuellen Maschinen finden Sie Hilfe bei der Suche nach virtuellen Maschinen, die VBS verwenden.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
3. Klicken Sie auf **VM-Optionen**.
4. Deaktivieren Sie das Kontrollkästchen **Aktivieren** für die virtualisierungsbasierte Sicherheit.

   Sie werden in einer Meldung daran erinnert, VBS im Gastbetriebssystem zu deaktivieren.
5. Klicken Sie auf **OK**.
6. Stellen Sie sicher, dass auf der Registerkarte **Übersicht** der virtuellen Maschine in der Beschreibung des Gastbetriebssystems nicht mehr „Virtualisierungsbasierte Sicherheit – Aktiviert“ angezeigt wird.

Identifizieren von VBS-fähigen virtuellen Maschinen

Sie können ermitteln, auf welcher Ihrer virtuellen Maschinen VBS zu Berichterstellungs- und Übereinstimmungszwecken aktiviert ist.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Wählen Sie eine vCenter Server-Instanz, ein Datencenter oder einen Host in der Bestandsliste aus.
3. Klicken Sie auf der Registerkarte **VMs** auf **Virtuelle Maschinen**.
4. Um die Spalte **VBS** anzuzeigen, klicken Sie auf **Spalten verwalten** und aktivieren Sie das Kontrollkästchen **VBS**.
5. Durchsuchen Sie die Spalte **VBS** nach „Vorhanden“.

Sichern der vSphere-Netzwerke 13

Die Sicherung von vSphere-Netzwerken ist ein wesentlicher Bestandteil des Schutzes 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*.

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.

Verwenden von 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.

Hostbasierte Firewalls können die Leistung beeinträchtigen. Stimmen Sie Ihre Sicherheitsbedürfnisse mit den Leistungszielen ab, bevor Sie hostbasierte Firewalls auf virteullen Maschinen an anderen Positionen im virtuellen Netzwerk installieren.

Weitere Informationen hierzu finden Sie unter Absichern des Netzwerks mit Firewalls.

Verwenden der Netzwerksegmentierung

Behalten Sie verschiedene Zonen aus virtuellen Maschinen innerhalb eines Hosts auf verschiedenen Netzwerksegmenten bei. Wenn Sie jede virtuelle Maschinenzone in deren eigenem Netzwerksegment isolieren, minimieren Sie das Risiko eines Datenverlusts zwischen zwei Zonen. Segmentierung verhindert verschiedene Bedrohungen, einschließlich ARP-Manipulation (Address Resolution Protocol). Bei der ARP-Manipulation verändert ein Angreifer

die ARP-Tabelle dahingehend, dass MAC- und IP-Adressen neu zugeordnet werden, und erhält somit Zugriff auf Netzwerkverkehr von und zu einem Host. Angreifer verwenden diese ARP-Manipulation für Man-in-the-Middle-Angriffe (MITM), für Denial of Service-Angriffe (DoS), zur Übernahme des Zielsystems und zur anderweitigen Beeinträchtigung des virtuellen Netzwerks.

Durch eine umsichtige Planung der Segmentierung wird das Risiko von Paketübertragungen zwischen VM-Zonen gesenkt. Durch die Segmentierung werden Spionageangriffe verhindert, die das Senden von Netzwerkverkehr an das Opfer erforderlich machen. So kann ein Angreifer auch keinen unsicheren Dienst in einer virtuellen Maschinenzone aktivieren, um auf andere virtuelle Maschinenzonen im Host zuzugreifen. Die Segmentierung können Sie mithilfe einer der beiden folgenden Methoden implementieren.

- Verwenden Sie getrennte physische Netzwerkadapter für Zonen virtueller Maschinen, damit die Zonen auch tatsächlich voneinander getrennt sind. Die Beibehaltung getrennter physischer Netzwerkadapter für die virtuellen Maschinenzonen stellt unter Umständen die sicherste Methode nach dem Anlegen des ersten Segments dar. Dieser Ansatz ist weniger anfällig für Konfigurationsfehler.
- Richten Sie virtuelle LANs (VLANs) zur Absicherung des Netzwerks ein. VLANs bieten fast alle Sicherheitsvorteile, die der Installation physisch getrennter Netzwerke innewohnen, ohne dass zusätzliche Hardware angeschafft werden muss. Bei Verwendung von VLANs fallen keine Kosten für Bereitstellung und Verwaltung zusätzlicher Geräte, Verkabelung usw. an. Weitere Informationen hierzu finden Sie unter Absichern virtueller Maschinen durch VLANs.

Verhindern des nicht autorisierten Zugriffs auf virtuelle Maschinen

Anforderungen an die Sicherung von virtuellen Maschinen entsprechen häufig den Anforderungen an die Sicherung physischer Maschinen.

- Wenn ein VM-Netzwerk an ein physisches Netzwerk angeschlossen ist, kann es ebenso Sicherheitslücken aufweisen wie ein Netzwerk, das aus physischen Maschinen besteht.
- Selbst wenn Sie keine virtuelle Maschine mit dem physischen Netzwerk verbinden, kann die virtuelle Maschine von anderen virtuellen Maschinen angegriffen werden.

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. Dennoch kann jede virtuelle Maschine oder VM-Gruppe innerhalb des Netzwerks weiterhin Ziel eines unerlaubten Zugriffs durch andere virtuelle Maschinen sein. Schützen Sie Ihre virtuellen Maschinen vor unerlaubtem Zugriff.

Weitere Informationen zum Schutz virtueller Maschinen finden Sie im NIST-Dokument mit dem Titel „Sichere virtuelle Netzwerkkonfiguration zum Schutz virtueller Maschinen (VM)“ unter:

https://csrc.nist.gov/publications/detail/sp/800-125b/final

Lesen Sie als Nächstes die folgenden Themen:

- Absichern des Netzwerks mit Firewalls

- Sichern des physischen Switches auf ESXi-Hosts
- Sichern von Standard-Switch-Ports durch Sicherheitsrichtlinien
- Sichern von vSphere Standard-Switches
- Schutz von Standard-Switches und VLANs
- Sichern von vSphere Distributed Switches und verteilten Portgruppen
- Absichern virtueller Maschinen durch VLANs
- Erstellen mehrerer Netzwerke auf einem einzelnen ESXi-Host
- Verwenden von Internet Protocol Security auf ESXi-Hosts
- Sicherstellen der ordnungsgemäßen SNMP-Konfiguration auf ESXi-Hosts
- vSphere Networking, empfohlene Vorgehensweisen für die Sicherheit

Absichern des Netzwerks mit Firewalls

Sicherheitsadministratoren verwenden Firewalls, um das Netzwerk oder ausgewählte Komponenten innerhalb des Netzwerks vor unerlaubten Zugriffen zu schützen.

Firewalls kontrollieren den Zugriff auf die Geräte in ihrem Umfeld, indem sie alle Ports außer denen abriegeln, die der Administrator explizit oder implizit als zulässig definiert. Die Ports, die Administratoren öffnen, erlauben Datenverkehr zwischen Geräten auf beiden Seiten der Firewall.

Wichtig Mit der ESXi-Firewall in ESXi 5.5 und höher kann der vMotion-Datenverkehr nicht pro Netzwerk gefiltert werden. Daher müssen Sie Regeln für Ihre externe Firewall installieren, um sicherzustellen, dass keine eingehenden Verbindungen mit dem vMotion-Socket hergestellt werden können.

In der Umgebung mit virtuellen Maschinen können Sie das Layout für die Firewalls zwischen den Komponenten planen.

- Firewalls zwischen physischen Maschinen, z. B. vCenter Server-Systemen und ESXi-Hosts.
- Firewalls zwischen zwei virtuellen Maschinen – beispielsweise zwischen einer virtuellen Maschine, die als externer Webserver dient, und einer virtuellen Maschine, die an das interne Firmennetzwerk angeschlossen ist.
- Firewalls zwischen einem physischen Computer und einer virtuellen Maschine, wenn Sie beispielsweise eine Firewall zwischen einen physischen Netzwerkadapter und eine virtuelle Maschine schalten.

Die Nutzungsweise von Firewalls in einer ESXi-Konfiguration hängt davon ab, wie Sie das Netzwerk nutzen möchten und wie sicher die einzelnen Komponenten sein müssen. Wenn Sie zum Beispiel ein virtuelles Netzwerk erstellen, in dem jede virtuelle Maschine eine andere Benchmark-Testsuite für die gleiche Abteilung ausführt, ist das Risiko ungewollten Zugriffs von

einer virtuellen Maschine auf eine andere minimal. Eine Konfiguration, bei der Firewalls zwischen den virtuellen Maschinen vorhanden sind, ist daher nicht erforderlich. Um jedoch eine Störung der Testläufe durch einen externen Host zu verhindern, kann eine Firewall am Eingangspunkt zum virtuellen Netzwerk konfiguriert werden, um alle virtuellen Maschinen zu schützen.

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

Firewalls in Konfigurationen mit vCenter Server

Wenn Sie über vCenter Server auf ESXi-Hosts zugreifen, schützen Sie vCenter Server normalerweise durch eine Firewall.

Firewalls müssen an den Zugangspunkten vorhanden sind. Eine Firewall kann zwischen den Clients und vCenter Server vorhanden sein, oder vCenter Server und die Clients können sich beide hinter einer Firewall befinden.

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

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

Firewalls können je nach Netzwerkauslastung und der für Clients erforderlichen Sicherheitsstufe auch an anderen Zugriffspunkten im Netzwerk hinzugefügt werden. Bestimmen Sie die Installationspunkte für Ihre Firewalls anhand der Sicherheitsrisiken für Ihre Netzwerkkonfiguration. Die folgenden Firewall-Installationspunkte werden häufig verwendet.

- Zwischen dem vSphere Client oder einem Netzwerkverwaltungs-Client eines Drittanbieters und vCenter Server.
- Wenn die Benutzer über einen Webbrowser auf virtuelle Maschinen zugreifen, zwischen dem Webbrowser und dem ESXi-Host.
- Wenn die Benutzer über den vSphere Client auf virtuelle Maschinen zugreifen, zwischen dem vSphere Client und dem ESXi-Host. Diese Verbindung ist ein Zusatz zu der Verbindung zwischen dem vSphere Client und vCenter Server und benötigt einen anderen Port.
- Zwischen vCenter Server und den ESXi-Hosts.
- Zwischen den ESXi-Hosts in Ihrem Netzwerk. Zwar ist der Datenverkehr zwischen Hosts normalerweise vertrauenswürdig, aber Sie können bei befürchteten Sicherheitsrisiken zwischen den einzelnen Computern dennoch Firewalls zwischen den Hosts installieren.

Wenn Sie Firewalls zwischen ESXi-Hosts hinzufügen und die Migration virtueller Maschinen zwischen diesen Hosts planen, öffnen Sie Ports in einer beliebigen Firewall, die den Quellhost von den Zielhosts trennt.

- Zwischen ESXi-Hosts und Netzwerkspeicher, z. B. NFS- oder iSCSI-Speicher. Diese Ports sind nicht VMware-spezifisch. Konfigurieren Sie sie anhand der Spezifikationen für das jeweilige Netzwerk.

Herstellen einer Verbindung mit einem vCenter Server über eine Firewall

Öffnen Sie TCP-Port 443 in der Firewall, um vCenter Server den Empfang von Daten zu ermöglichen.

vCenter Server verwendet standardmäßig TCP-Port 443, um die Datenübertragung von seinen Clients zu überwachen. Wenn eine Firewall zwischen vCenter Server und den Clients vorhanden ist, müssen Sie eine Verbindung konfigurieren, über die vCenter Server Daten von den Clients empfangen kann. Die Firewall-Konfiguration hängt von den an Ihrer Site verwendeten Komponenten ab. Weitere Informationen erhalten Sie von Ihrem lokalen Firewall-Systemadministrator.

Verbinden von ESXi-Hosts über Firewalls

Wenn Sie eine Firewall zwischen Ihren ESXi-Hosts und vCenter Server eingerichtet haben, stellen Sie sicher, dass die verwalteten Hosts Daten empfangen können.

Öffnen Sie zum Konfigurieren einer Verbindung für den Empfang von Daten Ports für den Datenverkehr von Diensten, wie z. B. vSphere High Availability, vMotion und vSphere Fault Tolerance. In Konfigurieren der ESXi Firewall finden Sie eine Erläuterung zu Konfigurationsdateien, vSphere Client-Zugriff und Firewall-Befehlen. Eine Liste der Ports finden Sie im VMware-Tool „Ports und Protokolle“™ unter https://ports.vmware.com.

Firewalls für Konfigurationen ohne vCenter Server

Wenn vCenter Servernicht in Ihrer Umgebung vorhanden ist, können die Clients keine direkte Verbindung zum ESXi-Netzwerk herstellen.

Sie können auf verschiedene Arten eine Verbindung mit einem eigenständigen ESXi-Host herstellen.

- VMware Host Client
- ESXCLI-Schnittstelle
- vSphere Web Services SDK oder vSphere Automation SDKs
- Drittanbieterclients

Die Firewall-Anforderungen für eigenständige Hosts sind mit den Anforderungen vergleichbar, wenn ein vCenter Server vorhanden ist.

- Verwenden Sie eine Firewall, um die ESXi-Ebene oder je nach Konfiguration Ihre Clients und die ESXi-Ebene zu schützen. Diese Firewall bietet einen Grundschutz für das Netzwerk.
- Die Lizenzierung gehört in dieser Konfiguration zu dem ESXi-Paket, das Sie auf allen Hosts installieren. Da die Lizenzierung in ESXi integriert ist, wird ein separater License Server mit einer Firewall nicht benötigt.

Firewallports können mit ESXCLI oder dem VMware Host Client konfiguriert werden. Weitere Informationen hierzu finden Sie unter *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

Herstellen einer Verbindung mit der VM-Konsole über eine Firewall

Bestimmte Ports müssen für die Kommunikation zwischen Administrator bzw. Benutzer und der VM-Konsole geöffnet sein. Welche Ports geöffnet sein müssen, hängt vom Typ der VM-Konsole ab sowie davon, ob Sie die Verbindung über vCenter Server mit dem vSphere Client oder direkt mit dem ESXi-Host vom VMware Host Client aus herstellen.

Weitere Informationen zu Ports, Zweck und Klassifizierung (eingehend, ausgehend oder bidirektional) finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com.

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

Beim Herstellen einer Verbindung mit dem vSphere Client stellen Sie stets eine Verbindung zum vCenter Server-System her, das den ESXi-Host verwaltet, und greifen von hier aus auf die VM-Konsole zu.

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

- Die Firewall muss vSphere Client den Zugriff auf vCenter Server auf Port 443 erlauben.
- Die Firewall muss vCenter Server den Zugriff auf den ESXi-Host auf Port 902 erlauben.

Herstellen der Verbindung zu einer VMware Remote Console über den vSphere Client

Falls Sie vSphere Client verwenden und eine Verbindung zu einer VMware Remote Console (VMRC) herstellen, muss der folgende Zugriff möglich sein:

- Die Firewall muss dem vSphere Client Zugriff auf vCenter Server auf Port 443 gewähren.
- Die Firewall muss dem VMRC Zugriff auf vCenter Server auf Port 443 und auf den ESXi-Host auf Port 902 für VMRC-Versionen vor 11.0 und Port 443 für VMRC Version 11.0 und höher gewähren. Weitere Informationen zu den Portanforderungen von VMRC Version 11.0 und ESXi finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/76672.

Herstellen einer Direktverbindung zu ESXi-Hosts mit dem VMware Host Client

Sie können die VM-Konsole des VMware Host Client verwenden, wenn Sie eine direkte Verbindung zu einem ESXi-Host herstellen.

Hinweis Verwenden Sie den VMware Host Client nicht, um eine Direktverbindung mit Hosts herzustellen, die von einem vCenter Server-System verwaltet werden. Wenn Sie im VMware Host Client an Hosts dieses Typs Änderungen vornehmen, wird Ihre Umgebung instabil.

Die Firewall muss Zugriff auf den ESXi-Host auf Port 443 und 902 gewähren.

Der VMware Host Client verwendet Port 902 für Verbindungen der MKS-Aktivitäten des Gastbetriebssystems auf virtuellen Maschinen. Die Benutzer interagieren über diesen Port mit dem Gastbetriebssystem und den Anwendungen der virtuellen Maschine. Für diese Aufgabe unterstützt VMware nur diesen Port.

Sichern des physischen Switches auf ESXi-Hosts

Sichern Sie den physischen Switch auf jedem ESXi-Host, um zu verhindern, dass Angreifer Zugriff auf den Host und seine virtuellen Maschinen erhalten.

Für optimalen Host-Schutz 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 zu verhindern, dass der physische Switch möglichen DoS-Angriffen (Denial of Service) ausgesetzt ist, können Sie den Gast-BPDU-Filter für ESXi-Hosts aktivieren.
3. Melden Sie sich beim physischen Switch an und stellen Sie sicher, dass Dynamic Trunking Protocol (DTP) nicht für die physischen Switch-Ports aktiviert ist, die mit den ESXi-Hosts verbunden sind.
4. Prüfen Sie physische Switch-Ports routinemäßig, um sicherzustellen, dass sie ordnungsgemäß als Trunk-Ports konfiguriert sind, wenn sie mit VLAN-Trunking-Ports für virtuellen Switch verbunden sind.

Sichern von Standard-Switch-Ports durch Sicherheitsrichtlinien

Die VMkernel-Portgruppe bzw. die VM-Portgruppe auf einem Standard-Switch verfügt über eine konfigurierbare Sicherheitsrichtlinie. Die Sicherheitsrichtlinie bestimmt, wie streng der Schutz gegen Imitations- oder Abfangangriffe auf virtuelle Maschinen sein soll.

Ähnlich wie bei physischen Netzwerkadaptern können VM-Netzwerkadapter die Identität einer anderen virtuellen Maschine annehmen. Die Annahme einer fremden Identität stellt ein Sicherheitsrisiko dar.

- Ein Netzwerkadapter einer virtuellen Maschine kann Datenblöcke übertragen, die von einer anderen virtuellen Maschine zu stammen scheinen, damit er Datenblöcke aus dem Netzwerk empfangen kann, die für die jeweilige virtuelle Maschine bestimmt sind.
- Ein virtueller Netzwerkadapter kann so konfiguriert werden, dass er Datenblöcke empfängt, die für andere Maschinen bestimmt sind.

Wenn Sie eine VMkernel- oder eine VM-Portgruppe zu einem Standard-Switch hinzufügen, konfiguriert ESXi eine Sicherheitsrichtlinie für die Ports in der Gruppe. Mit dieser Sicherheitsrichtlinie können Sie sicherstellen, dass der Host verhindert, dass die Gastbetriebssysteme der virtuellen Maschinen andere Computer im Netzwerk imitieren können. Das Gastbetriebssystem, das die Annahme einer anderen Identität durchführen könnte, erkennt nicht, dass die die Annahme einer fremden Identität verhindert wurde.

Die Sicherheitsrichtlinie bestimmt, wie streng der Schutz gegen Imitations- oder Abfangangriffe auf virtuelle Maschinen sein soll. Weitere Informationen über die ordnungsgemäße Verwendung der Einstellungen im Sicherheitsprofil finden Sie im Abschnitt „Sicherheitsrichtlinie“ des Handbuchs *vSphere-Netzwerk*. In diesem Abschnitt wird Folgendes erläutert:

- Wie VM-Netzwerkadapter Übertragungen steuern.
- Wie auf dieser Ebene Angriffe durchgeführt werden

Sichern von vSphere Standard-Switches

Datenverkehr auf dem Standard-Switch kann vor Ebene 2-Angriffen gesichert werden, indem Sie einige der MAC-Adressmodi der VM-Netzwerkadapter beschränken.

Jeder VM-Netzwerkadapter weist eine ursprüngliche MAC-Adresse und eine geltende MAC-Adresse auf.

Anfängliche 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.

Was geschieht, wenn Sie einen VM-Netzwerkadapter erstellen?

Bei der Erstellung eines VM-Netzwerkadapters stimmen die geltende und die ursprünglich zugewiesene MAC-Adresse überein. Das Gastbetriebssystem kann die geltende MAC-Adresse jedoch jederzeit auf einen anderen Wert setzen. Wenn ein Betriebssystem die geltende MAC-Adresse ändert, empfängt der Netzwerkadapter Netzwerkdatenverkehr, der für die neue MAC-Adresse bestimmt ist.

Beim Versand von Datenpaketen über einen Netzwerkadapter schreibt das Gastbetriebssystem in der Regel die geltende MAC-Adresse des eigenen Netzwerkadapters in das Feld mit der Quell-MAC-Adresse der Ethernet-Frames. Die MAC-Adresse des Empfänger-Netzwerkadapters wird in das Feld mit der Ziel-MAC-Adresse geschrieben. Der empfangende Adapter akzeptiert Datenpakete nur dann, wenn die Ziel-MAC-Adresse im Paket mit seiner eigenen geltenden MAC-Adresse übereinstimmt.

Ein Betriebssystem kann Frames mit einer imitierten Quell-MAC-Adresse senden. Daher kann ein Betriebssystem die Identität eines vom Empfängernetzwerk autorisierten Netzwerkadapters annehmen und böswillige Angriffe auf die Geräte in einem Netzwerk durchführen.

Verwenden von Sicherheitsrichtlinien zum Schutz von Ports und Gruppen

Schützen Sie virtuellen Datenverkehr vor Imitierungs- und Abfangangriffen auf Layer 2, indem Sie eine Sicherheitsrichtlinie für Portgruppen oder Ports konfigurieren.

Die Sicherheitsrichtlinie für verteilte Portgruppen und Ports umfasst die folgenden Optionen:

- MAC-Adressänderungen (siehe MAC-Adressänderungen)
- Promiscuous-Modus (siehe Betrieb im Promiscuous-Modus)
- Gefälschte Übertragungen (siehe Gefälschte Übertragungen)

Sie können die Standardeinstellungen durch Auswählen des mit dem Host verknüpften virtuellen Switches über den vSphere Client anzeigen und ändern. Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

MAC-Adressänderungen

Die Sicherheitsrichtlinie eines virtuellen Switches beinhaltet die Option **MAC-Adressänderungen**. Mit dieser Option können virtuelle Maschinen Frames mit einer MAC-Adresse empfangen, die nicht mit der in der VMX konfigurierten Adresse identisch ist.

Wenn die Option **MAC-Adressänderungen** auf **Akzeptieren** festgelegt ist, akzeptiert ESXi Anforderungen, die geltende MAC-Adresse einer virtuellen Maschine in eine andere als die ursprünglich zugewiesene Adresse zu ändern.

Wenn die Option **MAC-Adressänderungen** auf **Ablehnen** festgelegt ist, lehnt ESXi Anforderungen ab, die geltende MAC-Adresse einer virtuellen Maschine in eine andere als die ursprünglich zugewiesene Adresse zu ändern. Diese Einstellung schützt den Host vor MAC-Imitationen. Der Port, der von dem Adapter der virtuellen Maschine zum Senden der Anforderung verwendet wird, ist deaktiviert, und der Adapter der virtuellen Maschine erhält keine weiteren Frames mehr, bis die geltende MAC-Adresse mit der ursprünglichen MAC-Adresse übereinstimmt. Das Gastbetriebssystem erkennt nicht, dass die Anforderung zum Ändern der MAC-Adresse nicht angenommen wurde.

Hinweis Der iSCSI-Initiator basiert darauf, dass er MAC-Adressänderungen von bestimmten Speichertypen erhalten kann. Wenn Sie ESXi-iSCSI mit iSCSI-Speicher verwenden, legen Sie die Option **MAC-Adressänderungen** auf **Akzeptieren** fest.

In bestimmten Situationen ist es tatsächlich notwendig, dass mehrere Adapter in einem Netzwerk die gleiche MAC-Adresse haben, zum Beispiel wenn Sie den Microsoft-Netzwerk-Lastausgleich im Unicast-Modus verwenden. Bei Verwendung des Microsoft-NetzwerkLastausgleichs im Standard-Multicast-Modus haben die Adapter nicht die gleiche MAC-Adresse.

Hinweis Ab vSphere 7.0 wurden die Standardwerte für **Gefälschte Übertragungen** und **MAC-Adressänderungen** in „Ablehnen“ anstelle von „Akzeptieren“ geändert. Wenden Sie sich an Ihren Speicheranbieter, um dies zu überprüfen.

Gefälschte Übertragungen

Die Option **Gefälschte Übertragungen** beeinflusst den Datenverkehr, der von einer virtuellen Maschine versendet wird.

Wenn die Option **Gefälschte Übertragungen** auf **Akzeptieren** festgelegt ist, vergleicht ESXi die Quell- und die geltende MAC-Adresse nicht.

Zum Schutz gegen MAC-Imitation können Sie die Option **Gefälschte Übertragungen** auf **Ablehnen** einstellen. In diesem Fall vergleicht der Host die Quell-MAC-Adresse, die vom Gastbetriebssystem übertragen wird, mit der geltenden MAC-Adresse für den Adapter der virtuellen Maschine, um festzustellen, ob sie übereinstimmen. Wenn die Adressen nicht übereinstimmen, verwirft der ESXi-Host das Paket.

Das Gastbetriebssystem erkennt nicht, dass der Adapter der virtuellen Maschine die Pakete mit der imitierten MAC-Adresse nicht senden kann. Der ESXi-Host fängt alle Pakete mit imitierten Adressen vor der Übermittlung ab. Das Gastbetriebssystem geht ggf. davon aus, dass die Pakete verworfen wurden.

Hinweis Ab vSphere 7.0 wurden die Standardwerte für **Gefälschte Übertragungen** und **MAC-Adressänderungen** in „Ablehnen“ anstelle von „Akzeptieren“ geändert.

Betrieb im Promiscuous-Modus

Der Promiscuous-Modus deaktiviert jegliche Empfangsfilterung, die der Adapter der virtuellen Maschine ausführt, sodass das Gastbetriebssystem den gesamten Datenverkehr aus dem Netzwerk empfängt. Standardmäßig kann der Adapter der virtuellen Maschine nicht im Promiscuous-Modus betrieben werden.

Der Promiscuous-Modus kann zwar für die Nachverfolgung von Netzwerkaktivitäten nützlich sein, aber er ist ein unsicherer Betriebsmodus, da jeder Adapter im Promiscuous-Modus Zugriff auf alle Pakete hat, selbst wenn manche Pakete nur für einen spezifischen Netzwerkadapter bestimmt sind. Das bedeutet, dass ein Administrator oder Root-Benutzer in einer virtuellen Maschine rein theoretisch den Datenverkehr, der für andere Gast- oder Hostbetriebssysteme bestimmt ist, einsehen kann.

Weitere Informationen zum Konfigurieren des VM-Adapters für den Promiscuous-Modus finden Sie im Thema zur Konfiguration der Sicherheitsrichtlinie für einen vSphere Standard Switch oder eine standardmäßige Portgruppe in der Dokumentation zu *vSphere-Netzwerk*.

Hinweis Unter bestimmten Umständen ist es notwendig, für einen Standard-Switch oder einen verteilten virtuellen Switch den Promiscuous-Modus zu konfigurieren, zum Beispiel wenn Sie eine Software zur Netzwerkeinbruchserkennung oder einen Paket-Sniffer verwenden.

Schutz von Standard-Switches und VLANs

VMware Standard-Switches bieten Schutzmaßnahmen gegen bestimmte Bedrohungen der VLAN-Sicherheit. Aufgrund der Art und Weise, wie Standard-Switches entworfen wurden, schützen sie VLANs vor einer Vielzahl von Angriffen, von denen viele VLAN-Hopping beinhalten.

Dieser Schutz garantiert nicht, dass die Konfiguration Ihrer virtuellen Maschinen gegen andere Arten von Angriffen geschützt ist. Standard-Switches schützen beispielsweise das physische Netzwerk nicht vor diesen Angriffen. Sie schützen nur das virtuelle Netzwerk.

Standard-Switches und VLANs können vor den folgenden Angriffstypen geschützt werden.

Da sich im Laufe der Zeit neue Sicherheitsbedrohungen entwickeln, sollten Sie dies nicht als vollständige Liste von Angriffen betrachten. Überprüfen Sie regelmäßig VMware-Sicherheitsressourcen im Internet, um mehr über Sicherheit, aktuelle Sicherheitswarnungen und VMware-Sicherheitstaktiken zu erfahren.

MAC-Flooding

Beim MAC-Flooding wird ein Switch mit Paketen überflutet, die MAC-Adressen enthalten, die als von verschiedenen Quellen stammend gekennzeichnet sind. Viele Switches verwenden eine Tabelle mit inhaltsadressierbarem Arbeitsspeicher, um die Quelladresse für jedes Paket zu erlernen und zu speichern. Wenn die Tabelle voll ist, kann der Switch in einen vollständig offenen Zustand übergehen, in dem jedes eingehende Paket an alle Ports gesendet wird, sodass der Angreifer den gesamten Datenverkehr des Switches sehen kann. Dieser Zustand kann zu Paketverlusten zwischen VLANs führen.

Obwohl VMware-Standard-Switches eine MAC-Adresstabelle speichern, beziehen sie die MAC-Adressen nicht aus dem beobachtbaren Datenverkehr und sind für diese Art von Angriff nicht anfällig.

802.1q- und ISL-Tagging-Angriffe

802.1q- und ISL-Tagging-Angriffe zwingen einen Switch dazu, Frames von einem VLAN in ein anderes umzuleiten, indem sie den Switch dazu bringen, als Trunk zu fungieren und den Datenverkehr an andere VLANs zu senden.

VMware-Standard-Switches führen das für diese Art von Angriff erforderliche dynamische Trunking nicht durch und sind daher nicht anfällig.

Angriffe mit doppelter Kapselung

Bei Angriffen mit doppelter Kapselung erstellt ein Angreifer ein doppelt gekapseltes Paket, bei dem die VLAN-Kennung im inneren Tag nicht mit der VLAN-Kennung im äußeren Tag übereinstimmt. Aus Gründen der Abwärtskompatibilität wird bei nativen VLANs das äußere Tag aus den übertragenen Paketen entfernt, sofern dies nicht anders konfiguriert ist. Wenn ein nativer VLAN-Switch das äußere Tag entfernt, bleibt nur das innere Tag übrig, und dieses innere Tag leitet das Paket an ein anderes VLAN weiter als das, das im nun fehlenden äußeren Tag angegeben ist.

VMware-Standard-Switches verwerfen alle doppelt gekapselten Frames, die eine virtuelle Maschine an einen Port sendet, der für ein bestimmtes VLAN konfiguriert ist. Daher sind sie nicht anfällig für diese Art von Angriff.

Multicast-Brute-Force-Angriffe

Hierbei wird eine große Anzahl von Multicast-Frames fast gleichzeitig an ein bekanntes VLAN gesendet, um den Switch zu überlasten, sodass er fälschlicherweise zulässt, dass einige der Frames an andere VLANs gesendet werden.

VMware-Standard-Switches lassen nicht zu, dass Frames ihre korrekte Broadcast-Domäne (VLAN) verlassen und sind für diese Art von Angriff nicht anfällig.

Spanning-Tree-Angriffe

Spanning-Tree-Angriffe zielen auf das Spanning-Tree-Protokoll (STP) ab, das zur Steuerung der Überbrückung zwischen Teilen des LAN verwendet wird. Der Angreifer sendet Bridge Protocol Data Unit (BPDU)-Pakete, die versuchen, die Netzwerktopologie zu ändern und sich als Root-Bridge zu etablieren. Als Root-Bridge kann der Angreifer den Inhalt der übertragenen Frames aussengen.

VMware-Standard-Switches unterstützen STP nicht und sind für diese Art von Angriffen nicht anfällig.

Zufällige Frame-Angriffe

Bei zufälligen Frame-Angriffen wird eine große Anzahl von Paketen gesendet, bei denen die Quell- und Zieladressen gleich bleiben, aber die Länge, der Typ oder der Inhalt der Felder zufällig geändert werden. Ziel dieses Angriffs ist es, zu erzwingen, dass Pakete fälschlicherweise an ein anderes VLAN umgeleitet werden.

VMware-Standard-Switches sind für diese Art von Angriff nicht anfällig.

Sichern von vSphere Distributed Switches und verteilten Portgruppen

Die Administratoren haben mehrere Optionen zum Sichern von vSphere Distributed Switches in ihrer vSphere-Umgebung.

Für VLANs in einem vSphere Distributed Switch gelten dieselben Regeln wie in einem Standard-Switch. Weitere Informationen finden Sie unter Schutz von Standard-Switches und VLANs.

Verfahren

1. Deaktivieren Sie für verteilte Portgruppen mit statischer Bindung die Funktion zum automatischen Erweitern.

   Die Funktion zum automatischen Erweitern ist standardmäßig aktiviert.

   Um die automatische Erweiterung zu deaktivieren, konfigurieren Sie die Eigenschaft `autoExpand` unter der verteilten Portgruppe mit dem vSphere Web Services SDK oder über eine Befehlszeilenschnittstelle. Siehe die Dokumentation zu *vSphere Web Services SDK*.
2. Stellen Sie sicher, dass alle privaten VLAN IDs aller vSphere Distributed Switches vollständig dokumentiert sind.
3. Bei Verwendung von VLAN-Tagging in einer dvPortgroup müssen die VLAN-IDs mit denen der externen VLAN-fähigen Upstream-Switches übereinstimmen. Wenn die VLAN-IDs nicht ordnungsgemäß aufgezeichnet werden, kann die versehentliche Wiederverwendung von IDs zu unbeabsichtigtem Datenverkehr führen. Ebenso kann bei fehlenden oder falschen VLAN-IDs der Datenverkehr zwischen physischen und virtuellen Maschinen blockiert werden.
4. Stellen Sie sicher, dass in einer virtuellen Portgruppe, die einem vSphere Distributed Switch zugeordnet ist, keine nicht verwendeten Ports vorhanden sind.
5. Kennzeichnen Sie alle vSphere Distributed Switches.

   Für mit einem ESXi-Host verknüpfte vSphere Distributed Switches ist ein Textfeld für den Namen des Switches erforderlich. Diese Bezeichnung dient als funktionaler Deskriptor für den Switch, genauso wie der mit einem physischen Switch verknüpfte Hostname. Die Bezeichnung am vSphere Distributed Switch zeigt die Funktion oder das IP-Subnetz des Switches an. Sie können zum Beispiel den Switch als intern bezeichnen, um anzugeben, dass er nur für interne Netzwerke auf dem privaten virtuellen Switch einer virtuellen Maschine dient. Über physikalische Netzwerkadapter erfolgt kein Datenverkehr.

6 Deaktivieren Sie die Netzwerk-Systemstatusprüfung für Ihre vSphere Distributed Switches, wenn Sie sie nicht regelmäßig verwenden.

   Die Netzwerk-Systemstatusprüfung ist standardmäßig deaktiviert. Nach der Aktivierung enthalten die Systemstatusprüfungspakete Informationen zum Host, Switch und Port, die ein Angreifer möglicherweise verwenden kann. Verwenden Sie die Netzwerk-Systemstatusprüfung nur zur Fehlerbehebung und deaktivieren Sie sie nach Abschluss der Fehlerbehebung.

7 Schützen Sie virtuellen Datenverkehr vor Imitierungs- und Abfangangriffen auf Layer 2, indem Sie eine Sicherheitsrichtlinie für Portgruppen oder Ports konfigurieren.

   Die Sicherheitsrichtlinie für verteilte Portgruppen und Ports umfasst die folgenden Optionen:

   - MAC-Adressänderungen (siehe MAC-Adressänderungen)
   - Promiscuous-Modus (siehe Betrieb im Promiscuous-Modus)
   - Gefälschte Übertragungen (siehe Gefälschte Übertragungen)

   Durch Auswahl von **Verteilte Portgruppen verwalten** im Kontextmenü des Distributed Switch und Klicken auf **Sicherheit** im Assistenten können Sie die aktuellen Einstellungen einsehen und ändern. Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

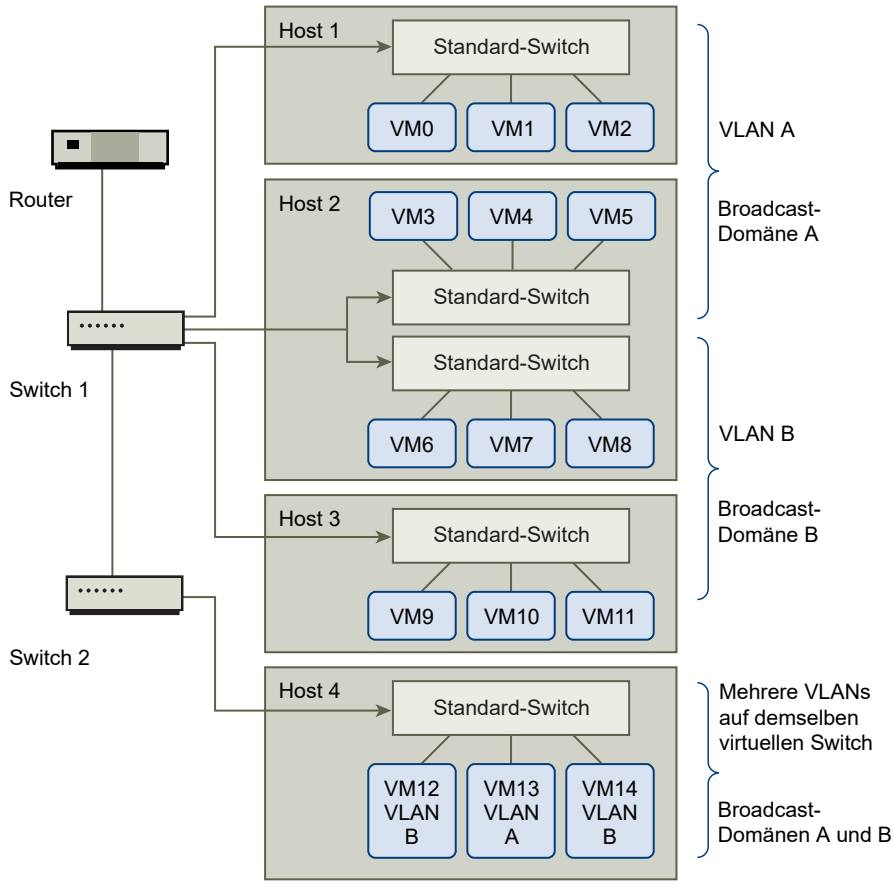
Absichern virtueller Maschinen durch VLANs

Das Netzwerk gehört zu den gefährdetsten Teilen eines jeden Systems. Ihre VM-Netzwerk muss genauso wie ihr physisches Netzwerk geschützt werden. Durch die Verwendung von VLANs kann die Sicherheit des Netzwerks in Ihrer Umgebung verbessert werden.

VLANs sind eine Netzwerkarchitektur nach dem IEEE-Standard und verfügen über spezifische Kennzeichnungsmethoden, durch die Datenpakete nur an die Ports weitergeleitet werden, die zum VLAN gehören. Wenn das VLAN ordnungsgemäß konfiguriert ist, ist es ein zuverlässiges Mittel zum Schutz einer Gruppe virtueller Maschinen vor zufälligem und böswilligem Eindringen.

Mit VLANs können Sie ein physisches Netzwerk so in Segmente aufteilen, dass zwei Computer oder virtuelle Maschinen im Netzwerk nur dann Pakete untereinander austauschen können, wenn sie zum gleichen VLAN gehören. So gehören zum Beispiel Buchhaltungsunterlagen und -transaktionen zu den wichtigsten vertraulichen internen Informationen eines Unternehmens. Wenn in einem Unternehmen die virtuellen Maschinen der Verkaufs-, Logistik- und Buchhaltungsmitarbeiter an das gleiche physische Netzwerk angeschlossen sind, können Sie die virtuellen Maschinen für die Buchhaltungsabteilung schützen, indem Sie VLANs einrichten.

Abbildung 13-1. Beispielplan eines VLAN



Bei dieser Konfiguration verwenden alle Mitarbeiter der Buchhaltungsabteilung virtuelle Maschinen im VLAN A, die Mitarbeiter der Vertriebsabteilung verwenden die virtuellen Maschinen im VLAN B.

Der Router leitet die Datenpakete mit Buchhaltungsdaten an die Switches weiter. Diese Pakete sind so gekennzeichnet, dass sie nur an VLAN A weitergeleitet werden dürfen. Daher sind die Daten auf die Broadcast-Domäne A beschränkt und können nur an die Broadcast-Domäne B weitergeleitet werden, wenn der Router entsprechend konfiguriert wurde.

Bei dieser VLAN-Konfiguration wird verhindert, dass Mitarbeiter des Vertriebs Datenpakete abfangen können, die für die Buchhaltungsabteilung bestimmt sind. Die Buchhaltungsabteilung kann zudem auch keine Datenpakete empfangen, die für den Vertrieb bestimmt sind. Virtuelle Maschinen, die an einen gemeinsamen virtuellen Switch angebunden sind, können sich dennoch in unterschiedlichen VLANs befinden.

Sicherheitsempfehlungen für VLANs

Wie Sie die VLANs einrichten, um Teile eines Netzwerks abzusichern, hängt von Faktoren wie dem Gastbetriebssystem und der Konfiguration der Netzwerkgeräte ab.

ESXi ist mit einer vollständigen VLAN-Implementierung nach IEEE 802.1q ausgestattet. Zwar kann VMware keine spezifischen Empfehlungen aussprechen, wie die VLANs eingerichtet werden sollten, es sollten jedoch bestimmte Faktoren berücksichtigt werden, wenn ein VLAN ein Bestandteil Ihrer Sicherheitsrichtlinien ist.

Sichern von VLANs

Administratoren haben mehrere Möglichkeiten, um die VLANs in ihrer vSphere-Umgebung zu sichern.

Verfahren

1. Stellen Sie sicher, dass für Portgruppen keine VLAN-Werte konfiguriert sind, die für physische Upstream-Switches reserviert sind.

   Legen Sie für VLAN-IDs keine Werte fest, die für den physischen Switch reserviert sind.

2. Stellen Sie sicher, dass für Portgruppen nicht VLAN 4095 konfiguriert ist, außer Sie verwenden Virtual Guest Tagging (VGT).

   In vSphere gibt es drei Arten von VLAN-Tagging:

   - External Switch Tagging (EST)
   - Virtual Switch Tagging (VST): Der virtuelle Switch kennzeichnet mit der konfigurierten VLAN-ID den eingehenden Datenverkehr für die angefügten virtuellen Maschinen und entfernt das VLAN-Tag im ausgehenden Datenverkehr. Zum Einrichten des VST-Modus weisen Sie eine VLAN-ID zwischen 1 und 4094 zu.
   - Virtual Guest Tagging (VGT): VLANs werden von virtuellen Maschinen abgewickelt. Zum Aktivieren des VGT-Modus legen Sie 4095 als VLAN-ID fest. Auf einem Distributed Switch können Sie mithilfe der Option **VLAN-Trunking** auch Datenverkehr der virtuellen Maschine basierend auf dem VLAN zulassen.

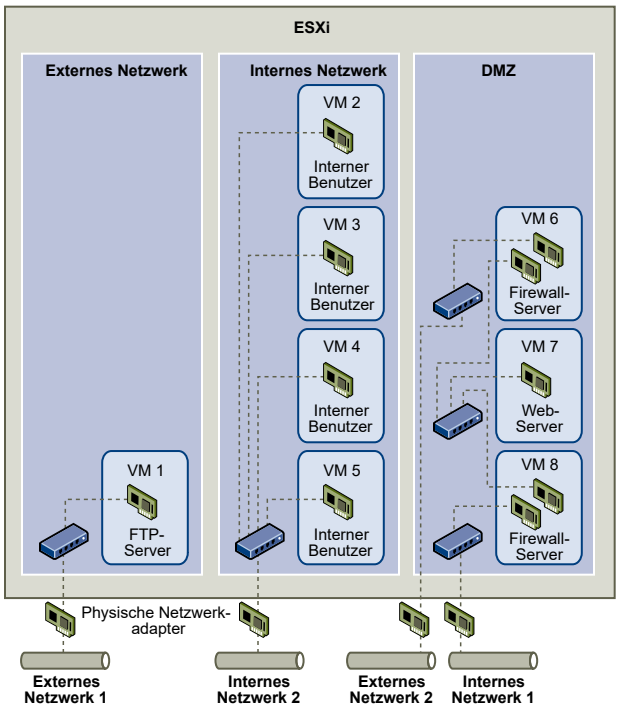
   Auf einem Standard-Switch können Sie den VLAN-Netzwerkmodus auf Switch- oder Portgruppenebene konfigurieren, und auf einem Distributed Switch auf der Ebene der verteilten Portgruppe oder des Ports.

3. Stellen Sie sicher, dass alle VLANs auf jedem virtuellen Switch vollständig dokumentiert sind und dass jeder virtuelle Switch alle erforderlichen VLANs und nur die erforderlichen VLANs aufweist.

Erstellen mehrerer Netzwerke auf einem einzelnen ESXi-Host

Das ESXi-System wurde so entworfen, dass Sie bestimmte Gruppen virtueller Maschinen an das interne Netzwerk, andere an das externe Netzwerk und wiederum andere an beide Netzwerke anbinden können - alle auf demselben Host. Diese Fähigkeit basiert auf der grundlegenden Isolierung virtueller Maschinen im Zusammenspiel mit der überlegt geplanten Nutzung von Funktionen zur virtuellen Vernetzung.

Abbildung 13-2. Konfigurierte externe Netzwerke, interne Netzwerke und DMZ auf einem ESXi-Host



In der Abbildung hat der Systemadministrator einen Host in drei verschiedene VM-Zonen unterteilt: FTP-Server, interne virtuelle Maschinen und DMZ. Jede Zone erfüllt eine bestimmte Funktion.

FTP-Serverzone

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 Netzwerkzone

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-Zone

Die virtuellen Maschinen 6 bis 8 wurden als DMZ konfiguriert, die von der Marketingabteilung dazu verwendet wird, die externe Website des Unternehmens bereitzustellen.

Diese VM-Gruppe ist dem externen Netzwerk 2 und dem internen Netzwerk 1 zugeordnet. Das Unternehmen nutzt das externe Netzwerk 2 zur Unterstützung der Webserver, die von der Marketing- und der Finanzabteilung zur Bereitstellung der Unternehmenswebsite und anderer webbasierter Anwendungen für externe Benutzer verwendet werden. Das interne Netzwerk 1 ist der Verbindungskanal, den die Marketingabteilung zur Veröffentlichung ihrer Inhalte auf der Unternehmenswebsite, zur Bereitstellung von Downloads und Diensten wie Benutzerforen verwendet.

Da diese Netzwerke vom externen Netzwerk 1 und vom internen Netzwerk 2 getrennt sind und die virtuellen Maschinen keine gemeinsamen Kontaktpunkte (Switches oder Adapter) aufweisen, besteht kein Angriffsrisiko für den FTP-Server oder die Gruppe interner virtueller Maschinen (weder als Ausgangspunkt noch als Ziel).

Vorteile der Verwendung von VM-Zonen

Wenn die Isolierung der virtuellen Maschinen genau beachtet wird, die virtuellen Switches ordnungsgemäß konfiguriert werden und die Netzwerktrennung eingehalten wird, können Sie alle drei Zonen der virtuellen Maschinen auf dem gleichen ESXi-Host unterbringen, ohne dass Datenverluste oder Ressourcenmissbräuche befürchtet werden müssen.

Das Unternehmen erzwingt die Isolierung der virtuellen Maschinengruppen durch die Verwendung mehrerer interner und externer Netzwerke und die Sicherstellung, dass die virtuellen Switches und physischen Netzwerkadapter jeder Gruppe von denen anderer Gruppen getrennt sind.

Da keiner der virtuellen Switches sich über mehrere Zonen erstreckt, können Sie das Risiko des Durchsickerns von Daten von einer Zone in eine andere ausschalten. Ein virtueller Switch kann aufbaubedingt keine Datenpakete direkt an einen anderen virtuellen Switch weitergeben. Datenpakete können nur unter folgenden Umständen von einem virtuellen Switch zu einem anderen gelangen:

- Wenn die virtuellen Switches an das gleiche physische LAN angeschlossen sind
- Wenn die virtuellen Switches an eine gemeinsame virtuelle Maschine angeschlossen sind, die unter Umständen zum Übertragen von Datenpaketen verwendet werden kann

In der Beispielkonfiguration wird keine dieser Bedingungen erfüllt. Wenn Sie sicherstellen möchten, dass es keine gemeinsamen virtuellen Switch-Pfade gibt, können Sie mögliche gemeinsame Kontaktpunkte suchen, indem Sie den Netzwerk-Switch-Plan im vSphere Client überprüfen.

Um die VM-Ressourcen zu schützen, konfigurieren Sie eine Ressourcenreservierung und einen Grenzwert für jede virtuelle Maschine, wodurch das Risiko von DoS- und DDoS-Angriffen verringert wird. Sie können den ESXi-Host und die virtuellen Maschinen weiter schützen, indem Sie Software-Firewalls am Front- und Back-End der DMZ installieren. Stellen Sie schließlich sicher, dass sich der Host hinter einer physischen Firewall befindet, und konfigurieren Sie die Netzwerkspeicherressourcen so, dass jede über einen eigenen virtuellen Switch verfügt.

Verwenden von Internet Protocol Security auf ESXi-Hosts

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 ESXi-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 den 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 auf ESXi-Hosts

ESXi kann eine Liste aller Sicherheitsverbindungen zur Verfügung stellen, die zur Verwendung durch Sicherheitsrichtlinien verfügbar sind. Die Liste enthält sowohl die vom Benutzer erstellten Sicherheitsverbindungen als auch die Sicherheitsverbindungen, die der VMkernel mithilfe von Internet Key Exchange installiert hat.

Sie können mithilfe des Befehls `esxcli` eine Liste der verfügbaren Sicherheitsverbindungen abrufen.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **`esxcli network ip ipsec sa list`** ein.

Ergebnisse

ESXi zeigt eine Liste aller verfügbaren Sicherheitsverbindungen an.

Hinzufügen einer IPsec-Sicherheitsverbindung zu einem ESXi-Host

Fügen Sie eine Sicherheitsverbindung hinzu, um Verschlüsselungsparameter für den zugeordneten IP-Datenverkehr festzulegen.

Sie können eine Sicherheitsverbindung mithilfe des Befehls `esxcli` hinzufügen.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **`esxcli network ip ipsec sa add`** zusammen mit einer oder mehreren der nachfolgenden Optionen ein.

Option	Beschreibung
`--sa-source=` ***Quelladresse***	Erforderlich. Geben Sie die Quelladresse an.
`--sa-destination=` ***Zieladresse***	Erforderlich. Geben Sie die Zieladresse an.
`--sa-mode=` ***Modus***	Erforderlich. Geben Sie als Modus entweder `transport` oder `tunnel` an.
`--sa-spi=` ***Sicherheitsparameter-Index***	Erforderlich. Geben Sie den Sicherheitsparameter-Index an. Der Sicherheitsparameter-Index identifiziert die Sicherheitsverbindung dem Host gegenüber. Er muss eine Hexadezimalzahl mit dem Präfix 0x sein. Jede von Ihnen erstellte Sicherheitsverbindung muss eine eindeutige Kombination aus Protokoll und Sicherheitsparameter-Index besitzen.
`--encryption-algorithm=` ***Verschlüsselungsalgorithmus***	Erforderlich. Verwenden Sie einen der folgenden Parameter, um den Verschlüsselungsalgorithmus anzugeben. ■ `3des-cbc` ■ `aes128-cbc` ■ `null` (bietet keine Verschlüsselung)
`--encryption-key=` ***Verschlüsselungsschlüssel***	Erforderlich, wenn Sie einen Verschlüsselungsalgorithmus angeben. Geben Sie den Verschlüsselungsschlüssel an. Sie können Schlüssel als ASCII-Text oder als Hexadezimalzahl mit dem Präfix 0x eingeben.
`--integrity-algorithm=` ***Authentifizierungsalgorithmus***	Erforderlich. Geben Sie den Authentifizierungsalgorithmus an: `hmac-sha1` oder `hmac-sha2-256`.
`--integrity-key=` ***Authentifizierungsschlüssel***	Erforderlich. Geben Sie den Authentifizierungsschlüssel an. Sie können Schlüssel als ASCII-Text oder als Hexadezimalzahl mit dem Präfix 0x eingeben.
`--sa-name=`***Name***	Erforderlich. Geben Sie einen Namen für die Sicherheitsverbindung an.

Beispiel: Befehl für eine neue Sicherheitsverbindung

Im folgenden Beispiel wurden Zeilenumbrüche hinzugefügt, um die Lesbarkeit zu verbessern.

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x697076367265616479 6c6f676f3364657363362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x69707636726561647 96c6f67736861316f757432
--sa-name sa1
```

Entfernen einer IPsec-Sicherheitsverbindung auf einem ESXi-Host

Sie können eine Sicherheitsverbindung mithilfe des ESXCLI-Befehls entfernen.

Voraussetzungen

Stellen Sie sicher, dass die gewünschte Sicherheitsverbindung zurzeit nicht verwendet wird. Wenn Sie versuchen, eine Sicherheitsverbindung zu entfernen, die gerade verwendet wird, schlägt der Entfernungsvorgang fehl.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **`esxcli network ip ipsec sa remove --sa-name`** ***`security_association_name`*** ein.

Auflisten der verfügbaren IPsec-Sicherheitsrichtlinien auf einem ESXi-Host

Die verfügbaren Sicherheitsrichtlinien können Sie mit dem Befehl ESXCLI auflisten.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **`esxcli network ip ipsec sp list`** ein.

Ergebnisse

Der Host zeigt eine Liste aller verfügbaren Sicherheitsrichtlinien an.

Erstellen einer IPSec-Sicherheitsrichtlinie auf einem ESXi-Host

Erstellen Sie eine Sicherheitsrichtlinie, um festzulegen, wann die in einer Sicherheitsverbindung angegebenen Authentifizierungs- und Verschlüsselungsparameter verwendet werden sollen. Sie können eine Sicherheitsrichtlinie mithilfe des ESXCLI-Befehls hinzufügen.

Voraussetzungen

Fügen Sie vor dem Erstellen einer Sicherheitsrichtlinie eine Sicherheitsverbindung mit den entsprechenden Authentifizierungs- und Verschlüsselungsparametern hinzu, wie unter Hinzufügen einer IPsec-Sicherheitsverbindung zu einem ESXi-Host beschrieben.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **`esxcli network ip ipsec sp add`** zusammen mit einer oder mehreren der nachfolgenden Optionen ein.

Option	Beschreibung
`--sp-source=` ***Quelladresse***	Erforderlich. Geben Sie Quell-IP-Adresse und die Präfixlänge an.
`--sp-destination=` ***Zieladresse***	Erforderlich. Geben Sie Zieladresse und die Präfixlänge an.
`--source-port=` ***Port***	Erforderlich. Geben Sie den Quellport an. Der Quellport muss eine Zahl zwischen 0 und 65535 sein.
`--destination-port=` ***Port***	Erforderlich. Geben Sie den Zielport an. Der Quellport muss eine Zahl zwischen 0 und 65535 sein.
`--upper-layer-protocol=` ***Protokoll***	Verwenden Sie einen der folgenden Parameter, um das Protokoll für höhere Schichten anzugeben. ■ `tcp` ■ `udp` ■ `icmp6` ■ `any`
`--flow-direction=` ***Richtung***	Wählen Sie als Richtung, in der Sie den Datenverkehr überwachen möchten, entweder `in` oder `out` aus.
`--action=` ***Aktion***	Geben Sie mithilfe eines der folgenden Parameters die Aktion an, die ausgeführt werden soll, wenn auf Datenverkehr mit den angegebenen Parametern gestoßen wird. ■ `none`: Keine Aktion ausführen. ■ `discard`: Keinen ein- oder ausgehenden Datenverkehr zulassen. ■ `ipsec`: Die in der Sicherheitsverbindung angegebenen Authentifizierungs- und Verschlüsselungsinformationen verwenden, um zu ermitteln, ob die Daten aus einer vertrauenswürdigen Quelle stammen.
`--sp-mode=` ***Modus***	Geben Sie als Modus entweder `tunnel` oder `transport` an.
`--sa-name=` ***Name der Sicherheitsverbindung***	Erforderlich. Geben Sie den Namen der Sicherheitsverbindung an, die die Sicherheitsrichtlinie verwenden soll.
`--sp-name=` ***Name***	Erforderlich. Geben Sie einen Namen für die Sicherheitsrichtlinie an.

Beispiel: Befehl für eine neue Sicherheitsrichtlinie

Im folgenden Beispiel wurden Zeilenumbrüche hinzugefügt, um die Lesbarkeit zu verbessern.

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
```

```
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sa1
--sp-name=sp1
```

Entfernen einer IPsec-Sicherheitsrichtlinie auf einem ESXi-Host

Sie können eine Sicherheitsrichtlinie mithilfe des ESXCLI-Befehls vom ESXi-Host entfernen.

Voraussetzungen

Stellen Sie sicher, dass die gewünschte Sicherheitsrichtlinie zurzeit nicht verwendet wird. Wenn Sie versuchen, eine Sicherheitsrichtlinie zu entfernen, die gerade verwendet wird, schlägt der Entfernungsvorgang fehl.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **`esxcli network ip ipsec sp remove --sa-name`** ***`Name der Sicherheitsrichtlinie`*** ein.

  Um alle Sicherheitsrichtlinien zu entfernen, geben Sie den Befehl **`esxcli network ip ipsec sp remove --remove-all`** ein.

Sicherstellen der ordnungsgemäßen SNMP-Konfiguration auf ESXi-Hosts

Wenn SNMP nicht ordnungsgemäß konfiguriert ist, können Überwachungsinformationen an einen bösartigen Host gesendet werden. Der bösartige Host kann dann mithilfe dieser Informationen einen Angriff planen.

ESXi enthält einen SNMP-Agenten, der Benachrichtigungen (Traps und Informs) senden und `GET`-, `GETBULK`- und `GETNEXT`-Anforderungen empfangen kann. SNMP ist standardmäßig nicht aktiviert. SNMP muss auf jedem ESXi-Host konfiguriert werden. Für die Konfiguration können Sie ESXCLI, PowerCLI oder das vSphere Web Services SDK verwenden.

Detaillierte Informationen zum Konfigurieren von SNMP, einschließlich SNMP v3, finden Sie in der Dokumentation *vSphere-Überwachung und -Leistung*. SNMP v3 bietet eine höhere Sicherheit als SNMP v1 und SNMP v2c, einschließlich der Schlüsselauthentifizierung und -verschlüsselung. Unter *ESXCLI – Referenz* finden Sie weitere Informationen zu den `esxcli system snmp`-Befehlsoptionen.

Verfahren

1 Führen Sie den folgenden Befehl aus, um festzustellen, ob SNMP verwendet wird.

  ```
  esxcli system snmp get
  ```

2 Führen Sie zum Aktivieren von SNMP den folgenden Befehl aus.

```
esxcli system snmp set --enable true
```

3 Führen Sie folgenden Befehl aus, um SNMP zu deaktivieren.

```
esxcli system snmp set --enable false
```

vSphere Networking, empfohlene Vorgehensweisen für die Sicherheit

Die Einhaltung der Best Practices für die Netzwerksicherheit dient der Integritätswahrung Ihrer vSphere-Bereitstellung.

Allgemeine Empfehlungen für die vSphere-Netzwerksicherheit

Das Befolgen allgemeiner Netzwerksicherheitsempfehlungen ist der erste Schritt zum Absichern Ihrer vSphere-Netzwerkumgebung. Anschließend können Sie sich spezielle Bereiche vornehmen, wie Absichern des Netzwerks mit Firewalls oder Verwendung von IPsec.

Empfehlungen zum Sichern einer vSphere-Netzwerkumgebung

- Das Spanning-Tree-Protokoll (STP) erkennt und verhindert die Bildung von Schleifen in der Netzwerktopologie. Virtuelle VMware-Switches verhindern Schleifen anderweitig, bieten aber keine direkte Unterstützung für STP. Wenn sich die Netzwerktopologie ändert, dauert es zwischen 30 und 50 Sekunden, bis das Netzwerk die Topologie erneut erlernt. Während dieser Zeit darf kein Datenverkehr übertragen werden. Zur Vermeidung dieser Probleme haben Netzwerkanbieter Funktionen zum Aktivieren von Switch-Ports erstellt, die die Weiterleitung des Datenverkehrs fortsetzen. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/1003804. In der Dokumentation des Netzwerkanbieters finden Sie Informationen zu geeigneten Konfigurationen für das Netzwerk und die Netzwerkhardware.
- Stellen Sie sicher, dass Netflow-Daten für einen verteilten virtuellen Switch nur an autorisierte Collector-IP-Adressen gesendet werden. Netflow-Exporte werden nicht verschlüsselt und können Informationen über das virtuelle Netzwerk enthalten. Diese vertraulichen Informationen können unter Umständen während der Übertragung von Angreifern angezeigt und erfasst werden. Wenn ein Netflow-Export erforderlich ist, prüfen Sie, ob alle Netflow-Ziel-IP-Adressen korrekt sind.
- Stellen Sie mithilfe der rollenbasierten Zugriffssteuerung sicher, dass nur autorisierte Administratoren Zugriff auf virtuelle Netzwerkkomponenten haben. Geben Sie beispielsweise Administratoren virtueller Maschinen nur Zugriff auf Portgruppen, in denen sich ihre virtuellen Maschinen befinden. Geben Sie Netzwerkadministratoren Berechtigungen für alle virtuellen Netzwerkkomponenten, aber keinen Zugriff auf virtuelle Maschinen. Durch Beschränkung des Zugriffs verringert sich das Risiko einer Fehlkonfiguration, sei es zufällig oder absichtlich, und wichtige Sicherheitskonzepte der Trennung der Verantwortlichkeiten und der geringsten Berechtigung werden in Kraft gesetzt.

- Stellen Sie sicher, dass für Portgruppen nicht der Wert des nativen VLAN konfiguriert ist. Physische Switches werden häufig mit einem nativen VLAN konfiguriert, bei dem es sich standardmäßig um VLAN 1 handelt. ESXi verfügt nicht über ein natives VLAN. Frames, für die das VLAN in der Portgruppe angegeben ist, weisen ein Tag auf, aber Frames, für die kein VLAN in der Portgruppe angegeben ist, werden nicht gekennzeichnet. Dies kann zu Problemen führen, da mit „1“ gekennzeichnete virtuelle Maschinen am Ende zum nativen VLAN des physischen Switches gehören.

  Beispielsweise werden Frames in VLAN 1 von einem physischen Cisco-Switch nicht gekennzeichnet, da VLAN1 das native VLAN auf diesem physischen Switch ist. Frames vom ESXi-Host, die als VLAN 1 festgelegt sind, werden jedoch mit einer „1“ gekennzeichnet. Das führt dazu, dass für das native VLAN bestimmter Datenverkehr vom ESXi-Host nicht korrekt weitergeleitet wird, da er mit einer „1“ gekennzeichnet ist, statt keine Kennzeichnung aufzuweisen. Datenverkehr vom physischen Switch, der vom nativen VLAN stammt, ist nicht sichtbar, da er nicht gekennzeichnet ist. Wenn die ESXi-Portgruppe für den virtuellen Switch die native VLAN-ID verwendet, ist Datenverkehr von virtuellen Maschinen auf diesem Port nicht für das native VLAN auf dem Switch sichtbar, da der Switch nicht gekennzeichneten Datenverkehr erwartet.
- Stellen Sie sicher, dass für Portgruppen keine VLAN-Werte konfiguriert sind, die für physische Upstream-Switches reserviert sind. Physische Switches reservieren bestimmte VLAN-IDs zu internen Zwecken und erlauben mit diesen Werten konfigurierten Datenverkehr in vielen Fällen nicht. Beispielsweise reservieren Cisco Catalyst-Switches in der Regel die VLANs 1001 bis 1024 und 4094. Die Verwendung eines reservierten VLAN kann einen Denial-of-Service-Fehler im Netzwerk verursachen.
- Stellen Sie sicher, dass für Portgruppen nicht VLAN 4095 konfiguriert ist, außer für Virtual Guest Tagging (VGT). Durch Festlegen von VLAN 4095 für eine Portgruppe wird der VGT-Modus aktiviert. In diesem Modus übermittelt der virtuelle Switch alle Netzwerk-Frames an die virtuelle Maschine, ohne die VLAN-Tags zu ändern, und überlässt deren Verarbeitung der virtuellen Maschine.
- Beschränken Sie Außerkraftsetzungen für die Konfiguration auf Portebene auf einem verteilten virtuellen Switch. Außerkraftsetzungen für die Konfiguration auf Portebene sind standardmäßig deaktiviert. Bei aktivierten Außerkraftsetzungen können Sie andere Sicherheitseinstellungen für eine virtuelle Maschine verwenden als die Einstellungen auf Portgruppenebene. Für bestimmte virtuelle Maschinen sind andere Konfigurationen erforderlich. Dies muss jedoch unbedingt überwacht werden. Wenn Außerkraftsetzungen nicht überwacht werden, kann jeder, der sich Zugriff auf eine virtuelle Maschine mit einer weniger sicheren Konfiguration für den virtuellen Switch verschafft, diese Sicherheitslücke auszunutzen versuchen.
- Stellen Sie sicher, dass gespiegelter Verkehr auf einem Port des verteilten virtuellen Switches nur an autorisierte Collector-Ports oder VLANs gesendet wird. Ein vSphere Distributed Switch kann Datenverkehr zwischen Ports spiegeln, damit Paketerfassungsgeräte bestimmte Verkehrsflussdaten erfassen können. Bei der Portspiegelung wird eine Kopie des gesamten angegebenen Datenverkehrs in unverschlüsseltem Format gesendet. Dieser gespiegelte

Datenverkehr enthält die kompletten Daten in den erfassten Paketen und kann, wenn er an das falsche Ziel weitergeleitet wird, ein Datenleck verursachen. Wenn Portspiegelung erforderlich ist, sollten Sie sicherstellen, dass alle Ziel-VLAN-, Port- und Uplink-IDs der Portspiegelung richtig sind.

Bezeichnungen von vSphere-Netzwerkkomponenten

Das Identifizieren der unterschiedlichen Komponenten Ihrer vSphere-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 sind. Diese Bezeichnungen dienen als funktionale Deskriptoren für die Portgruppen und helfen Ihnen dabei, die Funktion jeder Portgruppe zu identifizieren, wenn das Netzwerk komplexer wird.
- Stellen Sie sicher, dass jeder vSphere Distributed Switch über eine eindeutige Netzwerkbezeichnung verfügt, die die Funktion oder das IP-Subnetz des Switches angibt. Diese Bezeichnung dient als funktionaler Deskriptor für den Switch, genauso wie physische Switches einen Hostnamen erfordern. Sie können den Switch beispielsweise als intern bezeichnen, um darauf hinzuweisen, dass er für interne Netzwerke dient. Sie können die Bezeichnung für einen virtuellen Standard-Switch nicht ändern.

Dokumentieren und Überprüfen der vSphere-VLAN-Umgebung

Überprüfen Sie Ihre VLAN-Umgebung regelmäßig, um Probleme zu vermeiden. Dokumentieren Sie Ihre vSphere-VLAN-Umgebung umfassend und stellen Sie sicher, dass VLAN-IDs nur einmal verwendet werden. Ihre Dokumentation kann bei der Fehlerbehebung helfen und spielt bei der Erweiterung Ihrer Umgebung eine wichtige Rolle.

Verfahren

1 Vollständige Dokumentation aller vSphere- und VLAN-IDs

   Bei Verwendung von VLAN-Tagging auf virtuellen Switches müssen die IDs mit denen der externen VLAN-fähigen Upstream-Switches übereinstimmen. Wenn die VLAN-IDs nicht vollständig nachverfolgbar sind, kann es zu Wiederverwendung von IDs kommen und damit zu Datenverkehr zwischen den falschen physischen und virtuellen Maschinen. Ebenso kann bei fehlenden oder falschen VLAN-IDs der Datenverkehr zwischen physischen und virtuellen Maschinen an unerwünschten Stellen blockiert werden.

2 Sorgen Sie für eine vollständige Dokumentation der VLAN-IDs von allen verteilten virtuellen Portgruppen (dvPortgroup-Instanzen).

   Bei Verwendung von VLAN-Tagging in einer dvPortgroup müssen die IDs mit denen der externen VLAN-fähigen Upstream-Switches übereinstimmen. Wenn die VLAN-IDs nicht

vollständig nachverfolgbar sind, kann es zu Wiederverwendung von IDs kommen und damit zu Datenverkehr zwischen den falschen physischen und virtuellen Maschinen. Ebenso kann bei fehlenden oder falschen VLAN-IDs der Datenverkehr zwischen physischen und virtuellen Maschinen an unerwünschten Stellen blockiert werden.

3 Sorgen Sie für eine vollständige Dokumentation der VLAN-IDs von allen verteilten virtuellen Switches.

   Private VLANs (PVLANs) für verteilte virtuelle Switches erfordern primäre und sekundäre VLAN-IDs. Diese IDs müssen mit denen der externen PVLAN-fähigen Upstream-Switches übereinstimmen. Wenn die VLAN-IDs nicht vollständig nachverfolgbar sind, kann es zu Wiederverwendung von IDs kommen und damit zu Datenverkehr zwischen den falschen physischen und virtuellen Maschinen. Ebenso kann bei fehlenden oder falschen PVLAN-IDs der Datenverkehr zwischen physischen und virtuellen Maschinen an unerwünschten Stellen blockiert werden.

4 Stellen Sie sicher, dass VLAN-Trunk-Links nur mit physischen Switch-Ports verbunden sind, die als Trunk-Links agieren.

   Beim Verbinden eines virtuellen Switches mit einem VLAN-Trunk-Port müssen Sie sowohl den virtuellen Switch als auch den physischen Switch am Uplink-Port ordnungsgemäß konfigurieren. Wenn der physische Switch nicht ordnungsgemäß konfiguriert ist, werden Frames mit dem VLAN 802.1q-Header an einen Switch weitergeleitet, der diese Frames nicht erwartet.

Einführung von Netzwerkisolierungspraktiken in vSphere

Mit Netzwerkisolierungspraktiken können Sie die Netzwerksicherheit in der vSphere-Umgebung erhöhen.

Isolieren des vSphere-Verwaltungsnetzwerks

Das vSphere-Verwaltungsnetzwerk bietet Zugriff auf die vSphere-Verwaltungsschnittstelle der einzelnen Komponenten. Die Dienste, die auf der Verwaltungsschnittstelle ausgeführt werden, bieten Angreifern die Chance, sich privilegierten Zugriff auf die Systeme zu verschaffen. Die Wahrscheinlichkeit ist hoch, dass Remoteangriffe mit der Verschaffung von Zugriff auf dieses Netzwerk beginnen. Wenn ein Angreifer sich Zugriff auf das Verwaltungsnetzwerk verschafft, hat er eine gute Ausgangsposition für ein weiteres Eindringen.

Kontrollieren Sie den Zugriff auf das Verwaltungsnetzwerk streng, indem Sie es mit der Sicherheitsebene der sichersten VM, die auf einem ESXi-Host oder -Cluster ausgeführt wird, schützen. Unabhängig davon, wie stark das Verwaltungsnetzwerk eingeschränkt ist, benötigen Administratoren Zugriff auf dieses Netzwerk, um die ESXi-Hosts und das vCenter Server-System zu konfigurieren.

Platzieren Sie die vSphere-Verwaltungsportgruppe in einem dedizierten VLAN auf einem üblichen Standard-Switch. Der Produktionsdatenverkehr (VM) kann den Standard-Switch freigeben, wenn das VLAN der vSphere-Verwaltungsportgruppe nicht von Produktions-VMs verwendet wird.

Überprüfen Sie, ob das Netzwerksegment nicht geroutet ist, mit Ausnahme von Netzwerken, in denen andere verwaltungsrelevante Elemente gefunden wurden. Das Routing eines Netzwerksegments kann für vSphere Replication sinnvoll sein. Stellen Sie insbesondere sicher, dass der Datenverkehr der Produktions-VM nicht zu diesem Netzwerk geroutet werden kann.

Kontrollieren Sie den Zugriff auf Verwaltungsfunktionen mithilfe eines der folgenden Ansätze streng.

- Konfigurieren Sie für den Zugriff auf das Verwaltungsnetzwerk in besonders vertraulichen Umgebungen ein kontrolliertes Gateway oder eine andere Kontrollmethode. Legen Sie beispielsweise fest, dass Administratoren eine Verbindung zum Verwaltungsnetzwerk über ein VPN herstellen müssen. Gestatten Sie den Zugriff auf das Verwaltungsnetzwerk nur vertrauenswürdigen Administratoren.
- Konfigurieren Sie Bastionhosts, die Verwaltungsclients ausführen.

Isolieren von Speicherdatenverkehr

Stellen Sie sicher, dass der IP-basierte Speicherdatenverkehr isoliert ist. IP-basierter Speicher umfasst iSCSI und NFS. 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. Jeder Benutzer mit Zugriff auf dieses Netzwerk kann IP-basierten Speicherdatenverkehr anzeigen. Um zu verhindern, dass unautorisierte Benutzer den IP-basierten Speicherdatenverkehr anzeigen, trennen Sie den IP-basierten Speicher-Netzwerkdatenverkehr logisch vom Produktionsdatenverkehr. Konfigurieren Sie die IP-basierten Speicheradapter auf getrennten VLANs oder Netzwerksegmenten im VMkernel-Verwaltungsnetzwerk, um zu verhindern, dass unautorisierte Benutzer den Datenverkehr einsehen.

Isolieren von vMotion-Datenverkehr

vMotion-Migrationsinformationen werden als einfacher Text übermittelt. Jeder Benutzer mit Zugriff auf das Netzwerk, über das diese Informationen fließen, kann sie anzeigen. Potenzielle Angreifer können vMotion-Datenverkehr abfangen, um an die Speicherinhalte einer VM zu gelangen. Sie können auch einen MITM-Angriff durchführen, bei dem die Inhalte während der Migration geändert werden.

Trennen Sie den vMotion-Datenverkehr vom Produktionsdatenverkehr in einem isolierten Netzwerk. Richten Sie das Netzwerk so ein, dass es nicht routing-fähig ist. Stellen Sie also sicher, dass kein Layer 3-Router dieses und andere Netzwerke umfasst, um Fremdzugriff auf das Netzwerk zu verhindern.

Verwenden Sie ein dediziertes VLAN auf einem üblichen Standard-Switch für die vMotion-Portgruppe. Der Produktionsdatenverkehr (VM) kann den gleichen Standard-Switch nutzen, wenn das VLAN der vMotion-Portgruppe VLAN nicht von Produktions-VMs verwendet wird.

Isolieren von vSAN-Datenverkehr

Isolieren Sie bei der Konfiguration Ihres vSAN-Netzwerks den vSAN-Datenverkehr in einem eigenen Schicht-2-Netzwerksegment. Sie können diesen Vorgang mithilfe von dedizierten Switches oder Ports oder mithilfe eines VLAN durchführen.

Bedarfsgerechtes Verwenden von virtuellen Switches mit der vSphere Network Appliance-API

Konfigurieren Sie den Host nicht zum Senden von Netzwerkinformationen an eine virtuelle Maschine, es sei denn, Sie verwenden Produkte, die die vSphere Network Appliance API (DvFilter) nutzen. Wenn die vSphere Network Appliance API aktiviert ist, kann ein Angreifer versuchen, eine virtuelle Maschine mit dem Filter zu verbinden. Diese Verbindung kann Zugriff auf das Netzwerk anderer virtueller Maschinen auf dem Host bereitstellen.

Wenn Sie ein Produkt verwenden, das diese API nutzt, überprüfen Sie, ob der Host ordnungsgemäß konfiguriert ist. Informationen finden Sie in den Abschnitten zu DvFilter in der Dokumentation *Entwickeln und Bereitstellen von vSphere-Lösungen, vServices und ESX-Agenten*. Wenn Ihr Host zum Verwenden der API eingerichtet ist, stellen Sie sicher, dass der Wert des Parameters `Net.DVFilterBindIpAddress` dem Produkt entspricht, das die API verwendet.

Verfahren

1. Navigieren Sie zum Host im Navigator von vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
4. Führen Sie einen Bildlauf nach unten zu `Net.DVFilterBindIpAddress` aus und überprüfen Sie, ob der Parameter einen leeren Wert aufweist.

   Die Reihenfolge der Parameter ist nicht streng alphabetisch. Geben Sie **`DVFilter`** in das Textfeld „Filter“ ein, um alle zugehörigen Parameter anzuzeigen.
5. Überprüfen Sie die Einstellung.
   - Wenn Sie die DvFilter-Einstellungen nicht verwenden, stellen Sie sicher, dass der Wert leer ist.
   - Wenn Sie die DvFilter-Einstellungen nicht verwenden, stellen Sie sicher, dass der Parameterwert richtig ist. Der Wert muss mit dem Wert übereinstimmen, den das Produkt, das den DvFilter verwendet, verwendet.

Empfohlene Vorgehensweisen für mehrere vSphere-Komponenten 14

Einige empfohlene Vorgehensweisen für die Sicherheit, wie das Einrichten von PTP oder NTP in Ihrer Umgebung, wirken sich auf mehr als eine vSphere-Komponente aus. Berücksichtigen Sie diese Empfehlungen beim Konfigurieren Ihrer Umgebung.

Weitere Informationen hierzu finden Sie unter Kapitel 3 Sichern der ESXi-Hosts und Kapitel 5 Sichern von virtuellen Maschinen.

Lesen Sie als Nächstes die folgenden Themen:

- Synchronisieren der Systemuhren im vSphere-Netzwerk
- Speichersicherheit, empfohlene Vorgehensweisen
- Überprüfen, ob das Senden von Hostleistungsdaten an Gastbetriebssysteme deaktiviert ist
- Einstellen von Zeitüberschreitungen für die ESXi Shell und den vSphere Client

Synchronisieren der Systemuhren im vSphere-Netzwerk

Stellen Sie sicher, dass auf allen Komponenten im vSphere-Netzwerk die Systemuhren synchronisiert sind. Wenn die Systemuhren auf den physischen Maschinen in Ihrem vSphere-Netzwerk nicht synchronisiert sind, werden SSL-Zertifikate und SAML-Token, die zeitabhängig sind, bei der Kommunikation zwischen Netzwerkmaschinen möglicherweise nicht als gültig erkannt.

Nicht synchronisierte Systemuhren können Authentifizierungsprobleme verursachen, was zu einer fehlgeschlagenen Installation führen bzw. verhindern kann, dass der `vmware-vpxd`-Dienst der vCenter Server gestartet wird.

Zeitinkonsistenzen in vSphere können bei verschiedenen Diensten zu einem Fehlschlagen des ersten Starts einer Komponente in Ihrer Umgebung führen, je nachdem, wo in der Umgebung die Zeit nicht korrekt ist und wann sie synchronisiert wird. Probleme treten am häufigsten auf, wenn der ESXi-Zielhost für den Ziel-vCenter Server nicht mit NTP oder PTP synchronisiert ist. Ebenso können Probleme auftreten, wenn die Ziel-vCenter Server zu einem ESXi-Host migriert wird, der aufgrund des vollautomatisierten DRS auf eine andere Zeit festgelegt ist.

Um Probleme mit der Zeitsynchronisierung zu verhindern, stellen Sie sicher, dass die folgenden Angaben korrekt sind, bevor Sie eine vCenter Server-Instanz installieren, migrieren oder aktualisieren.

- Der ESXi-Zielhost, auf dem der Ziel-vCenter Server bereitgestellt werden soll, ist mit NTP oder PTP synchronisiert.
- Der ESXi-Host, auf dem der Quell-vCenter Server ausgeführt wird, ist mit NTP oder PTP synchronisiert.
- Wenn die vCenter Server Appliance mit einem externen Platform Services Controller verbunden ist, stellen Sie beim Aktualisieren oder Migrieren von vSphere 6.7 auf vSphere 8.0 sicher, dass der ESXi-Host, der den externen Platform Services Controller ausführt, mit NTP oder PTP synchronisiert ist.
- Stellen Sie beim Upgraden oder Migrieren von vSphere 6.7 auf vSphere 8.0 sicher, dass der Quell-vCenter Server oder die vCenter Server Appliance und der externe Platform Services Controller die richtige Uhrzeit aufweisen.

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

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

Informationen zum Ändern der Einstellungen der Uhrzeitsynchronisierung für vCenter Server finden Sie unter *Konfigurieren der Systemzeitzone und Zeitsynchronisierungseinstellungen* in der Dokumentation *vCenter Server-Konfiguration*.

Eine Anleitung zum Bearbeiten der Uhrzeitkonfiguration für einen Host mithilfe des vSphere Client finden Sie unter *Bearbeiten der Uhrzeitkonfiguration für einen Host* in der Dokumentation *vCenter Server- und Hostverwaltung*.

Weitere Themen zum Lesen

- Synchronisieren der ESXi-Systemuhren mit einem NTP-Server

  Stellen Sie vor der Installation von vCenter Server sicher, dass auf allen Maschinen im vSphere-Netzwerk die Systemuhren synchronisiert sind.
- Konfigurieren der Einstellungen für die Uhrzeitsynchronisierung in vCenter Server

  Sie können die Einstellungen für die Uhrzeitsynchronisierung in vCenter Server nach der Bereitstellung ändern.

Synchronisieren der ESXi-Systemuhren mit einem NTP-Server

Stellen Sie vor der Installation von vCenter Server sicher, dass auf allen Maschinen im vSphere-Netzwerk die Systemuhren synchronisiert sind.

Diese Aufgabe erläutert, wie Sie NTP über den VMware Host Client einrichten.

Verfahren

1. Starten Sie den VMware Host Client und stellen Sie eine Verbindung mit dem ESXi-Host her.
2. Klicken Sie auf **Verwalten**.
3. Klicken Sie unter **System** auf **Datum und Uhrzeit** und anschließend auf **Einstellungen bearbeiten**.
4. Wählen Sie **NTP (Network Time Protocol) verwenden (NTP-Client aktivieren)** aus.
5. Geben Sie im Textfeld „NTP-Server“ die IP-Adresse oder den vollqualifizierten Domänennamen mindestens eines NTP-Servers ein, der synchronisiert werden soll.
6. Wählen Sie im Dropdown-Menü **Startrichtlinie für NTP-Dienst** die Option **Mit dem Host starten und beenden** aus.
7. Klicken Sie auf **Speichern**.

   Der Host wird mit dem NTP-Server synchronisiert.

Konfigurieren der Einstellungen für die Uhrzeitsynchronisierung in vCenter Server

Sie können die Einstellungen für die Uhrzeitsynchronisierung in vCenter Server nach der Bereitstellung ändern.

Wenn Sie vCenter Server bereitstellen, können Sie für die Uhrzeitsynchronisierung entweder einen NTP-Server oder VMware Tools auswählen. Wenn sich die Uhrzeiteinstellungen in Ihrem vSphere-Netzwerk ändern, können Sie vCenter Server bearbeiten und die Uhrzeitsynchronisierungseinstellungen anhand der Befehle in der Appliance-Shell konfigurieren.

Wenn Sie die regelmäßige Uhrzeitsynchronisierung aktivieren, legt VMware Tools die Uhrzeit des Gastbetriebssystems auf die Uhrzeit des Hostcomputers fest.

Nach der Uhrzeitsynchronisierung prüft VMware Tools minütlich, ob die Uhrzeit auf dem Gastbetriebssystem mit der Uhrzeit auf dem Host übereinstimmt. Ist dies nicht der Fall, wird die Uhrzeit auf dem Gastbetriebssystem wieder mit der Uhrzeit auf dem Host synchronisiert.

Native Uhrzeitsynchronisierungssoftware wie Network Time Protocol (NTP) ist normalerweise genauer als die regelmäßige Uhrzeitsynchronisierung von VMware Tools und daher vorzuziehen. Sie können nur eine Form der regelmäßigen Uhrzeitsynchronisierung in vCenter Server verwenden. Wenn Sie sich für die native Uhrzeitsynchronisierungssoftware entscheiden, wird die regelmäßige Uhrzeitsynchronisierung durch VMware Tools für vCenter Server deaktiviert.

Verwenden der Uhrzeitsynchronisierung von VMware Tools

Sie können vCenter Server für die Verwendung der Uhrzeitsynchronisierung von VMware Tools einrichten.

Verfahren

1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

2 Führen Sie den Befehl aus, um auf VMware Tools basierte Uhrzeitsynchronisierung zu aktivieren.

```
timesync.set --mode host
```

3 (Optional) Führen Sie den Befehl aus, um zu überprüfen, ob Sie die Uhrzeitsynchronisierung von VMware Tools erfolgreich angewendet haben.

```
timesync.get
```

Der Befehl gibt zurück, dass sich die Uhrzeitsynchronisierung im Host-Modus befindet.

Ergebnisse

Die Uhrzeit der Appliance wird mit der Uhrzeit des ESXi-Hosts synchronisiert.

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

Wenn Sie die vCenter Server für die Verwendung der NTP-basierten Uhrzeitsynchronisierung einrichten möchten, müssen Sie zuerst die NTP-Server zur vCenter Server-Konfiguration hinzufügen.

Verfahren

1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

2 Fügen Sie der vCenter Server-Konfiguration NTP-Server hinzu, indem Sie den folgenden `ntp.set`-Befehl ausführen.

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

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

Dieser Befehl entfernt die aktuellen NTP-Server (sofern vorhanden) und fügt der Konfiguration die neuen NTP-Server hinzu. Wenn die Uhrzeitsynchronisierung auf einem NTP-Server basiert, wird der NTP-Daemon neu gestartet, um die neuen NTP-Server erneut zu laden. Andernfalls ersetzt dieser Befehl die aktuellen NTP-Server in der NTP-Konfiguration durch die neuen NTP-Server, die Sie angeben.

3 (Optional) Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Sie die neuen NTP-Konfigurationseinstellungen erfolgreich angewendet haben.

```
ntp.get
```

Der Befehl gibt eine durch Leerzeichen getrennte Liste der Server zurück, die für die NTP-Synchronisierung konfiguriert sind. Bei aktivierter NTP-Synchronisierung gibt der Befehl zurück, dass die NTP-Konfiguration den Status „Erreichbar“ aufweist. Falls die NTP-Synchronisierung deaktiviert ist, gibt der Befehl zurück, dass die NTP-Konfiguration den Status „Ausgefallen“ aufweist.

4 (Optional) Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der NTP-Server erreichbar ist.

```
ntp.test --servers IP-addresses-or-host-names
```

Der Befehl gibt den Status der NTP-Server zurück.

Nächste Schritte

Falls die NTP-Synchronisierung deaktiviert ist, können Sie die Zeitsynchronisierungseinstellungen in vCenter Server so konfigurieren, dass sie auf einem NTP-Server basieren. Weitere Informationen hierzu finden Sie unter Synchronisieren der Uhrzeit in vCenter Server mit einem NTP-Server.

Synchronisieren der Uhrzeit in vCenter Server mit einem NTP-Server

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

Voraussetzungen

Richten Sie in der vCenter Server-Konfiguration mindestens einen NTP-Server (Network Time Protocol) ein. Weitere Informationen hierzu finden Sie unter Hinzufügen oder Ersetzen von NTP-Servern in der vCenter Server-Konfiguration.

Verfahren

1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

2 Führen Sie den Befehl aus, um NTP-basierte Uhrzeitsynchronisierung zu aktivieren.

```
timesync.set --mode NTP
```

3 (Optional) Führen Sie den Befehl aus, um zu überprüfen, ob Sie die NTP-Synchronisierung erfolgreich angewendet haben.

```
timesync.get
```

Der Befehl gibt zurück, dass sich die Uhrzeitsynchronisierung im NTP-Modus befindet.

Speichersicherheit, empfohlene Vorgehensweisen

Befolgen Sie die von Ihrem Speicheranbieter empfohlenen Vorgehensweisen für die Speichersicherheit. Sie können auch CHAP und beiderseitiges CHAP nutzen, um iSCSI-Speicher zu sichern, SAN-Ressourcen zu maskieren und in Zonen einzuteilen und die Kerberos-Anmeldedaten für NFS 4.1 zu konfigurieren.

Weitere Informationen finden Sie in der Dokumentation zu *Verwalten von VMware vSAN*.

Absichern von iSCSI-Speicher

Der Speicher, den Sie für einen Host konfigurieren, kann ein oder mehrere SANs (Speichernetzwerke) umfassen, die iSCSI verwenden. Wenn Sie iSCSI auf einem Host konfigurieren, können Sie Maßnahmen ergreifen, um Sicherheitsrisiken zu minimieren.

iSCSI ermöglicht den Zugriff auf SCSI-Geräte und den Austausch von Datensätzen durch die Nutzung von TCP/IP über einen Netzwerkport und nicht über einen direkten Anschluss an einem SCSI-Gerät. Eine iSCSI-Transaktion fasst Blöcke von rohen SCSI-Daten in iSCSI-Datensätzen zusammen und überträgt die Daten an das anfordernde Gerät bzw. den Benutzer.

iSCSI SANs unterstützen die effiziente Nutzung der bestehenden Ethernet-Infrastruktur, um Hosts den Zugriff auf Speicherressourcen zu gewähren, die sie dynamisch freigeben können. iSCSI SANs sind eine kostengünstige Speicherlösung für Umgebungen, die auf einen gemeinsamen Speicherpool angewiesen sind, um viele Benutzer zu bedienen. Wie in allen vernetzten Systemen sind auch iSCSI-SANs anfällig für Sicherheitsverletzungen.

Hinweis Die Anforderungen und Vorgehensweisen für die Absicherung von iSCSI-SANs ähneln denen für Hardware-iSCSI-Adapter, die Hosts zugewiesen sind, sowie für iSCSI, die direkt über den Host konfiguriert werden.

Schützen von iSCSI-Geräten

Um iSCSI-Geräte zu schützen, stellen Sie sicher, dass sich der ESXi-Host bzw. der Initiator beim iSCSI-Gerät bzw. dem Ziel authentifizieren kann, wenn der Host versucht, auf Daten auf der Ziel-LUN zuzugreifen.

Die Authentifizierung stellt sicher, dass der Initiator das Recht hat, auf ein Ziel zuzugreifen. Sie gewähren dieses Recht, wenn Sie auf dem iSCSI-Gerät die Authentifizierung konfigurieren.

ESXi unterstützt für iSCSI weder Secure Remote Protocol (SRP) noch Authentifizierungsverfahren mit öffentlichen Schlüsseln. Sie können Kerberos nur mit NFS 4.1 verwenden.

ESXi unterstützt sowohl CHAP-Authentifizierung als auch beiderseitige CHAP-Authentifizierung. In der Dokumentation *vSphere-Speicher* wird erläutert, wie Sie die beste Authentifizierungsmethode für Ihr iSCSI-Gerät auswählen und CHAP einrichten.

Stellen Sie die Eindeutigkeit Ihrer CHAP-Geheimnisse sicher. Legen Sie ein anderes gegenseitiges Authentifizierungskennwort für jeden Host fest. Wenn möglich, legen Sie für jeden Client jeweils ein Kennwort fest, das sich vom Kennwort des ESXi-Hosts unterscheidet. Eindeutige Kennwörter stellen sicher, dass bei Manipulation eines bestimmten Hosts ein Angreifer nicht einen beliebigen anderen Host erstellen und sich beim Speichergerät authentifizieren kann. Mit einem einzelnen gemeinsamen geheimen Schlüssel kann sich ein Angreifer durch die Manipulation eines Hosts möglicherweise beim Speichergerät authentifizieren.

Schützen eines iSCSI-SAN

Bei der Planung der iSCSI-Konfiguration sollten Sie Maßnahmen zur Verbesserung der allgemeinen Sicherheit des iSCSI-SAN ergreifen. Die iSCSI-Konfiguration ist nur so sicher wie das IP-Netzwerk. Wenn Sie also hohe Sicherheitsstandards bei der Netzwerkeinrichtung befolgen, schützen Sie auch den iSCSI-Speicher.

Nachfolgend sind einige spezifische Vorschläge zum Umsetzen hoher Sicherheitsstandards aufgeführt.

Schützen übertragener Daten

Eines der Hauptrisiken bei iSCSI-SANs ist, dass der Angreifer übertragene Speicherdaten mitschneiden kann.

Ergreifen Sie zusätzliche Maßnahmen, um zu verhindern, dass Angreifer iSCSI-Daten sehen können. Weder der Hardware-iSCSI-Adapter noch der ESXi-iSCSI-Initiator verschlüsseln Daten, die zu und von den Zielen übertragen werden. Dies macht die Daten anfälliger für Sniffing-Angriffe.

Wenn die virtuellen Maschinen die gleichen Standard-Switches und VLANs wie die iSCSI-Struktur verwenden, ist der iSCSI-Datenverkehr potenziell dem Missbrauch durch Angreifer der virtuellen Maschinen ausgesetzt. Um sicherzustellen, dass Angreifer die iSCSI-Übertragungen nicht überwachen können, achten Sie darauf, dass keine Ihrer virtuellen Maschinen das iSCSI-Speichernetzwerk sehen kann.

Wenn Sie einen Hardware-iSCSI-Adapter verwenden, erreichen Sie dies, indem Sie sicherstellen, dass der iSCSI-Adapter und der physische Netzwerkadapter von ESXi nicht versehentlich außerhalb des Hosts durch eine gemeinsame Verwendung des Switches oder in anderer Form verbunden sind. Wenn Sie iSCSI direkt über den ESXi-Host konfigurieren, können Sie dies erreichen, indem Sie den iSCSI-Speicher über einen anderen Standard-Switch konfigurieren als denjenigen, der durch Ihre virtuellen Maschinen verwendet wird.

Zusätzlich zum Schutz durch einen eigenen Standard-Switch können Sie das iSCSI-SAN durch die Konfiguration eines eigenen VLAN für das iSCSI-SAN schützen, um Leistung und Sicherheit zu verbessern. Wenn die iSCSI-Konfiguration sich in einem eigenen VLAN befindet, wird sichergestellt, dass keine Geräte außer dem iSCSI-Adapter Einblick in Übertragungen im iSCSI-SAN haben. Auch eine Netzwerküberlastung durch andere Quellen kann den iSCSI-Datenverkehr nicht beeinträchtigen.

Sichern der iSCSI-Ports

Wenn Sie die iSCSI-Geräte ausführen, öffnet ESXi keine Ports, die Netzwerkverbindungen überwachen. Durch diese Maßnahme wird die Chance, dass ein Angreifer über ungenutzte Ports in ESXi eindringen und Kontrolle über ihn erlangen kann, reduziert. Daher stellt der Betrieb von iSCSI kein zusätzliches Sicherheitsrisiko für das ESXi-Ende der Verbindung dar.

Beachten Sie, dass auf jedem iSCSI-Zielgerät mindestens ein freigegebener TCP-Port für iSCSI-Verbindungen vorhanden sein muss. Wenn es Sicherheitsprobleme in der Software des iSCSI-Geräts gibt, können die Daten unabhängig von ESXi in Gefahr sein. Installieren Sie alle Sicherheitspatches des Speicherherstellers und beschränken Sie die Anzahl der an das iSCSI-Netzwerk angeschlossenen Geräte, um dieses Risiko zu verringern.

Maskieren von SAN-Ressourcen und Einteilen derselben in Zonen

Sie können Zoneneinteilung und LUN-Maskierung verwenden, um SAN-Aktivitäten zu trennen und den Zugriff auf Speichergeräte zu beschränken.

Sie können den Zugriff auf Speicher in Ihrer vSphere-Umgebung schützen, indem Sie Zoneneinteilung und LUN-Maskierung für Ihre SAN-Ressourcen verwenden. Sie können zum Beispiel Zonen, die zum Testen definiert sind, unabhängig innerhalb des SAN verwalten, damit sie nicht mit der Aktivität in den Produktionszonen in Konflikt geraten. Ebenso können Sie verschiedene Zonen für verschiedene Abteilungen einrichten.

Berücksichtigen Sie beim Einrichten von Zonen etwaige Hostgruppen, die auf dem SAN-Gerät eingerichtet sind.

Zoneneinteilungs- und Maskierungsfunktionen für die einzelnen SAN-Switches und Festplatten-Arrays sowie die Tools für die LUN-Maskierung sind anbieterspezifisch.

Weitere Informationen finden Sie in der Dokumentation Ihres SAN-Anbieters und in der Dokumentation zu *vSphere-Speicher*.

Verwenden von Kerberos für NFS 4.1

Mit NFS-Version 4.1 unterstützt ESXi den Kerberos-Authentifizierungsmechanismus.

Beim RPCSEC_GSS-Kerberos-Mechanismus handelt es sich um einen Authentifizierungsdienst. Mit diesem Dienst kann ein auf ESXi installierter NFS 4.1-Client vor dem Mounten einer NFS-Freigabe seine Identität bei einem NFS-Server nachweisen. Die Kerberos-Sicherheit verwendet Verschlüsselung beim Einsatz in einer ungesicherten Netzwerkverbindung.

Die ESXi-Implementierung von Kerberos für NFS 4.1 weist die beiden Sicherheitsmodelle krb5 und krb5i auf, die ein unterschiedliches Sicherheitsniveau bieten.

- Kerberos nur für Authentifizierung (krb5) unterstützt die Identitätsprüfung.
- Kerberos für Authentifizierung und Datenintegrität (krb5i) bietet neben der Identitätsprüfung auch Datenintegritätsdienste. Mit diesen Diensten kann NFS-Datenverkehr vor Manipulation geschützt werden, indem Datenpakete auf potenzielle Modifikationen überprüft werden.

Kerberos unterstützt Verschlüsselungsalgorithmen, die nicht autorisierte Benutzer daran hindern, auf NFS-Datenverkehr zuzugreifen. Der NFS 4.1-Client in ESXi versucht, mithilfe des Algorithmus AES256-CTS-HMAC-SHA1-96 oder AES128-CTS-HMAC-SHA1-96 auf eine Freigabe auf dem NAS-Server zuzugreifen. Stellen Sie vor der Verwendung Ihrer NFS 4.1-Datenspeicher sicher, dass AES256-CTS-HMAC-SHA1-96 oder AES128-CTS-HMAC-SHA1-96 auf dem NAS-Server aktiviert ist.

In der folgenden Tabelle werden die von ESXi unterstützten Kerberos-Sicherheitsstufen verglichen.

Tabelle 14-1. Kerberos-Sicherheitstypen

		ESXi 6.0	ESXi 6.5 und höher
Kerberos nur für Authentifizierung (krb5)	Integritätsprüfsumme für RPC-Header	Ja mit DES	Ja mit AES
	Integritätsprüfsumme für RPC-Daten	Nein	Nein
Kerberos für Authentifizierung und Datenintegrität (krb5i)	Integritätsprüfsumme für RPC-Header	Kein krb5i	Ja mit AES
	Integritätsprüfsumme für RPC-Daten		Ja mit AES

Wenn Sie die Kerberos-Authentifizierung verwenden, ist Folgendes zu beachten:

- ESXi verwendet Kerberos zusammen mit der Active Directory-Domäne.
- Als vSphere-Administrator geben Sie Active Directory-Anmeldedaten an, um einem NFS-Benutzer Zugriff auf NFS 4.1-Kerberos-Datenspeicher zu erteilen. Ein einzelner Anmeldedatensatz wird zum Zugriff auf alle Kerberos-Datenspeicher, die auf diesem Host gemountet sind, verwendet.
- Wenn mehrere ESXi-Hosts den NFS 4.1-Datenspeicher gemeinsam nutzen, müssen Sie dieselben Active Directory-Anmeldedaten für alle Hosts verwenden, die auf den gemeinsam genutzten Datenspeicher zugreifen. Um den Zuweisungsvorgang zu automatisieren, legen Sie den Benutzer in Hostprofilen fest und wenden das Profil auf alle ESXi-Hosts an.
- Es ist nicht möglich, zwei Sicherheitsmechanismen (AUTH_SYS und Kerberos) für denselben NFS 4.1-Datenspeicher zu verwenden, der von mehreren Hosts gemeinsam genutzt wird.

Eine schrittweise Anleitung finden Sie in der Dokumentation *vSphere-Speicher*.

Überprüfen, ob das Senden von Hostleistungsdaten an Gastbetriebssysteme deaktiviert ist

vSphere umfasst Leistungsindikatoren für virtuelle Maschinen auf Windows-Betriebssystemen, bei denen VMware Tools installiert ist. Leistungsindikatoren ermöglichen den Besitzern virtueller Maschinen eine exakte Leistungsanalyse innerhalb des Gastbetriebssystems. Standardmäßig legt vSphere gegenüber der virtuellen Gastmaschine keine Hostinformationen offen.

Standardmäßig ist die Funktion zum Senden von Hostleistungsdaten an eine virtuelle Maschine deaktiviert. Durch diese Standardeinstellung wird verhindert, dass eine virtuelle Maschine detaillierte Informationen über den physischen Host erhält. Tritt ein Sicherheitsverstoß im Zusammenhang mit der virtuellen Maschine auf, werden durch die Einstellung dem Angreifer keine Hostdaten zur Verfügung gestellt.

Hinweis Die grundlegende Vorgehensweise wird im Folgenden beschrieben. Verwenden Sie die ESXCLI- oder VMware PowerCLI-Befehle, um diese Aufgabe auf allen Hosts gleichzeitig auszuführen.

Verfahren

1. Navigieren Sie auf dem ESXi-System, das die virtuelle Maschine hostet, zur VMX-Datei.

   Die Konfigurationsdateien der virtuellen Maschinen befinden sich im Verzeichnis `/vmfs/volumes/`*`Datenspeicher`*, wobei es sich bei *Datenspeicher* um den Namen des Speichergeräts handelt, auf dem die Dateien der virtuellen Maschine gespeichert sind.

2. Stellen Sie sicher, dass in der VMX-Datei der folgende Parameter gesetzt ist.

   ```
   tools.guestlib.enableHostInfo=FALSE
   ```

3. Speichern und schließen Sie die Datei.

Ergebnisse

Von der virtuellen Gastmaschine aus können keine Leistungsinformationen abgerufen werden.

Einstellen von Zeitüberschreitungen für die ESXi Shell und den vSphere Client

Um zu verhindern, dass Angreifer eine Sitzung im Leerlauf verwenden können, legen Sie Zeitüberschreitungen für die ESXi Shell und den vSphere Client fest.

Zeitüberschreitung für ESXi Shell

Für ESXi Shell können Sie die folgenden Zeitüberschreitungen über den vSphere Client oder über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) festlegen.

Verfügbarkeits-Zeitüberschreitung

Der Zeitüberschreitungswert für die Verfügbarkeit gibt die Zeitspanne an, während der Sie sich nach der Aktivierung der ESXi Shell anmelden müssen. Nach Ablauf dieser Zeitspanne wird der Dienst deaktiviert und die Benutzer können sich nicht mehr anmelden.

Leerlauf-Zeitüberschreitung

Der Zeitüberschreitungswert für die Leerlaufzeit gibt die Zeitspanne an, die verstreichen darf, bis Sie bei interaktiven Sitzungen, die sich im Leerlauf befinden, abgemeldet werden. Änderungen an den Zeitüberschreitungswerten für die Leerlaufzeit werden erst wirksam, wenn sich ein Benutzer das nächste Mal bei der ESXi Shell anmeldet. Änderungen wirken sich nicht auf vorhandene Sitzungen aus.

Ändern der vSphere Client-Zeitüberschreitung

vSphere Client-Sitzungen werden standardmäßig nach 120 Minuten beendet. So ändern Sie die Standardeinstellungen:

1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.

2 Wählen Sie die Registerkarte **Konfigurieren** und unter **Einstellungen** die Option **Allgemein** aus.

3 Klicken Sie auf **Bearbeiten**.

4 Wählen Sie **Zeitüberschreitungseinstellungen**.

5 Geben Sie die gewünschten Einstellungen ein und klicken Sie auf **Speichern**.

vSphere-TLS-Konfiguration

15

Ab 8.0 Update 3 unterstützt vSphere TLS 1.3 und 1.2 über die Verwendung von TLS-Profilen. TLS-Profile vereinfachen die Verwaltung von TLS-Parametern und verbessern außerdem die Unterstützbarkeit.

vSphere 8.0 Update 3 aktiviert das TLS-Standardprofil COMPATIBLE auf ESXi- und vCenter Server-Hosts. Das COMPATIBLE-Profil unterstützt TLS 1.3- und einige TLS 1.2-Verbindungen.

Sie können TLS-Profile auf ESXi-Hosts entweder mithilfe von vSphere Configuration Profiles- oder `esxcli`-Befehlen verwalten. Auf vCenter Server-Hosts können Sie TLS-Profile mithilfe von APIs verwalten. Beispielsweise können Sie Developer Center im vSphere Client verwenden. Weitere Informationen finden Sie im *Programmierhandbuch zu den vSphere Automation SDKs* und im *Programmierhandbuch zur vSphere Automation REST API*.

vCenter Server und Envoy

vCenter Server führt zwei Reverse-Proxy-Dienste aus:

- VMware-Reverse-Proxy-Dienst, `rhttpproxy`
- Envoy

Bei Envoy handelt es sich um einen Edge- und Dienst-Proxy, der als Open Source bereitgestellt wird. Envoy belegt Port 443 und alle eingehenden vCenter Server-Anfragen werden über Envoy weitergeleitet. `rhttpproxy` dient als Konfigurationsverwaltungsserver für Envoy. Folglich wird die TLS-Konfiguration auf `rhttpproxy` angewendet, wodurch die Konfiguration an Envoy gesendet wird.

Implementieren von TLS mithilfe von TLS-Profilen durch vSphere

vSphere 8.0 Update 3 implementiert TLS 1.3 durch Gruppierung von Parametern, einschließlich Protokollversionen, Gruppen (auch Curves genannt) und Verschlüsselungen, in ein einzelnes TLS-Profil. Dieses TLS-Profil wird systemweit angewendet. Die Verwendung eines einzelnen TLS-Profils erleichtert den verwaltungstechnischen Aufwand Ihrer Hosts. Sie müssen einzelne

TLS-Parameter nicht mehr manuell konfigurieren, obwohl diese Funktion bei Bedarf weiterhin verfügbar ist. TLS-Profile verbessern auch die Unterstützbarkeit erheblich. Die Gruppierung von Parametern in TLS-Profile vereinfacht den Satz an VMware-geprüften TLS-Lösungen, aus denen ausgewählt werden kann. In ESXi werden TLS-Profile in vSphere Configuration Profiles integriert.

Die folgenden TLS-Profile werden in ESXi bereitgestellt:

- COMPATIBLE: Das Standardprofil. Die genaue Zuordnung der Parameter in diesem Profil kann von Version zu Version geändert werden. Das Profil ist jedoch garantiert mit allen unterstützten Produkten und Versionen kompatibel (derzeit N-2-Versionen). Demnach kann ein ESXi-Host aus Version N, der das COMPATIBLE-Profil verwendet, mit einem Host von Version N-2 kommunizieren.
- NIST_2024: Ein restriktiveres Profil, das speziell den NIST 2024-Standard unterstützt. Die genaue Zuordnung der Parameter in diesem Profil wird garantiert, um den NIST 2024-Standard über alle Versionen hinweg zu erfüllen. Dieses Profil ist garantiert nur mit aktuellen oder neueren Versionen und nicht mit älteren Versionen kompatibel.
- MANUAL: Verwenden Sie dieses Profil, um eine Ad-hoc-Konfiguration zu erstellen und zu testen, in der Sie die TLS-Parameter manuell angeben. Es wird nicht garantiert, dass ein MANUAL-Profil fehlerfrei funktioniert. Sie müssen ein MANUAL-Profil testen, auch über Software-Upgrades hinweg. Wenn Sie ein MANUAL-Profil verwenden, wird das Systemverhalten standardmäßig zunächst auf das zuvor ausgewählte Profil (COMPATIBLE oder NIST_2024) festgelegt und bleibt so lange bestehen, bis Sie Änderungen vornehmen. Sie müssen `esxcli`-Befehle verwenden, um das TLS-Profil MANUAL zu verwalten. Weitere Informationen zum Ändern der Parameter im TLS-Profil MANUAL finden Sie im Hilfetext, der in `esxcli` enthalten ist.

Wenn Sie das TLS-Profil auf den gewünschten Zustand festlegen, müssen Sie den ESXi-Host neu starten oder den vLCM-Cluster standardisieren, in dem sich der ESXi-Host befindet, um Änderungen zu übernehmen.

Die folgenden Tabellen zeigen die Details der TLS-Profile für ESXi und vCenter Server in vSphere 8.0 Update 3. In der Spalte mit der Verschlüsselungsliste werden die TLS-Verschlüsselungen für TLS 1.2- und frühere Protokolle angezeigt. In der Spalte mit den Verschlüsselungs-Suites werden die Verschlüsselungen für das TLS 1.3-Protokoll angezeigt.

Tabelle 15-1. ESXi TLS 1.3-Profile

TLS-Profilname	TLS-Protokollversionen	Verschlüsselungsliste	Verschlüsselungssammlungen	Curves	Von VMware unterstützt?
COMPATIBLE	TLS 1.3 und TLS 1.2	ECDHE+AESGCM:ECDHE+AES	TLS_AES_256_GCM_SHA384; TLS_AES_128_GCM_SHA256	prime256v1:secp384r1:secp521r1	Ja
NIST_2024	TLS 1.3 und TLS 1.2	ECDHE+AESGCM	TLS_AES_256_GCM_SHA384; TLS_AES_128_GCM_SHA256	prime256v1:secp384r1:secp521r1	Ja
MANUAL	Alle	Alle	Alle	Alle	Nein

Hinweise:

- Unterstützte Einstellungen (Protokolle, Verschlüsselungsliste, Verschlüsselungs-Suites und Curves) stellen höchstens das dar, was unterstützt wird.
- Das NIST_2024-Profil gilt nur für eingehende Verbindungen.
- Das kryptografische Modul „BoringSSL“, das in vSphere 8.0 Update 3 verwendet wird, hat die FIPS-Zertifizierung für die Verwendung von TLS 1.3 noch nicht erreicht. Dies führt dazu, dass Port 443 (Reverse-Proxy) in ESXi und vCenter Server mithilfe von TLS 1.2 kommuniziert. Von den TLS-Profilen COMPATIBLE und NIST_2024 wird TLS 1.3 ohne FIPS nicht verwendet.

Die folgenden vCenter Server TLS 1.3-Profile werden bereitgestellt:

- COMPATIBLE: Das Standardprofil. Die genaue Zuordnung der Parameter in diesem Profil kann von Version zu Version geändert werden. Das Profil ist jedoch garantiert mit allen unterstützten Produkten und Versionen kompatibel (derzeit N-2-Versionen).
- NIST_2024: Ein restriktiveres Profil, das speziell den NIST 2024-Standard unterstützt. Die genaue Zuordnung der Parameter in diesem Profil wird garantiert, um den NIST 2024-Standard über alle Versionen hinweg zu erfüllen. Dieses Profil ist garantiert nur mit aktuellen oder neueren Versionen und nicht mit älteren Versionen kompatibel.
- COMPATIBLE-NON-FIPS: Ein geändertes Profil, das eine TLS 1.3-Verbindung ohne FIPS über den Envoy-Proxy zulässt. FIPS ist nicht aktiviert.

Tabelle 15-2. vCenter Server TLS 1.3-Profile

TLS-Profilname	TLS-Protokollversionen	Verschlüsselungssammlungen	Curves	FIPS aktiviert?	Von VMware unterstützt?
COMPATIBLE	TLS 1.3	TLS_AES_256_GCM_SHA384; TLS_AES_128_GCM_SHA256	prime256v1:secp384r1:secp521r1	Ja	Ja
	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 AES256-GCM-SHA384 AES128-GCM-SHA256 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES128-SHA AES256-SHA AES128-SHA			
NIST_2024	TLS 1.3	TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256	prime256v1:secp384r1:secp521r1	Ja	Ja

Tabelle 15-2. vCenter Server TLS 1.3-Profile (Fortsetzung)

TLS-Profilname	TLS-Protokollversionen	Verschlüsselungssammlungen	Curves	FIPS aktiviert?	Von VMware unterstützt?
	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256			
COMPATIBLE-NON-FIPS	TLS 1.3	TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256	prime256v1:secp384r1:secp521r1	Nein	Ja
	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 AES256-GCM-SHA384 AES128-GCM-SHA256 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES128-SHA AES256-SHA AES128-SHA			

TLS und eingehende sowie ausgehende Verbindungen in ESXi und vCenter Server

ESXi 8.0 Update 3 unterstützt TLS 1.3 sowohl für eingehende (Server) als auch für ausgehende Verbindungen (Client). Die eingehenden ESXi-Verbindungen (Server) sind von größter Bedeutung, und es gilt das restriktivere NIST_2024 Profil.

Für ESXi können Sie die Einstellungen COMPATIBLE, NIST_2024 und MANUAL für eingehende Verbindungen (Server) verwenden. Sie können die Einstellungen COMPATIBLE und MANUAL für ausgehende Verbindungen (Client) verwenden.

vCenter Server TLS-Profile übernehmen ihre Einstellungen sowohl für eingehende als auch für ausgehende Verbindungen.

Einige vSphere-Dienste machen Ports verfügbar, die TLS-Verbindungen akzeptieren, während die meisten Dienste den Reverse-Proxy verwenden. Alle eingehenden Verbindungen akzeptieren standardmäßig TLS 1.2 und TLS 1.3. Derzeit ist TLS 1.3 für Port 443 (Reverse-Proxy) deaktiviert, und die Kommunikation erfolgt über TLS 1.2. Ausgehende Verbindungen unterstützen TLS 1.2 und TLS 1.3. Weitere Informationen finden Sie unter TLS 1.3 auf Port 443 in ESXi und FIPS.

TLS und Lebenszyklusverwaltung

Durch das Upgrade oder die Migration eines ESXi-Hosts oder vCenter Server-Hosts zu 8.0 Update 3 wird standardmäßig das TLS-Profil COMPATIBLE aktiviert. vSphere 8.0 Update 3 unterstützt TLS 1.3 und TLS 1.2 für eine minimale Out of the box-Bare-Interoperabilität. In Zukunft wird beim Upgrade auf eine höhere Version von ESXi oder vCenter Server das aktuelle TLS-Profil verwendet, solange dieses Profil nicht stillgelegt wurde.

Wenn Sie ein Upgrade auf eine neue Version durchführen, legen Sie als Best Practice zuerst das TLS-Profil auf COMPATIBLE fest.

Wenn Sie vor dem Upgrade auf vSphere 8.0 Update 3 lokale Änderungen auf Dienstebene vornehmen, wird dem Host nach dem Upgrade das COMPATIBLE-Profil zugewiesen, das diese Änderungen nicht berücksichtigt. Damit der Host diese Änderungen berücksichtigt, wechseln Sie zum MANUAL-Profil. Weitere Informationen finden Sie unter Ändern des TLS-Profils eines ESXi-Hosts mithilfe des vSphere Client oder Ändern des TLS-Profils eines ESXi-Hosts mithilfe der CLI.

Warnung Das TLS-Profil MANUAL funktioniert nicht fehlerfrei über Upgrades hinweg. Sie müssen überprüfen, ob ein bearbeitetes TLS-Profil MANUAL versionsübergreifend funktioniert, oder zum TLS-Profil COMPATIBLE wechseln.

TLS 1.3 auf Port 443 in ESXi und FIPS

Derzeit deaktiviert vSphere TLS 1.3 auf Port 443. Die Version des kryptografischen Moduls „BoringSSL“, das in vSphere 8.0 Update 3 verwendet wird, ist nicht FIPS-zertifiziert für TLS 1.3. Wenn Sie das TLS-Profil COMPATIBLE oder NIST_2024 verwenden, kommunizieren alle Ports außer 443 über TLS 1.3. Derzeit verwendet Port 443 aufgrund dieses Problems TLS 1.2.

Informationen zum Aktivieren von TLS 1.3 ohne FIPS auf Port 443 finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/92473.

Lesen Sie als Nächstes die folgenden Themen:

- Verwalten der vSphere-TLS

Verwalten der vSphere-TLS

Ab vSphere 8.0 Update 3 können Sie TLS-Profile für ESXi mithilfe von vSphere Client, des `esxcli`-Befehls oder der APIs verwalten. Für vCenter Server verwalten Sie TLS-Profile mithilfe von APIs.

Wenn Sie vSphere Configuration Profiles verwenden, können Sie die TLS-Einstellung für ESXi-Hosts auf vLCM-Clusterebene verwalten. Sie können die TLS-Einstellung für den Cluster ändern und den Cluster anhand dieser neuen Konfiguration standardisieren. Weitere Informationen finden Sie im Kapitel zum Verwalten von vSphere Configuration Profiles in der Dokumentation zum *Verwalten des Lebenszyklus von Host und Cluster*.

Für eigenständige ESXi-Hosts und Nicht-vLCM-Cluster müssen Sie das TLS-Profil mithilfe der `esxcli`-Befehle verwalten. Weitere Informationen finden Sie in der Dokumentation zum *ESXCLI – Konzepte und Beispiele* und in der Online-Hilfe zu `esxcli`.

Derzeit können Sie vCenter Server TLS-Profile nur mithilfe von APIs verwalten. Weitere Informationen finden Sie im *Programmierhandbuch zu den vSphere Automation SDKs* und im *Programmierhandbuch zur vSphere Automation REST API*.

Anzeigen des TLS-Profils eines ESXi-Hosts mit vSphere Client

Sie können vSphere Client verwenden, um das TLS-Profil eines ESXi-Hosts anzuzeigen, der Teil eines vLCM-Clusters ist.

In vSphere Configuration Profiles verwenden nicht explizit konfigurierte Einstellungen die Standardwerte aus dem entsprechenden Profil. Für TLS-Profile lautet die Standardeinstellung COMPATIBLE.

Informationen zum Anzeigen des TLS-Profils eines eigenständigen oder Nicht-vLCM-Clusters auf einem ESXi-Host finden Sie unter Anzeigen des TLS-Profils eines ESXi-Hosts mithilfe der CLI.

Voraussetzungen

Sie haben vSphere Configuration Profiles aktiviert und eine Entwurfskonfiguration für den Cluster erstellt. Informationen finden Sie in der Dokumentation *Verwalten des Lebenszyklus von Host und Cluster*.

Verfahren

1. Navigieren Sie in vSphere Client zum vLCM-Cluster, den Sie mit einem einzelnen Image verwalten.
2. Klicken Sie auf der Registerkarte **Konfigurieren** auf **Gewünschter Zustand > Konfiguration**.
3. Klicken Sie auf der Registerkarte **Einstellungen** auf **System**.
4. Klicken Sie auf **tls_client** oder **tls_server**, um anzuzeigen, welches TLS-Profil im aktuellen gewünschten Konfigurationsdokument definiert ist.

Anzeigen des TLS-Profils eines ESXi-Hosts mithilfe der CLI

Sie können die CLI verwenden, um das aktuell konfigurierte TLS-Profil eines ESXi-Hosts anzuzeigen.

Für eigenständige ESXi-Hosts und Nicht-vLCM-Cluster müssen Sie das TLS-Profil mithilfe der `esxcli`-Befehle verwalten. Weitere Informationen finden Sie unter *ESXCLI – Referenz*. Für ESXi-Hosts in einem vLCM-Cluster können Sie entweder vSphere Configuration Profiles oder `esxcli`-Befehle verwenden.

Voraussetzungen

Aktivieren Sie entweder SSH oder die ESXi Shell auf dem ESXi-Host.

Verfahren

1 Stellen Sie eine Verbindung zum ESXi-Host her.

   Sie können SSH oder ESXi Shell verwenden.

2 Führen Sie den folgenden Befehl aus, um das aktuell konfigurierte TLS-Profil anzuzeigen.

```
esxcli system tls [client | server] get
```

3 Führen Sie den folgenden Befehl aus, um die Parameter im aktuell konfigurierten TLS-Profil anzuzeigen:

```
esxcli system tls [client | server] get --show-profile-defaults
```

Ändern des TLS-Profils eines ESXi-Hosts mithilfe des vSphere Client

Sie können das TLS-Profil eines ESXi-Hosts ändern. Das Standardmäßige TLS-Profil ist KOMPATIBEL.

Voraussetzungen

Sie haben vSphere Configuration Profiles aktiviert und eine Entwurfskonfiguration für den Cluster erstellt. Informationen finden Sie in der Dokumentation *Verwalten des Lebenszyklus von Host und Cluster*.

Verfahren

1 Navigieren Sie in vSphere Client zu einem Cluster, den Sie mit einem einzelnen Image verwalten.

2 Klicken Sie auf der Registerkarte **Konfigurieren** auf **Gewünschter Zustand > Konfiguration**.

3 Klicken Sie auf der Registerkarte **Einstellungen** auf **System**.

4 Klicken Sie auf **tls_client** oder **tls_server**.

   Je nachdem, ob die Einstellung zuvor geändert wurde, klicken Sie entweder auf **Konfigurationseinstellungen** oder auf **Bearbeiten**.

5 Wählen Sie ein TLS-Profil im Dropdown-Menü aus.

6 Klicken Sie auf **Speichern**.

7 Standardisieren Sie den Cluster anhand der Entwurfskonfiguration.

   a Um den Cluster anhand der Entwurfskonfiguration zu standardisieren, klicken Sie auf der Registerkarte **Entwurf** auf **Änderungen anwenden**.

   b Folgen Sie den Schritten im Assistenten **Standardisieren**. Weitere Informationen finden Sie in der Dokumentation *Verwalten des Lebenszyklus von Host und Cluster*.

Ergebnisse

Alle ESXi-Hosts im Cluster sind mit der gewünschten Konfiguration kompatibel.

Ändern des TLS-Profils eines ESXi-Hosts mithilfe der CLI

Sie können das TLS-Profil eines ESXi-Hosts ändern. Das Standardmäßige TLS-Profil ist KOMPATIBEL.

Für eigenständige ESXi-Hosts und Nicht-vLCM-Cluster müssen Sie das TLS-Profil mithilfe der `esxcli`-Befehle verwalten. Weitere Informationen finden Sie unter *ESXCLI – Referenz*. Für ESXi-Hosts in einem vLCM-Cluster können Sie entweder vSphere Configuration Profiles oder `esxcli`-Befehle verwenden.

Voraussetzungen

Aktivieren Sie entweder SSH oder die ESXi Shell auf dem ESXi-Host.

Verfahren

1. Stellen Sie eine Verbindung zum ESXi-Host her.

   Sie können dazu SSH oder die ESXi Shell verwenden.
2. Versetzen Sie den ESXi-Host in den Wartungsmodus.
3. Um das TLS-Profil zu ändern, führen Sie den folgenden Befehl aus.

   ```
   esxcli system tls [client | server] set --profile [COMPATIBLE | NIST_2024 | MANUAL]
   ```

   Hinweis Wenn Sie Änderungen an den TLS-Parametern vornehmen möchten (entweder auf System- oder Dienstebene), wählen Sie das Profil MANUELL aus.
4. Starten Sie den ESXi-Host neu, damit die Änderungen wirksam werden.
5. Nachdem der ESXi-Host neu gestartet wurde, beenden Sie den Wartungsmodus.

Bearbeiten der Parameter im MANUAL TLS-Profil in der CLI

Den Parametersatz im MANUAL TLS-Profil können Sie bearbeiten. Um TLS-Parameter wie Verschlüsselungsliste und Verschlüsselungssuite zu ändern, müssen Sie für das TLS-Profil zuerst auf MANUAL festlegen.

Warnung Broadcom unterstützt das MANUAL TLS-Profil nicht. Es werden nur die TLS-Profile COMPATIBLE und NIST_2024 unterstützt. Die Verwendung des MANUAL TLS-Profils erfolgt auf eigene Gefahr.

Die Parameter im MANUAL TLS-Profil verwalten Sie über `esxcli`-Befehle. Die Verwaltung der Parameter des MANUAL TLS-Profils ist nicht in vSphere Configuration Profiles integriert.

Sie können TLS-Parameter nicht für einzelne vSphere-Dienste festlegen. Änderungen, die Sie unter Verwendung des MANUAL TLS-Profils vornehmen, werden auf Systemebene angewendet.

Voraussetzungen

Aktivieren Sie entweder SSH oder die ESXi Shell auf dem ESXi-Host.

Ändern Sie das TLS-Profil in MANUAL. Sehen Sie hierzu Ändern des TLS-Profils eines ESXi-Hosts mithilfe des vSphere Client oder Ändern des TLS-Profils eines ESXi-Hosts mithilfe der CLI.

Verfahren

1. Stellen Sie eine Verbindung zum ESXi-Host her.

   Sie können dazu SSH oder die ESXi Shell verwenden.
2. Versetzen Sie den ESXi-Host in den Wartungsmodus.
3. Stellen Sie sicher, dass das TLS-Profil auf MANUAL festgelegt ist.

   ```
   esxcli system tls [client | server] get
   ```
4. Führen Sie folgende Befehle aus, um die Parameter zu ändern.

   ```
   esxcli system tls [client | server] set --cipher-list=str
   esxcli system tls [client | server] set --cipher-suite=str
   esxcli system tls [client | server] set --groups=str
   esxcli system tls [client | server] set --protocol-versions=str
   ```

   str ist hier eine Zeichenfolge im OpenSSL-Stil, d. h. durch Doppelpunkte, Kommas oder Leerzeichen getrennt. Beispiel: `--cipher-list=ECDHE+AESGCM:ECDHE+AES`

   Weitere Informationen erhalten Sie, indem Sie folgenden Befehl ausführen:

   ```
   esxcli system tls [client | server] set --help
   ```
5. Starten Sie den ESXi-Host neu, damit die Änderungen wirksam werden.
6. Nachdem der ESXi-Host neu gestartet wurde, beenden Sie den Wartungsmodus.

Beispiel

Im folgenden Beispiel wird zuerst das TLS-Profil auf MANUAL festgelegt. Dann wird ein restriktiverer Satz Kurven (Gruppen) festgelegt. Damit die Änderungen wirksam werden, ist ein Neustart erforderlich.

```
[root@host1] esxcli system tls server get
   Profile: COMPATIBLE
   Cipher List: <profile default>
   Cipher Suite: <profile default>
   Groups: <profile default>
   Protocol Versions: <profile default>
   Reboot Required: false
[root@host1] esxcli system tls server set --profile MANUAL
[root@host1] esxcli system tls server get
   Profile: MANUAL
   Cipher List: ECDHE+AESGCM:ECDHE+AES
   Cipher Suite: TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384
   Groups: prime256v1:secp384r1:secp521r1
   Protocol Versions: tls1.2,tls1.3
   Reboot Required: true
[root@host1] esxcli system tls server set --groups=prime256v1:secp384r1
```

```
[root@host1] esxcli system tls server get
   Profile: MANUAL
   Cipher List: TLS_AES_128_CCM_SHA256
   Cipher Suite: TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384
   Groups: prime256v1:secp384r1
   Protocol Versions: tls1.2,tls1.3
   Reboot Required: true
```

Verwalten des TLS-Profils eines vCenter Server-Hosts

Sie verwenden die APIs, um das TLS-Profil für einen vCenter Server-Host anzuzeigen und zu ändern.

Zur Ausführung von HTTP-Anforderungen stehen mehrere Möglichkeiten zur Verfügung. Diese Aufgabe zeigt die Verwendung von Developer Center im vSphere Client zum Verwalten von TLS-Profilen. Im *VMware vCenter Server Management-Programmierhandbuch* finden Sie weitere Informationen zur Verwendung von APIs zum Verwalten der vCenter Server Appliance.

Verfahren

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

2 Wählen Sie im Menü die Option **Developer Center** aus.

3 Klicken Sie auf **API-Explorer**.

4 Wählen Sie im Dropdown **API auswählen** die Option **Appliance** aus.

Die folgenden API-Kategorien und -Aktionen sind verfügbar.

Tabelle 15-3. vCenter Server TLS-APIs

Option	API-Kategorie	Zugeordnete Aktion
Ruft die Liste aller TLS-Profile und deren Konfiguration ab.	tls/profiles/	GET
Ruft die Parameter eines bestimmten TLS-Profils ab.	tls/profiles/{id}	GET
Ruft den Namen des aktuellen TLS-Profils ab, das global konfiguriert ist.	tls/profiles/global/	GET
Legt eines der Standardprofile fest, die von Ihnen global angegeben werden.	tls/profiles/global/	PUT **Hinweis** Mit dieser Aktion werden die vCenter Server-Dienste neu gestartet.
Ruft die Parameter des aktuellen TLS-Profils ab, das global konfiguriert ist.	tls/manual-parameters/global	GET

Hinweis Derzeit können Sie die Parameter eines vCenter Server TLS-Profils nicht ändern.

5 Führen Sie den gewünschten Befehl aus.

Definierte Rechte

16

In den folgenden Tabellen werden die Standardrechte aufgelistet, die mit einem Benutzer kombiniert und einem Objekt zugeordnet werden können, wenn sie für eine Rolle ausgewählt werden.

Stellen Sie beim Festlegen der Berechtigungen sicher, dass alle Objekttypen mit geeigneten Rechten für jede spezielle Aktion eingerichtet sind. Für einige Vorgänge sind neben dem Zugriff auf das bearbeitete Objekt auch Zugriffsberechtigungen für den Root-Ordner oder den übergeordneten Ordner erforderlich. Einige Vorgänge erfordern Zugriff oder Leistungsberechtigung für einen übergeordneten Ordner und ein verwandtes Objekt. Siehe auch Verwenden des Rechte-Recorders.

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.

Lesen Sie als Nächstes die folgenden Themen:

- Alarmrechte
- Rechte für Auto Deploy und Image-Profile
- Zertifikatsrechte
- Berechtigungen der Zertifizierungsstelle
- Berechtigungen der Zertifikatsverwaltung
- CNS-Rechte
- Rechte für Computing-Richtlinien
- Rechte für Inhaltsbibliotheken
- Rechte für Verschlüsselungsvorgänge
- dvPort-Gruppenrechte
- Rechte für Distributed Switches
- Rechte für Datencenter
- Berechtigungen für Datenspeicher
- Rechte für Datenspeicher-Cluster

- ESX Agent Manager-Rechte
- Rechte für Erweiterungen
- Rechte für Bereitstellungsfunktion externer Statistiken
- Rechte für Ordner
- Globale Rechte
- Interaktion mit den Gastdaten-Veröffentlichungsrechten
- Rechte für den verknüpften Hybridmodus
- Rechte für Bereitstellungsfunktion für Aktualisierungen des Systemzustands
- Host-CIM-Rechte
- Rechte für die Hostkonfiguration
- Host-Entropie-Pool-Rechte
- Intel Software Guard Extensions-Hostrechte
- Rechte für die Hostbestandsliste
- Rechte für lokale Hostoperationen
- Host-Statistikrechte
- Trusted Platform Module (TPM)-Hostrechte
- vSphere Replication-Rechte von Hosts
- Hostprofil-Berechtigungen
- vCenter Server-Profilrechte
- vSphere Namespaces-Rechte
- Netzwerkberechtigungen
- NSX-Rechte
- VMware Observability-Rechte
- OvfManager-Rechte
- Rechte für die Interaktion mit Partner-REST-Daemons
- Leistungsrechte
- Plug-In-Rechte
- Rechte für die Replizierung als Dienst
- Rechte für Berechtigungen
- Rechte für VM-Speicherrichtlinien
- Rechte für Ressourcen
- Rechte für geplante Aufgaben

- Sitzungsrechte
- Speicheransichtsberechtigungen
- Rechte für Supervisor-Dienste
- Rechte für Aufgaben
- Mandantenmanagerrechte
- Transfer Service-Rechte
- Rechte für VcTrusts/VcIdentity
- Rechte für „Administrator der vertrauenswürdigen Infrastruktur“
- vApp-Rechte
- Rechte für VcIdentityProviders
- Rechte für die Konfiguration von VMware vSphere Lifecycle Manager
- Gewünschte Rechte für die Konfigurationsverwaltung von VMware vSphere Lifecycle Manager
- Rechte für ESXi-Integritätsperspektiven für VMware vSphere Lifecycle Manager
- Rechte für VMware vSphere Lifecycle Manager-Depots
- Allgemeine Rechte für VMware vSphere Lifecycle Manager
- Rechte für die Hardwarekompatibilität von VMware vSphere Lifecycle Manager
- Rechte für VMware vSphere Lifecycle Manager-Images
- Rechte für die Standardisierung von VMware vSphere Lifecycle Manager-Images
- Rechte für VMware vSphere Lifecycle Manager-Einstellungen
- Rechte für die Verwaltung von VMware vSphere Lifecycle Manager-Baselines
- Rechte zum Verwalten von Patches und Upgrades für VMware vSphere Lifecycle Manager
- Rechte zum Hochladen von Dateien für VMware vSphere Lifecycle Manager
- Rechte zum Ändern der VM-Konfiguration
- Rechte für Vorgänge als Gast auf virtuellen Maschinen
- Rechte für die Interaktion virtueller Maschinen
- Rechte zum Bearbeiten der Bestandsliste einer 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
- Rechte für VM-Klassen

- vSAN-Rechte
- Rechte für vSAN-Statistiken
- vSphere-Zonen-Rechte
- vService-Rechte
- vSphere-Tag-Berechtigungen
- vSphere Client-Rechte
- vSphere Data Protection-Rechte
- vSphere Stats-Rechte

Alarmrechte

Alarmrechte steuern die Fähigkeit, Alarme für Bestandslistenobjekte zu erstellen, zu ändern und darauf zu reagieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-1. Alarmrechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Alarm bestätigen	Ermöglicht die Unterdrückung aller Alarmaktionen für alle ausgelösten Alarme.	Objekt, für das ein Alarm definiert ist	Alarm.Acknowledge
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	Alarm.Create
Alarmaktion deaktivieren	Ermöglicht das Verhindern, dass eine Alarmaktion ausgeführt wird, nachdem ein Alarm ausgelöst wurde. Der Alarm selbst ist nicht deaktiviert.	Objekt, für das ein Alarm definiert ist	Alarm.DisableActions
Deaktivieren oder Aktivieren des Alarms für Element	Ermöglicht das Aktivieren oder Deaktivieren eines bestimmten Alarms für einen bestimmten Zieltyp.	Objekt, für das der Alarm ausgelöst werden kann	Alarm.ToggleEnableOnEntity

Tabelle 16-1. Alarmrechte (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Alarm ändern	Ermöglicht die Änderung der Eigenschaften eines Alarms.	Objekt, für das ein Alarm definiert ist	Alarm.Edit
Alarm entfernen	Ermöglicht das Löschen eines Alarms.	Objekt, für das ein Alarm definiert ist	Alarm.Delete
Alarmstatus festlegen	Ermöglicht das Ändern des Status des konfigurierten Ereignisalarms. Der Status kann den Wert **Normal**, **Warnung** oder **Alarm** annehmen.	Objekt, für das ein Alarm definiert ist	Alarm.SetStatus

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. Weitere Informationen zu Auto Deploy finden Sie in der Dokumentation *Installation und Einrichtung von VMware ESXi*.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-2. Auto Deploy-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **-Host** ■ **Maschine verknüpfen**	Ermöglicht Benutzern das Zuordnen eines Hosts zu einem Computer.	vCenter Server	AutoDeploy.Host.AssociateMachine
■ **Image-Profil** ■ **Erstellen** ■ **Bearbeiten**	**Erstellen** ermöglicht das Erstellen von Image-Profilen. **Bearbeiten** ermöglicht das Bearbeiten von Image-Profilen.	vCenter Server	AutoDeploy.Profile.Create AutoDeploy.Profile.Edit

Tabelle 16-2. Auto Deploy-Rechte (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Regel** ■ **Erstellen** ■ **Bearbeiten** ■ **Löschen**	**Erstellen** ermöglicht das Erstellen von Auto Deploy-Regeln. **Bearbeiten** ermöglicht das Bearbeiten von Auto Deploy-Regeln. **Löschen** ermöglicht das Löschen von Auto Deploy-Regeln.	vCenter Server	AutoDeploy.Rule.Create AutoDeploy.Rule.Edit AutoDeploy.Rule.Delete
■ **Regelsatz** ■ **Aktivieren** ■ **Bearbeiten**	**Aktivieren** ermöglicht das Aktivieren von Auto Deploy-Regelsätzen. **Bearbeiten** ermöglicht das Bearbeiten von Auto Deploy-Regelsätzen.	vCenter Server	AutoDeploy.RuleSet.Activate AutoDeploy.RuleSet.Edit

Zertifikatsrechte

Zertifikatsrechte bestimmen, welche Benutzer ESXi-Zertifikate verwalten können.

Dieses Recht bestimmt, wer die Zertifikatsverwaltung für ESXi-Hosts durchführen kann. Im Abschnitt zu den erforderlichen Rechten für Zertifikatverwaltungsvorgänge der Dokumentation *vSphere-Authentifizierung* finden Sie Informationen zur vCenter Server-Zertifikatsverwaltung.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-3. Rechte für Hostzertifikate

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Zertifikate verwalten	Ermöglicht die Zertifikatsverwaltung für ESXi-Hosts.	vCenter Server	Certificate.Manage

Berechtigungen der Zertifizierungsstelle

Mit Berechtigungen der Zertifizierungsstelle werden Aspekte der VMCA-Zertifikate (VMware Certificate Authority) gesteuert.

Tabelle 16-4. Berechtigungen der Zertifizierungsstelle

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Erstellen/Löschen (Administratorrecht).	Ermöglicht Vollzugriff auf Administratorebene für die Verwaltung von vCenter Server-Zertifikaten.	vCenter Server	CertificateAuthority.Administer
Erstellen/Löschen (unter Administratorrecht).	Ermöglicht die Anzeige des VMCA-Rootzertifikats auf der Seite „Zertifikatsverwaltung“ im vSphere Client.	vCenter Server	CertificateAuthority.Manage

Berechtigungen der Zertifikatsverwaltung

Über die Berechtigungen der Zertifikatsverwaltung werden die Benutzer bestimmt, die vCenter Server-Zertifikate verwalten können.

Tabelle 16-5. Berechtigungen der Zertifikatsverwaltung

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Erstellen/Löschen (Administratorrecht).	Ermöglicht Vollzugriff auf Administratorebene auf verschiedene interne APIs und Funktionen für zertifikatsbezogene vCenter Server-Vorgänge.	vCenter Server	CertificateManagement.Administer
Erstellen/Löschen (unter Administratorrecht).	Ermöglicht verringerten administrativen Zugriff auf verschiedene interne APIs und Funktionen. Mit dieser Berechtigung werden zertifikatsbezogene Vorgänge so eingeschränkt, dass der Benutzer Nicht-Administratorrechte nicht eskalieren kann. Zu den zulässigen Vorgängen gehören: ■ Erzeugen von Zertifikatsignieranforderungen ■ Erstellen und Abrufen vertrauenswürdiger Stammzertifikatsketten ■ Löschen vertrauenswürdiger Stammzertifikatsketten, die von einem Benutzer mit der Berechtigung **Zertifikatverwaltung.Erstellen/Löschen (unter Administratorrechten).** erstellt wurden ■ Abrufen von Maschinen-SSL-Zertifikaten ■ Abrufen der Signaturzertifikatsketten zum Validieren von Token, die von vCenter Server ausgegeben wurden	vCenter Server	CertificateManagement.Manage

CNS-Rechte

Mit CNS-Rechten (Cloud Native Store) werden die Benutzer gesteuert, die auf die CNS-Benutzeroberfläche zugreifen können.

Tabelle 16-6. CNS-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Durchsuchbar	Ermöglicht dem Speicheradministrator die Anzeige der CNS-Benutzeroberfläche (Cloud Native Storage).	Root-vCenter Server	Cns.Searchable

Rechte für Computing-Richtlinien

Rechte für Computing-Richtlinien steuern die Fähigkeit zum Verwalten von Computing-Richtlinien.

Tabelle 16-7. Rechte für Computing-Richtlinien

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Computing-Richtlinie erstellen und löschen	Ermöglicht das Erstellen und Löschen von Computing-Richtlinien.	Root-vCenter Server	ComputePolicy.Manage

Rechte für Inhaltsbibliotheken

Inhaltsbibliotheken bieten einfache und effiziente Verwaltung für Vorlagen virtueller Maschinen und vApps. Mit Rechten für Inhaltsbibliotheken wird gesteuert, wer verschiedene Aspekte von Inhaltsbibliotheken anzeigen oder verwalten darf.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis Die Vererbung von Berechtigungen für Inhaltsbibliotheken geschieht im Kontext einer einzelnen vCenter Server-Instanz. Inhaltsbibliotheken sind jedoch aus Sicht der Bestandsliste keine direkt untergeordneten Elemente eines vCenter Server-Systems. Das direkt übergeordnete Element für Inhaltsbibliotheken ist das globale Rootobjekt. Diese Beziehung bedeutet, dass wenn Sie eine Berechtigung auf vCenter Server-Ebene festlegen und an die untergeordneten Objekte weitergeben, die Berechtigung für Datencenter, Ordner, Cluster, Hosts, virtuelle Maschinen usw. gilt. Diese Berechtigung gilt jedoch nicht für die Inhaltsbibliotheken, die in dieser vCenter Server-Instanz angezeigt werden und die Sie verwenden. Um eine Berechtigung für eine Inhaltsbibliothek in zuzuweisen, muss ein Administrator dem Benutzer die Berechtigung als globale Berechtigung erteilen. Globale Berechtigungen unterstützen das lösungsübergreifende Zuweisen von Berechtigungen von einem globalen Stammobjekt aus.

Tabelle 16-8. Rechte für Inhaltsbibliotheken

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Bibliothekselement hinzufügen	Ermöglicht das Hinzufügen von Elementen in einer Bibliothek.	Bibliothek	ContentLibrary.AddLibraryItem
Stammzertifikat zum Truststore hinzufügen	Ermöglicht das Hinzufügen von Stammzertifikaten zum Speicher für vertrauenswürdige Stammzertifikate.	vCenter Server	ContentLibrary.AddCertToTrustStore
Vorlage einchecken	Ermöglicht das Einchecken von Vorlagen.	Bibliothek	ContentLibrary.CheckInTemplate
Vorlage auschecken	Ermöglicht das Auschecken von Vorlagen.	Bibliothek	ContentLibrary.CheckOutTemplate
Abonnement für veröffentlichte Bibliothek erstellen	Ermöglicht das Erstellen eines Bibliotheksabonnements.	Bibliothek	ContentLibrary.AddSubscription
Lokale Bibliothek erstellen	Ermöglicht die Erstellung lokaler Bibliotheken auf dem festgelegten vCenter Server-System.	vCenter Server	ContentLibrary.CreateLocalLibrary

Tabelle 16-8. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Harbor-Registrierung erstellen oder löschen	Ermöglicht das Erstellen oder Löschen des VMware Tanzu Harbor-Registrierungsdiens ts.	vCenter Server für die Erstellung. Registrierung für Löschen.	ContentLibrary.ManageRegistry
Abonnierte Bibliothek erstellen	Ermöglicht die Erstellung abonnierter Bibliotheken.	vCenter Server	ContentLibrary.CreateSubscribedLibrary
Harbor-Registrierungsproje kt erstellen, löschen oder bereinigen	Ermöglicht das Erstellen, Löschen oder Bereinigen von VMware Tanzu Harbor-Registrierungsproje kten.	Registrierung	ContentLibrary.ManageRegistryProject
Bibliothekselement löschen	Ermöglicht das Löschen von Bibliothekselemente n.	Bibliothek. Legen Sie diese Berechtigung zum Weitergeben an alle Bibliothekselemen te fest.	ContentLibrary.DeleteLibraryItem
Lokale Bibliothek löschen	Ermöglicht das Löschen einer lokalen Bibliothek.	Bibliothek	ContentLibrary.DeleteLocalLibrary
Stammzertifikat aus dem Truststore löschen	Ermöglicht das Löschen von Stammzertifikaten aus dem Speicher für vertrauenswürdige Stammzertifikate.	vCenter Server	ContentLibrary.DeleteCertFromTrustStore
Abonnierte Bibliothek löschen	Ermöglicht das Löschen einer abonnierten Bibliothek.	Bibliothek	ContentLibrary.DeleteSubscribedLibrary
Abonnement einer veröffentlichten Bibliothek löschen	Ermöglicht das Löschen eines Abonnements in einer Bibliothek.	Bibliothek	ContentLibrary.DeleteSubscription
Dateien herunterladen	Ermöglicht das Herunterladen von Dateien aus der Inhaltsbibliothek.	Bibliothek	ContentLibrary.DownloadSession

Tabelle 16-8. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
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.	ContentLibrary.EvictLibraryItem
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	ContentLibrary.EvictSubscribedLibrary

Tabelle 16-8. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Speicher importieren	Ermöglicht einem Benutzer den Import eines Bibliothekselements, wenn die Quelldatei-URL mit `ds://` oder `file://` beginnt. Dieses Recht ist für den Administrator der Inhaltsbibliothek standardmäßig deaktiviert. Da ein Import aus einer Speicher-URL den Import von Inhalten impliziert, aktivieren Sie dieses Recht nur im Bedarfsfall und wenn keine Sicherheitsbedenken für den Benutzer bestehen, der den Import ausführt.	Bibliothek	ContentLibrary.ImportStorage
Harbor-Registrierungsressourcen auf der angegebenen Computing-Ressource verwalten	Ermöglicht die Verwaltung von VMware Tanzu Harbor-Registrierungsressourcen.	Computing-Cluster	ContentLibrary.ManageClusterRegistryResource

Tabelle 16-8. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
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	ContentLibrary.ProbeSubscription
Bibliothekselement für seine Abonnenten veröffentlichen	Ermöglicht die Veröffentlichung von Bibliothekselementen an Abonnenten.	Bibliothek. Legen Sie diese Berechtigung zum Weitergeben an alle Bibliothekselemente fest.	ContentLibrary.PublishLibraryItem
Bibliothek für ihre Abonnenten veröffentlichen	Ermöglicht die Veröffentlichung von Bibliotheken an Abonnenten.	Bibliothek	ContentLibrary.PublishLibrary
Speicherinfos lesen	Ermöglicht das Lesen des Inhaltsbibliotheksspeichers.	Bibliothek	ContentLibrary.ReadStorage
Bibliothekselement synchronisieren	Ermöglicht die Synchronisation von Bibliothekselementen.	Bibliothek. Legen Sie diese Berechtigung zum Weitergeben an alle Bibliothekselemente fest.	ContentLibrary.SyncLibraryItem
Abonnierte Bibliothek synchronisieren	Ermöglicht die Synchronisation von abonnierten Bibliotheken.	Bibliothek	ContentLibrary.SyncLibrary

Tabelle 16-8. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Typenintrospektion	Ermöglicht einem Lösungsbenutzer oder einer API, den Typ der Unterstützungs-Plug-Ins für den Content Library Service zu untersuchen.	Bibliothek	ContentLibrary.TypeIntrospection
Konfigurationseinstellungen aktualisieren	Ermöglicht die Aktualisierung der Konfigurationseinstellungen. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	Bibliothek	ContentLibrary.UpdateConfiguration
Dateien aktualisieren	Ermöglicht Ihnen das Hochladen von Inhalt in die Inhaltsbibliothek. Ermöglicht Ihnen außerdem, Dateien aus einem Bibliothekselement zu entfernen.	Bibliothek	ContentLibrary.UpdateSession
Bibliothek aktualisieren	Ermöglicht Updates für die Inhaltsbibliothek.	Bibliothek	ContentLibrary.UpdateLibrary
Bibliothekselement aktualisieren	Ermöglicht Updates für Bibliothekselemente.	Bibliothek. Legen Sie diese Berechtigung zum Weitergeben an alle Bibliothekselemente fest.	ContentLibrary.UpdateLibraryItem
Lokale Bibliothek aktualisieren	Ermöglicht Updates lokaler Bibliotheken.	Bibliothek	ContentLibrary.UpdateLocalLibrary
Abonnierte Bibliothek aktualisieren	Ermöglicht die Aktualisierung der Eigenschaften einer abonnierten Bibliothek.	Bibliothek	ContentLibrary.UpdateSubscribedLibrary

Tabelle 16-8. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Abonnement einer veröffentlichten Bibliothek aktualisieren	Ermöglicht Aktualisierungen der Abonnementparameter. Benutzer können Parameter wie die vCenter Server-Instanzspezifikation der abonnierten Bibliothek und die Platzierung der zugehörigen VM-Vorlagenelemente aktualisieren.	Bibliothek	ContentLibrary.UpdateSubscription
Konfigurationseinstellungen anzeigen	Ermöglicht das Anzeigen der Konfigurationseinstellungen. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	Bibliothek	ContentLibrary.GetConfiguration

Rechte für Verschlüsselungsvorgänge

Mit Rechten für Verschlüsselungsvorgänge wird gesteuert, wer welchen Verschlüsselungsvorgangstyp für welchen Objekttyp durchführen kann.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-9. Rechte für Verschlüsselungsvorgänge

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Direktzugriff	Erlaubt Benutzern den Zugriff auf verschlüsselte Ressourcen. Benutzer können virtuelle Maschinen exportieren, mit NFC auf virtuelle Maschinen zugreifen und eine Konsolensitzung auf einer verschlüsselten virtuellen Maschine öffnen.	Virtuelle Maschine, Host oder Datenspeicher	Cryptographer.Access
Festplatte hinzufügen	Erlaubt Benutzern das Hinzufügen einer Festplatte zu einer verschlüsselten virtuellen Maschine.	Virtuelle Maschine	Cryptographer.AddDisk
Klonen	Erlaubt Benutzern das Klonen einer verschlüsselten virtuellen Maschine.	Virtuelle Maschine	Cryptographer.Clone
Entschlüsseln	Erlaubt Benutzern das Entschlüsseln einer virtuellen Maschine oder Festplatte.	Virtuelle Maschine	Cryptographer.Decrypt
Verschlüsseln	Erlaubt Benutzern das Verschlüsseln einer virtuellen Maschine oder VM-Festplatte.	Virtuelle Maschine	Cryptographer.Encrypt

Tabelle 16-9. Rechte für Verschlüsselungsvorgänge (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Neue verschlüsseln	Erlaubt Benutzern das Verschlüsseln einer virtuellen Maschine während der Erstellung einer virtuellen Maschine bzw. einer Festplatte während der Festplattenerstellung.	Ordner der virtuellen Maschine	Cryptographer.EncryptNew
Verschlüsselungsrichtlinien verwalten	Erlaubt Benutzern die Verwaltung von VM-Speicherrichtlinien mithilfe von Verschlüsselungs-E/A-Filtern. Standardmäßig nutzen virtuelle Maschinen, die die Speicherrichtlinie Verschlüsselung verwenden, keine anderen Speicherrichtlinien.	vCenter Server-Root-Ordner	Cryptographer.ManageEncryptionPolicy

Tabelle 16-9. Rechte für Verschlüsselungsvorgänge (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
KMS verwalten	Erlaubt Benutzern die Verwaltung des Schlüsselmanagementservers (Key Management Server) für das vCenter Server-System. Zu den Verwaltungsaufgaben zählen das Hinzufügen und Entfernen von KMS-Instanzen sowie das Einrichten einer Vertrauensstellung für den KMS.	vCenter Server-System	Cryptographer.ManageKeyServers
Schlüssel verwalten	Erlaubt Benutzern die Ausführung von Schlüsselverwaltungsvorgängen. Diese Vorgänge werden über den vSphere Client nicht unterstützt, können jedoch mit `crypto-util` oder der API ausgeführt werden.	vCenter Server-Root-Ordner	Cryptographer.ManageKeys

Tabelle 16-9. Rechte für Verschlüsselungsvorgänge (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Migrieren	Erlaubt Benutzern die Migration einer verschlüsselten virtuellen Maschine auf einen anderen ESXi-Host. Unterstützt die Migration mit bzw. ohne vMotion und Storage vMotion. Die Migration zu einer anderen vCenter Server-Instanz wird unterstützt.	Virtuelle Maschine	Cryptographer.Migrate
Erneut verschlüsseln	Erlaubt Benutzern die erneute Verschlüsselung von virtuellen Maschinen oder Festplatten mit einem anderen Schlüssel. Dieses Recht ist für detaillierte und oberflächliche erneute Verschlüsselungsvorgänge erforderlich.	Virtuelle Maschine	Cryptographer.Recrypt
VM registrieren	Erlaubt Benutzern die Registrierung einer verschlüsselten virtuellen Maschine bei einem anderen ESXi-Host.	Ordner der virtuellen Maschine	Cryptographer.RegisterVM

Tabelle 16-9. Rechte für Verschlüsselungsvorgänge (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Host registrieren	Erlaubt Benutzern die Aktivierung der Verschlüsselung auf einem Host. Die Verschlüsselung auf einem Host kann explizit oder bei der Erstellung der virtuellen Maschine aktiviert werden.	Hostordner für eigenständige Hosts, Cluster für Hosts im Cluster	Cryptographer.RegisterHost
KMS-Informationen lesen	Ermöglicht Benutzern die Auflistung von vSphere Native Key Providern auf dem vCenter Server und auf Hosts. Ermöglicht Benutzers außerdem, Informationen zum vSphere Native Key Provider abzurufen.	vCenter Server oder Host	Cryptographer.ReadKeyServersInfo

dvPort-Gruppenrechte

Rechte für verteilte virtuelle Portgruppen steuern die Fähigkeit, verteilte virtuelle Portgruppen zu erstellen, zu löschen und zu ändern.

In der Tabelle sind die Rechte beschrieben, die zum Erstellen und Konfigurieren von verteilten virtuellen Portgruppen erforderlich sind.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-10. Rechte für verteilte virtuelle Portgruppen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Erstellen	Ermöglicht das Erstellen einer verteilten virtuellen Portgruppe.	Virtuelle Portgruppen	DVPortgroup.Create
Löschen	Ermöglicht das Löschen einer verteilten virtuellen Portgruppe. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Virtuelle Portgruppen	DVPortgroup.Delete
Ändern	Ermöglicht das Ändern der Konfiguration einer verteilten virtuellen Portgruppe.	Virtuelle Portgruppen	DVPortgroup.Modify
Richtlinienvorgang	Ermöglicht das Festlegen der Richtlinien einer verteilten virtuellen Portgruppe.	Virtuelle Portgruppen	DVPortgroup.PolicyOp
Geltungsbereichsvorgang	Ermöglicht das Festlegen des Geltungsbereichs einer verteilten virtuellen Portgruppe.	Virtuelle Portgruppen	DVPortgroup.ScopeOp

Rechte für Distributed Switches

Rechte für Distributed Switches steuern die Fähigkeit, Aufgaben im Zusammenhang mit der Verwaltung von Distributed Switch-Instanzen durchzuführen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-11. Rechte für vSphere Distributed Switch

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Erstellen	Ermöglicht das Erstellen eines Distributed Switch.	Datencenter, Netzwerkordner	DVSwitch.Create
Löschen	Ermöglicht das Entfernen eines Distributed Switch. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Distributed Switches	DVSwitch.Delete
Hostvorgang	Ermöglicht das Ändern der Hostmitglieder eines Distributed Switch.	Distributed Switches	DVSwitch.HostOp
Ändern	Ermöglicht das Ändern der Konfiguration eines Distributed Switch.	Distributed Switches	DVSwitch.Modify
Verschieben	Ermöglicht das Verschieben eines vSphere Distributed Switch in einen anderen Ordner.	Distributed Switches	DVSwitch.Move
Network I/O Control-Vorgang	Ermöglicht das Ändern der Ressourceneinstellungen für einen vSphere Distributed Switch.	Distributed Switches	DVSwitch.ResourceManagement
Richtlinienvorgang	Ermöglicht das Ändern der Richtlinie eines vSphere Distributed Switch.	Distributed Switches	DVSwitch.PolicyOp
Portkonfigurationsvorgang	Ermöglicht das Ändern der Konfiguration eines Ports in einem vSphere Distributed Switch.	Distributed Switches	DVSwitch.PortConfig
Porteinstellungsvorgang	Ermöglicht das Ändern der Einstellung eines Ports in einem vSphere Distributed Switch.	Distributed Switches	DVSwitch.PortSetting
VSPAN-Vorgang	Ermöglicht das Ändern der VSPAN-Konfiguration eines vSphere Distributed Switch.	Distributed Switches	DVSwitch.Vspan

Rechte für Datencenter

Rechte für Datencenter steuern die Fähigkeit, Datencenter in der Bestandsliste des vSphere Client zu erstellen und zu bearbeiten.

Alle Rechte für Datencenter werden nur in vCenter Server verwendet. Das Recht **Datencenter erstellen** wird in Datencenterordnern oder im Stammobjekt definiert. Alle anderen Rechte für Datencenter werden mit Datencentern, Datencenterordnern oder dem Stammobjekt kombiniert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-12. Rechte für Datencenter

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Datencenter erstellen	Ermöglicht das Erstellen eines neuen Datencenters.	Datencenterordner oder Stammobjekt	Datacenter.Create
Datencenter verschieben	Ermöglicht das Verschieben eines Datencenters. Das Recht muss für Quelle und Ziel vorhanden sein.	Datencenter, Quelle und Ziel	Datacenter.Move
Konfiguration des Netzwerkprotokollprofils	Ermöglicht die Konfiguration des Netzwerkprofils für ein Datencenter.	Datencenter	Datacenter.IpPoolConfig
IP-Pool-Zuteilung abfragen	Ermöglicht die Konfiguration eines Pools von IP-Adressen.	Datencenter	Datacenter.IpPoolQueryAllocations
Datencenter neu konfigurieren	Ermöglicht die Neukonfiguration eines Datencenters.	Datencenter	Datacenter.Reconfigure
IP-Zuteilung freigeben	Ermöglicht die Freigabe der zugewiesenen IP-Zuteilung für ein Datencenter.	Datencenter	Datacenter.IpPoolReleaseIp
Datencenter entfernen	Ermöglicht das Entfernen eines Datencenters. Dieser Vorgang kann nur ausführt werden, wenn diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Datencenter und übergeordnetes Objekt	Datacenter.Delete
Datencenter umbenennen	Ermöglicht das Ändern des Namens eines Datencenters.	Datencenter	Datacenter.Rename
Carbon-Informationen des Datencenters aktualisieren	Ermöglicht das Erfassen von Metriken im Zusammenhang mit Energie- und Carbon-Messungen.	Datencenter	Datacenter.UpdateCarbonInfo

Berechtigungen für Datenspeicher

Rechte für Datenspeicher steuern die Fähigkeit, Datenspeicher zu durchsuchen, zu verwalten und Speicherplatz zuzuteilen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-13. Berechtigungen für Datenspeicher

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Speicher zuteilen	Ermöglicht die Zuteilung von Speicherplatz auf einem Datenspeicher für eine virtuelle Maschine, einen Snapshot, einen Klon oder eine virtuelle Festplatte.	Datenspeicher	Datastore.AllocateSpace
Datenspeicher durchsuchen	Ermöglicht die Suche nach Dateien in einem Datenspeicher.	Datenspeicher	Datastore.Browse
Datenspeicher-E/A-Verwaltung konfigurieren	Ermöglicht die Konfiguration von Storage I/O Control.	Datenspeicher	Datastore.ConfigIOManagement
Datenspeicher konfigurieren	Ermöglicht die Konfiguration eines Datenspeichers.	Datenspeicher	Datastore.Config
Dateivorgänge auf niedriger Ebene	Ermöglicht die Durchführung von Lese-, Schreib-, Lösch- und Umbenennungsvorgängen im Datenspeicherbrowser.	Datenspeicher	Datastore.FileManagement

Tabelle 16-13. Berechtigungen für Datenspeicher (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Datenspeicher verschieben	Ermöglicht das Verschieben eines Datenspeichers zwischen Ordnern. Das Recht muss für Quelle und Ziel vorhanden sein.	Datenspeicher, Quelle und Ziel	Datastore.Move
Datenspeicher entfernen	Ermöglicht das Entfernen eines Datenspeichers. Dieses Recht ist veraltet. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Datenspeicher	Datastore.Delete
Datei entfernen	Ermöglicht das Löschen von Dateien im Datenspeicher. Dieses Recht ist veraltet. Weisen Sie das Recht **Dateivorgänge auf niedriger Ebene** zu.	Datenspeicher	Datastore.DeleteFile
Datenspeicher umbenennen	Ermöglicht das Umbenennen eines Datenspeichers.	Datenspeicher	Datastore.Rename

Tabelle 16-13. Berechtigungen für Datenspeicher (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Dateien der virtuellen Maschine aktualisieren	Ermöglicht das Aktualisieren der Dateipfade der VM-Dateien auf einem Datenspeicher, nachdem der Datenspeicher neu signiert wurde.	Datenspeicher	Datastore.UpdateVirtualMachineFiles
Metadaten der virtuellen Maschine aktualisieren	Ermöglicht das Aktualisieren von Metadaten der virtuellen Maschine für einen Datenspeicher.	Datenspeicher	Datastore.UpdateVirtualMachineMetadata

Rechte für Datenspeicher-Cluster

Datenspeicher-Clusterrechte steuern die Konfiguration des Datenspeicher-Clusters für Speicher-DRS.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-14. Rechte für Datenspeicher-Cluster

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Datenspeicher-Cluster konfigurieren	Ermöglicht das Erstellen von und die Konfiguration von Einstellungen für Datenspeicher-Cluster für Speicher-DRS.	Datenspeicher-Cluster	StoragePod.Config

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 Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-15. ESX Agent Manager

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Konfigurieren	Ermöglicht die Bereitstellung einer virtuellen Maschine eines Agenten auf einem Host oder Cluster.	virtuelle Maschinen	EAM.Config
Ändern	Ermöglicht Änderungen an einer virtuellen Maschine eines Agenten, wie z. B. das Ausschalten oder Löschen der virtuellen Maschine.	virtuelle Maschinen	EAM.Modify
Anzeigen	Ermöglicht die Anzeige einer virtuellen Maschine eines Agenten.	virtuelle Maschinen	EAM.View

Rechte für Erweiterungen

Berechtigungen für Erweiterungen steuern die Fähigkeit, Erweiterungen zu installieren und zu verwalten.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-16. Rechte für Erweiterungen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Erweiterung registrieren	Ermöglicht die Registrierung einer Erweiterung (Plug-In).	Root-vCenter Server	Extension.Register
Registrierung der Erweiterung aufheben	Ermöglicht die Aufhebung der Registrierung einer Erweiterung (Plug-In).	Root-vCenter Server	Extension.Unregister
Erweiterung aktualisieren	Ermöglicht die Aktualisierung einer Erweiterung (Plug-In).	Root-vCenter Server	Extension.Update

Rechte für Bereitstellungsfunktion externer Statistiken

Rechte für die Bereitstellungsfunktion externer Statistiken steuern die Möglichkeit, vCenter Server über Statistiken des proaktiven Distributed Resource Scheduler (DRS) zu benachrichtigen.

Diese Rechte gelten für eine ausschließlich VMware-interne API.

Rechte für Ordner

Berechtigungen für Ordner steuern die Fähigkeit, Ordner zu erstellen und zu verwalten.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-17. Rechte für Ordner

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Ordner erstellen	Ermöglicht das Erstellen eines neuen Ordners.	Ordner	Folder.Create
Ordner löschen	Ermöglicht das Löschen eines Ordners. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Ordner	Folder.Delete

Tabelle 16-17. Rechte für Ordner (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Ordner verschieben	Ermöglicht das Verschieben eines Ordners. Das Recht muss für Quelle und Ziel vorhanden sein.	Ordner	Folder.Move
Ordner umbenennen	Ermöglicht das Ändern des Namens eines Ordners.	Ordner	Folder.Rename

Globale Rechte

Globale Rechte steuern globale Aufgaben im Zusammenhang mit Aufgaben, Skripts und Erweiterungen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-18. Globale Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Als vCenter Server agieren	Ermöglicht die Vorbereitung oder Initiierung eines vMotion-Sendevorgangs bzw. eines vMotion-Empfangsvorgangs.	Root-vCenter Server	Global.VCServer
Aufgabe abbrechen	Ermöglicht den Abbruch einer ausgeführten oder in der Warteschlange abgelegten Aufgabe.	Bestandslistenobjekt mit Bezug zur Aufgabe	Global.CancelTask
Kapazitätsplanung	Ermöglicht die Aktivierung der Nutzung der Kapazitätsplanung für die Planung der Konsolidierung physischer Maschinen auf virtuelle Maschinen.	Root-vCenter Server	Global.CapacityPlanning
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.Diagnostics

Tabelle 16-18. Globale Rechte (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Methoden deaktivieren	Ermöglicht Servern für vCenter Server-Erweiterungen das Deaktivieren bestimmter Vorgänge für Objekte, die von vCenter Server verwaltet werden.	Root-vCenter Server	Global.DisableMethods
Methoden aktivieren	Ermöglicht Servern für vCenter Server-Erweiterungen das Aktivieren bestimmter Vorgänge für Objekte, die von vCenter Server verwaltet werden.	Root-vCenter Server	Global.EnableMethods
Global-Tag	Ermöglicht das Hinzufügen oder Entfernen von Global-Tags.	Root-Host oder vCenter Server	Global.GlobalTag
Zustand	Ermöglicht das Anzeigen des Status der vCenter Server-Komponenten.	Root-vCenter Server	Global.Health
Lizenzen	Ermöglicht das Anzeigen installierter Lizenzen und das Hinzufügen bzw. Entfernen von Lizenzen.	Root-Host oder vCenter Server	Global.Licenses
Ereignis protokollieren	Ermöglicht das Protokollieren eines benutzerdefinierten Ereignisses für ein bestimmtes verwaltetes Element.	Beliebiges Objekt	Global.LogEvent
Benutzerdefinierte Attribute verwalten	Ermöglicht das Hinzufügen, Entfernen oder Umbenennen von benutzerdefinierten Felddefinitionen.	Root-vCenter Server	Global.ManageCustomFields
Proxy	Ermöglicht Zugriff auf eine interne Schnittstelle für das Hinzufügen oder Entfernen von Endpunkten zu oder vom Proxy.	Root-vCenter Server	Global.Proxy
Skriptaktion	Ermöglicht das Planen einer Skriptaktion zusammen mit einem Alarm.	Beliebiges Objekt	Global.ScriptAction
Dienst-Manager	Ermöglicht die Verwendung des `resxtop` Befehls in ESXCLI.	Root-Host oder vCenter Server	Global.ServiceManagers
Benutzerdefinierte Attribute festlegen	Ermöglicht das Anzeigen, Erstellen oder Entfernen benutzerdefinierter Attribute für ein verwaltetes Objekt.	Beliebiges Objekt	Global.SetCustomField

Tabelle 16-18. Globale Rechte (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Einstellungen	Ermöglicht das Lesen und Ändern von vCenter Server-Konfigurationseinstellungen zur Laufzeit.	Root-vCenter Server	Global.Settings
System-Tag	Ermöglicht das Hinzufügen oder Entfernen von System-Tags.	Root-vCenter Server	Global.SystemTag

Interaktion mit den Gastdaten-Veröffentlichungsrechten

Interagieren Sie mit den Gastdaten-Veröffentlichungsrechten, um den Zugriff auf die veröffentlichten Gastdaten auf dem HOST-GDP-Dienst zu steuern.

Tabelle 16-19. Interaktion mit den Gastdaten-Veröffentlichungsrechten

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Abonnieren des Gastdaten-Veröffentlichungsdienstes auf ESX-Hosts	Ermöglicht den Zugriff auf die veröffentlichten Gastdaten auf dem Host-GDP-Dienst.	Hosts	GuestDataPublisher.GetData

Rechte für den verknüpften Hybridmodus

Rechte für den verknüpften Hybridmodus steuern Aspekte der Verknüpfung Ihrer Cloud-vCenter Server-Instanz mit einer lokalen vCenter Single Sign-On-Domäne. (Gilt für VMware Cloud on AWS.)

Tabelle 16-20. Rechte für den verknüpften Hybridmodus

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Erstellen	Ermöglicht den vollständigen Administratorzugriff zum Erstellen und Löschen von Communitys.	SDDC	HLM.Create
Verwalten	Ermöglicht das Erstellen einer Vertrauensstellung für Quellen und den Zugriff auf Communitys (Leseebene).	SDDC	HLM.Manage

Rechte für Bereitstellungsfunktion für Aktualisierungen des Systemzustands

Rechte für die Bereitstellungsfunktion für Aktualisierungen des Systemzustands steuern die Möglichkeit für Hardwareanbieter, vCenter Server über Proactive HA-Ereignisse zu benachrichtigen.

Diese Rechte gelten für eine ausschließlich VMware-interne API.

Host-CIM-Rechte

Host-CIM-Rechte steuern die Verwendung von CIM für die Statusüberwachung des Hosts.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-21. Host-CIM-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **CIM** ■ **CIM-Interaktion**	Ermöglicht es einem Client, ein Ticket für CIM-Dienste abzurufen.	Hosts	Host.Cim.CimInteraction

Rechte für die Hostkonfiguration

Rechte für die Hostkonfiguration steuern die Fähigkeit, Hosts zu konfigurieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-22. Rechte für die Hostkonfiguration

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Konfiguration** ■ **Erweiterte Einstellungen**	Ermöglicht das Festlegen erweiterter Optionen für die Hostkonfiguration.	Hosts	Host.Config.AdvancedConfig
■ **Konfiguration** ■ **Authentifizierungsspeicher**	Ermöglicht das Konfigurieren von Active Directory-Authentifizierungsspeichern.	Hosts	Host.Config.AuthenticationStore

Tabelle 16-22. Rechte für die Hostkonfiguration (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Konfiguration** ■ **PciPassthru-Einstellungen ändern**	Ermöglicht Änderungen an den PciPassthru-Einstellungen eines Hosts.	Hosts	Host.Config.PciPassthru
■ **Konfiguration** ■ **SNMP-Einstellungen ändern**	Ermöglicht Änderungen an den SNMP-Einstellungen eines Hosts.	Hosts	Host.Config.Snmp
■ **Konfiguration** ■ **Datums- und Uhrzeiteinstellungen ändern**	Ermöglicht das Ändern der Datums- und Uhrzeiteinstellungen auf dem Host.	Hosts	Host.Config.DateTime
■ **Konfiguration** ■ **Einstellungen ändern**	Ermöglicht das Einstellen des Sperrmodus auf ESXi-Hosts.	Hosts	Host.Config.Settings
■ **Konfiguration** ■ **Verbindung**	Ermöglicht Änderungen am Verbindungsstatus eines Hosts („Verbunden“ oder „Nicht verbunden“).	Hosts	Host.Config.Connection
■ **Konfiguration** ■ **Firmware**	Ermöglicht Updates der Firmware des ESXi-Hosts.	Hosts	Host.Config.Firmware
■ **Konfiguration** ■ **GuestStore-Einstellungen**	Ermöglicht Änderungen am GuestStore.	GuestStore-Repository	Host.Config.GuestStore
■ **Konfiguration** ■ **Hyper-Threading**	Ermöglicht das Aktivieren und Deaktivieren von Hyper-Threading in einem Host-CPU-Scheduler.	Hosts	Host.Config.HyperThreading
■ **Konfiguration** ■ **Image-Konfiguration**	Ermöglicht Änderungen am Image, das einem Host zugeordnet ist.		Host.Config.Image
■ **Konfiguration** ■ **Wartung**	Ermöglicht das Aktivieren bzw. Deaktivieren des Wartungsmodus für den Host sowie das Herunterfahren und Neustarten des Hosts.	Hosts	Host.Config.Maintenance
■ **Konfiguration** ■ **Arbeitsspeicherkonfiguration**	Ermöglicht Änderungen an der Hostkonfiguration.	Hosts	Host.Config.Memory
■ **Konfiguration** ■ **NVDIMM**	Ermöglicht das Lesen und Konfigurieren von nichtflüchtigen DIMMs.	Hosts	Host.Config.Nvdimm

Tabelle 16-22. Rechte für die Hostkonfiguration (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Konfiguration** ■ **Netzwerkkonfiguration**	Ermöglicht das Konfigurieren von Netzwerk, Firewall und vMotion-Netzwerk.	Hosts	Host.Config.Network
■ **Konfiguration** ■ **Betrieb**	Ermöglicht das Konfigurieren der Energieverwaltungseinstellungen des Hosts.	Hosts	Host.Config.Power
■ **Konfiguration** ■ **ProductLocker-Einstellungen**	Ermöglicht die Konfiguration des ESXi-Ordners „productlocker“.	Hosts	Host.Config.ProductLocker
■ **Konfiguration** ■ **Quarantäne**	Ermöglicht das Versetzen eines Hosts in den Quarantänemodus.	Hosts	Host.Config.Quarantine
■ **Konfiguration** ■ **Patch abfragen**	Ermöglicht das Abfragen installierbarer Patches und das Installieren von Patches auf dem Host.	Hosts	Host.Config.Patch
■ **Konfiguration** ■ **Sicherheitsprofil und Firewall**	Ermöglicht das Konfigurieren von Internetdiensten wie SSH, Telnet, SNMP und Hostfirewall.	Hosts	Host.Config.NetService
■ **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.Config.Storage
■ **Konfiguration** ■ **System-Management**	Ermöglicht Erweiterungen eine Änderung des Dateisystems auf dem Host.	Hosts	Host.Config.SystemManagement

Tabelle 16-22. Rechte für die Hostkonfiguration (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Konfiguration** ■ **Systemressourcen**	Ermöglicht das Aktualisieren der Konfiguration der Systemressourcenhierarchie.	Hosts	Host.Config.Resources
■ **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	Host.Config.AutoStart

Host-Entropie-Pool-Rechte

Host-Entropie-Pool-Rechte steuern die Fähigkeit, ESXi-Host-Entropie anzuzeigen und hinzuzufügen.

Tabelle 16-23. Host-Entropie-Pool-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Entropie-Pool** ■ **Lesen**	Ermöglicht das Lesen der Host-Entropie-Pool-Informationen.	Hosts	Host.Entropy.Read
■ **Entropie-Pool** ■ **Schreiben**	Ermöglicht das Hinzufügen von Entropie zum Host-Entropie-Pool.	Hosts	Host.Entropy.Write

Intel Software Guard Extensions-Hostrechte

Intel Software Guard Extensions-Hostrechte steuern Aspekte des Remote-Nachweises auf ESXi-Multi-Socket-Hosts.

Tabelle 16-24. Intel Software Guard Extensions (SGX) – Hostberechtigungen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Intel Software Guard Extensions (SGX)** ■ **Intel Software Guard Extensions (SGX) – Host registrieren**	Ermöglicht die Registrierung von Hosts mit dem Intel SGX-Registrierungsdienst (damit SGX-Arbeitslasten den Remote-Nachweis von SGX durchführen können, wenn sie auf SGX-fähigen Hosts mit mehreren Sockets ausgeführt werden).	Hosts	Host.Sgx.Register

Rechte für die Hostbestandsliste

Rechte für die Hostbestandsliste steuern das Hinzufügen von Hosts zur Bestandsliste, das Hinzufügen von Hosts zu Clustern und das Verschieben von Hosts in der Bestandsliste.

In der Tabelle sind die Rechte beschrieben, die zum Hinzufügen und Verschieben von Hosts und Clustern in der Bestandsliste erforderlich sind.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-25. Rechte für die Hostbestandsliste

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Bestandsliste** ■ **Host zu Cluster hinzufügen**	Ermöglicht das Hinzufügen eines Hosts zu einem vorhandenen Cluster.	Cluster	Host.Inventory.AddHostToCluster
■ **Bestandsliste** ■ **Eigenständigen Host hinzufügen**	Ermöglicht das Hinzufügen eines eigenständigen Hosts.	Hostordner	Host.Inventory.AddStandaloneHost
■ **Bestandsliste** ■ **Cluster erstellen**	Ermöglicht das Erstellen eines neuen Clusters.	Hostordner	Host.Inventory.CreateCluster
■ **Bestandsliste** ■ **Clusterlebenszyklus verwalten**	Ermöglicht die Verwaltung des Clusters.	Cluster	Host.Inventory.ManageClusterLifecyle
■ **Bestandsliste** ■ **Cluster ändern**	Ermöglicht das Ändern der Eigenschaften eines Clusters.	Cluster	Host.Inventory.EditCluster

Tabelle 16-25. Rechte für die Hostbestandsliste (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **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.Inventory.MoveCluster
■ **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.Inventory.MoveHost
■ **Bestandsliste** ■ **Cluster entfernen**	Ermöglicht das Löschen eines Clusters oder eines eigenständigen Hosts. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Cluster, Server	Host.Inventory.DeleteCluster
■ **Bestandsliste** ■ **Host entfernen**	Ermöglicht das Entfernen eines Hosts. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Hosts und übergeordnetes Objekt	Host.Inventory.RemoveHostFromCluster
■ **Bestandsliste** ■ **Cluster umbenennen**	Ermöglicht das Umbenennen eines Clusters.	Cluster	Host.Inventory.RenameCluster

Rechte für lokale Hostoperationen

Rechte für lokale Hostoperationen steuern Aktionen, die bei einer Direktverbindung zwischen dem VMware Host Client und einem Host durchgeführt werden.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-26. Rechte für lokale Hostoperationen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Lokale Vorgänge** ■ **Host zu vCenter hinzufügen**	Ermöglicht die Installation und das Entfernen von vCenter-Agenten (z. B. vpxa und aam) auf einem Host.	Root-Host	Host.Local.InstallAgent
■ **Lokale Vorgänge** ■ **Virtuelle Maschine erstellen**	Ermöglicht es, eine neue virtuelle Maschine auf einer Festplatte von Grund auf zu erstellen, ohne diese auf dem Host zu registrieren.	Root-Host	Host.Local.CreateVM
■ **Lokale Vorgänge** ■ **Virtuelle Maschine löschen**	Ermöglicht das Löschen einer virtuellen Maschine auf einer Festplatte. Wird für registrierte und nicht registrierte virtuelle Maschinen unterstützt.	Root-Host	Host.Local.DeleteVM
■ **Lokale Vorgänge** ■ **Benutzergruppen verwalten**	Ermöglicht die Verwaltung lokaler Konten auf einem Host.	Root-Host	Host.Local.ManageUserGroups
■ **Lokale Vorgänge** ■ **Virtuelle Maschine neu konfigurieren**	Ermöglicht die erneute Konfiguration einer virtuellen Maschine.	Root-Host	Host.Local.ReconfigVM

Host-Statistikrechte

Host-Statistikrechte steuern die Fähigkeit, auf statistische Informationen von einer Datenverarbeitungseinheit (DPU) zuzugreifen.

Diese Rechte gelten für eine ausschließlich VMware-interne API.

Trusted Platform Module (TPM)-Hostrechte

Trusted Platform Module (TPM)-Hostrechte steuern Vorgänge im Zusammenhang mit der Verwaltung von TPM-Chips (Trusted Platform Module).

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-27. Trusted Platform Module (TPM)-Hostrechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Trusted Platform Module** ■ **Lesen** ■ **Versiegelung aufheben**	**Lesen** ermöglicht das Lesen detaillierter Informationen über den Status des auf dem ESXi-Host installierten TPM. **Versiegelung aufheben** ermöglicht das Anfordern eines ESXi-Hosts zum Entschlüsseln einer Herausforderung, um ihren Status zu beweisen.	Hosts	Host.Tpm.Read Host.Tpm.Unseal

vSphere Replication-Rechte von Hosts

vSphere Replication-Rechte von Hosts steuern die Verwendung der VM-Replizierung durch VMware vCenter Site Recovery Manager™ für einen Host.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-28. vSphere Replication-Rechte von Hosts

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **vSphere Replication** ■ **Replizierung verwalten**	Ermöglicht die Verwaltung der Replizierung virtueller Maschinen auf diesem Host.	Hosts	Host.Hbr.HbrManagement

Hostprofil-Berechtigungen

Hostprofil-Rechte steuern Vorgänge im Zusammenhang mit dem Erstellen und Ändern von Hostprofilen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-29. Hostprofil-Berechtigungen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Bereinigen	Ermöglicht das Löschen von Informationen zu Profilen.	Root-vCenter Server	Profile.Clear
Erstellen	Ermöglicht das Erstellen eines Hostprofils.	Root-vCenter Server	Profile.Create
Löschen	Ermöglicht das Löschen eines Hostprofils.	Root-vCenter Server	Profile.Delete
Bearbeiten	Ermöglicht das Bearbeiten eines Hostprofils.	Root-vCenter Server	Profile.Edit
Exportieren	Ermöglicht das Exportieren eines Hostprofils.	Root-vCenter Server	Profile.Export
Anzeigen	Ermöglicht das Anzeigen eines Hostprofils.	Root-vCenter Server	Profile.View

vCenter Server-Profilrechte

vCenter Server-Profilrechte steuern Aspekte beim Auflisten von Profilen sowie beim Exportieren und Importieren von Konfigurationen von einem vCenter Server in einen anderen.

Tabelle 16-30. vCenter Server-Profilrechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Leserechte für vCenter Server-Profile	Ermöglicht das Auflisten und Exportieren von vCenter Server-Profilen.	vCenter Server	Infraprofile.Read
Schreibrechte für vCenter Server-Profile	Ermöglicht das Importieren eines Profils in einen anderen vCenter Server und dessen Validierung.	vCenter Server	Infraprofile.Write

vSphere Namespaces-Rechte

Mit Berechtigungen für Namespaces wird gesteuert, wer VMware vSphere® mit VMware Tanzu™-Namespaces erstellen und verwalten kann.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-31. Berechtigungen für Namespaces

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Lässt Vorgänge zur Außerbetriebnahme von Festplatten zu	Ermöglicht die Außerbetriebnahme von Datenspeichern.	Datenspeicher	Namespaces.ManageDisks
Dateien der Arbeitslastkomponente sichern	Ermöglicht das Sichern der Inhalte des etcd-Clusters (wird nur in VMware Cloud on AWS verwendet).	Cluster	Namespaces.Backup
Verfügbare Namespaces auflisten	Ermöglicht das Auflisten der zugänglichen Namespaces.	Cluster	Namespaces.ListAccess
Clusterweite Konfiguration ändern	Ermöglicht das Ändern der clusterweiten Konfiguration sowie das Aktivieren und Deaktivieren von Cluster-Namespaces.	Cluster	Namespaces.Manage
Clusterweite Namespace-Self-Service-Konfiguration ändern	Ermöglicht das Ändern der Namespace-Self-Service-Konfiguration.	Cluster (zum Aktivieren und Deaktivieren) Vorlagen (zum Ändern der Konfiguration) vCenter Server (zum Erstellen einer Vorlage)	Namespaces.SelfServiceManage
Namespace-Konfiguration ändern	Ermöglicht das Ändern der Optionen für die Namespace-Konfiguration, wie z. B. Ressourcenzuteilung und Benutzerberechtigungen.	Cluster	Namespaces.Configure

Tabelle 16-31. Berechtigungen für Namespaces (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Clusterfunktionen umschalten	Ermöglicht die Änderung des Status von Clusterfunktionen (wird intern nur für VMware Cloud on AWS verwendet).	Cluster	Namespaces.ManageCapabilities
Upgrade von Clustern auf neuere Versionen durchführen	Ermöglicht die Initiierung des Cluster-Upgrades.	Cluster	Namespaces.Upgrade

Netzwerkberechtigungen

Rechte für Netzwerk steuern Aufgaben im Zusammenhang mit der Netzwerkverwaltung.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-32. Netzwerkberechtigungen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Netzwerk zuweisen	Ermöglicht das Zuweisen eines Netzwerks zu einer virtuellen Maschine.	Netzwerke, virtuelle Maschinen	Network.Assign
Konfigurieren	Ermöglicht das Konfigurieren eines Netzwerks.	Netzwerke, virtuelle Maschinen	Network.Config
Netzwerk verschieben	Ermöglicht das Verschieben eines Netzwerks zwischen Ordnern. Das Recht muss für Quelle und Ziel vorhanden sein.	Netzwerke	Network.Move
Entfernen	Ermöglicht das Entfernen eines Netzwerks. Dieses Recht ist veraltet. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Netzwerke	Network.Delete

NSX-Rechte

NSX-Rechte steuern Aufgaben im Zusammenhang mit der NSX-Verwaltung.

Tabelle 16-33. NSX-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
NSX-Konfiguration lesen	Ermöglicht das Lesen von NSX-Objekten.	NSX	Nsx.Read
NSX-Konfiguration verwalten	Ermöglicht die Verwaltung von NSX-Objekten aus der Perspektive eines vSphere-Administrators.	NSX	Nsx.Manage
NSX-Konfiguration ändern	Ermöglicht die Verwaltung von NSX-Objekten aus der Perspektive eines Unternehmensadministrators.	NSX	Nsx.ModifyAll

VMware Observability-Rechte

VMware Observability-Rechte steuern die Fähigkeit eines Agenten, auf die Observability-APIs in vCenter Server zuzugreifen.

Diese Rechte gelten für eine ausschließlich VMware-interne API.

OvfManager-Rechte

OvfManager-Rechte steuern die Fähigkeit, auf vService Manager zuzugreifen.

Diese Rechte gelten für eine ausschließlich VMware-interne API.

Rechte für die Interaktion mit Partner-REST-Daemons

Die Rechte für die Interaktion mit Partner-REST-Daemons steuern den Zugriff auf Lese- und Schreibvorgänge.

Tabelle 16-34. Rechte für die Interaktion mit Partner-REST-Daemons

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
GET-Vorgang über den REST-Daemon eines Partners ausführen	Ermöglicht dem vom Partner bereitgestellten REST-Client die Durchführung von GET-Vorgängen.	Der Benutzer des Partners, der GET-Vorgänge durchführt.	PartnerRestDaemon.Read
Änderungsvorgang am REST-Daemon eines Partners durchführen	Ermöglicht dem vom Partner bereitgestellten REST-Client die Durchführung von POST-, PUT- und DELETE-Vorgängen.	Der Benutzer des Partners, der POST-, PUT- oder DELETE-Vorgänge durchführt.	PartnerRestDaemon.Write

Leistungsrechte

Leistungsrechte steuern das Ändern von Einstellungen für Leistungsstatistiken.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-35. Leistungsrechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Intervalle ändern	Ermöglicht das Erstellen, Entfernen und Aktualisieren von Intervallen zum Sammeln von Leistungsdaten.	Root-vCenter Server	Performance.ModifyIntervals

Plug-In-Rechte

Plug-In-Rechte steuern die Verwaltung von vSphere Client-Plug-Ins.

Tabelle 16-36. Plug-In-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Plug-Ins verwalten	Ermöglicht die Verwaltung von vSphere Client-Plug-Ins.	vCenter Server	Plugin.Management

Rechte für die Replizierung als Dienst

Die Rechte für die Replizierung als Dienst steuern den Zugriff auf verschiedene interne APIs und Funktionen im Zusammenhang mit der vCenter Server-Verknüpfung.

Diese Rechte gelten für eine ausschließlich VMware-interne API.

Rechte für Berechtigungen

Berechtigungsrechte steuern das Zuweisen von Rollen und Berechtigungen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-37. Rechte für Berechtigungen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Berechtigung ändern	Ermöglicht das Definieren einer oder mehrerer Berechtigungsregeln für eine Instanz oder das Aktualisieren von Regeln, wenn diese für einen bestimmten Benutzer oder eine bestimmte Gruppe der Instanz bereits vorhanden sind. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Beliebiges Objekt und übergeordnetes Objekt	Authorization.ModifyPermissions
Recht ändern	Ermöglicht das Ändern der Gruppe oder Beschreibung eines Rechts. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	Beliebiges Objekt	Authorization.ModifyPrivileges
Rolle ändern	Ermöglicht das Aktualisieren des Namens einer Rolle und der mit der Rolle verbundenen Rechte.	Beliebiges Objekt	Authorization.ModifyRoles

Tabelle 16-37. Rechte für Berechtigungen (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
vTContainer ändern	Ermöglicht das Erstellen, Aktualisieren und Löschen von vTContainer-Instanzen.	vTContainer-Objekte	Authorization.ModifyVTContainers
vTContainer-Zuordnungen ändern	Ermöglicht das Erstellen und Löschen einer vTContainer-Zuordnung.	vTContainer-Zuordnungsobjekte	Authorization.ModifyVTContainerMappings
Rollenberechtigungen neu zuweisen	Ermöglicht das Zuweisen aller Berechtigungen einer Rolle zu einer anderen Rolle.	Beliebiges Objekt	Authorization.ReassignRolePermissions

Rechte für VM-Speicherrichtlinien

VM-Speicherrechte steuern Vorgänge im Zusammenhang mit Speicherprofilen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-38. Rechte für VM-Speicher

Rechtename	Beschreibung	Erforderlich bei	Rechtename in der API
VM-Speicherrichtlinien aktualisieren	Ermöglicht Änderungen an Speicherprofilen wie das Erstellen und Aktualisieren von Speicherfunktionen und Speicherprofilen für virtuelle Maschinen.	Root-vCenter Server	StorageProfile.Update
VM-Speicherrichtlinien anzeigen	Ermöglicht die Anzeige von definierten Storage Capabilities und Speicherprofilen.	Root-vCenter Server	StorageProfile.View

Rechte für Ressourcen

Rechte für Ressourcen steuern die Erstellung und Verwaltung von Ressourcenpools sowie die Migration von virtuellen Maschinen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-39. Rechte für Ressourcen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Empfehlung anwenden	Ermöglicht das Akzeptieren eines Vorschlags des Servers zum Ausführen einer Migration mit vMotion.	Cluster	Resource.ApplyRecommendation
vApp dem Ressourcenpool zuweisen	Ermöglicht die Zuweisung einer vApp zu einem Ressourcenpool.	Ressourcenpools	Resource.AssignVAppToPool
Virtuelle Maschine zu Ressourcenpool zuweisen	Ermöglicht die Zuweisung einer virtuellen Maschine zu einem Ressourcenpool.	Ressourcenpools	Resource.AssignVMToPool
Ressourcenpool erstellen	Ermöglicht die Erstellung von Ressourcenpools.	Ressourcenpools, Cluster	Resource.CreatePool
Ausgeschaltete virtuelle Maschine migrieren	Ermöglicht die Migration einer ausgeschalteten virtuellen Maschine auf einen anderen Ressourcenpool oder Host.	virtuelle Maschinen	Resource.ColdMigrate
Eingeschaltete virtuelle Maschine migrieren	Ermöglicht die Migration mithilfe von vMotion einer eingeschalteten virtuellen Maschine auf einen anderen Ressourcenpool oder Host.	virtuelle Maschinen	Resource.HotMigrate
Ressourcenpool ändern	Ermöglicht Änderungen an den Zuweisungen eines Ressourcenpools.	Ressourcenpools	Resource.EditPool
Ressourcenpool verschieben	Ermöglicht das Verschieben eines Ressourcenpools. Das Recht muss für Quelle und Ziel vorhanden sein.	Ressourcenpools	Resource.MovePool
vMotion abfragen	Ermöglicht die Abfrage der allgemeinen vMotion-Kompatibilität einer virtuellen Maschine mit einer Hostgruppe.	Root-vCenter Server	Resource.QueryVMotion

Tabelle 16-39. Rechte für Ressourcen (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Ressourcenpool entfernen	Ermöglicht das Löschen eines Ressourcenpools. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Ressourcenpools	Resource.DeletePool
Ressourcenpool umbenennen	Ermöglicht das Umbenennen eines Ressourcenpools.	Ressourcenpools	Resource.RenamePool

Rechte für geplante Aufgaben

Rechte für geplante Aufgaben steuern das Erstellen, Bearbeiten und Entfernen von geplanten Aufgaben.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-40. Rechte für geplante Aufgaben

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Aufgaben erstellen	Ermöglicht die Planung einer Aufgabe. Wird zusätzlich zu den Rechten zum Ausführen der geplanten Aktion zum Planungszeitpunkt benötigt.	Beliebiges Objekt	ScheduledTask.Create
Aufgabe ändern	Ermöglicht die Neukonfiguration der Eigenschaften der geplanten Aufgabe.	Beliebiges Objekt	ScheduledTask.Edit

Tabelle 16-40. Rechte für geplante Aufgaben (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Aufgabe entfernen	Ermöglicht das Entfernen einer geplanten Aufgabe aus der Warteschlange.	Beliebiges Objekt	ScheduledTask.Delete
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	ScheduledTask.Run

Sitzungsrechte

Sitzungsrechte steuern die Fähigkeit von Erweiterungen, Sitzungen auf dem vCenter Server-System zu öffnen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis Weisen Sie Sitzungsberechtigungen nur Administratoren oder vertrauenswürdigen Benutzern zu.

Tabelle 16-41. Sitzungsrechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Benutzeridentität annehmen	Ermöglicht die Imitation eines anderen Benutzers. Diese Funktion wird von Erweiterungen verwendet.	Root-vCenter Server	Sessions.ImpersonateUser
Meldung	Ermöglicht das Festlegen der globalen Anmeldenachricht.	Root-vCenter Server	Sessions.GlobalMessage
Sitzung überprüfen	Ermöglicht die Überprüfung der Sitzungsgültigkeit.	Root-vCenter Server	Sessions.ValidateSession

Tabelle 16-41. Sitzungsrechte (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Sitzungen anzeigen und beenden	Ermöglicht das Anzeigen von Sitzungen und das Erzwingen der Abmeldung der angemeldeten Benutzer.	Root-vCenter Server	Sessions.TerminateSession
privilege.StorageProfile.ViewPermissions.label	Ermöglicht das Erfassen von Sitzungen.	Root-vCenter Server	Sessions.CollectPrivilegeChecks

Speicheransichtsberechtigungen

Speicheransichtsberechtigungen bestimmen die Rechte für Speicherüberwachungsdienst-APIs.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-42. Speicheransichtsberechtigungen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Dienst konfigurieren	Erlaubt berechtigten Benutzern die Verwendung aller Speicherüberwachungsdienst-APIs. Verwenden Sie **Speicheransichten.Anzeigen** für Rechte bezüglich schreibgeschützter Speicherüberwachungsdienst-APIs.	Root-vCenter Server	StorageViews.ConfigureService
Anzeigen	Erlaubt berechtigten Benutzern die Verwendung schreibgeschützter Speicherüberwachungsdienst-APIs.	Root-vCenter Server	StorageViews.View

Rechte für Supervisor-Dienste

Rechte für Supervisor-Dienste steuern, wer Supervisor-Dienste in der vSphere with Tanzu-Umgebung erstellen und verwalten kann.

Tabelle 16-43. Rechte für Supervisor-Dienste

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Supervisor-Dienste verwalten	Ermöglicht das Erstellen, Aktualisieren oder Löschen eines Supervisor-Diensts. Darüber hinaus können Sie einen Supervisor-Dienst auf einem Cluster installieren und eine Supervisor-Dienstversion erstellen oder löschen.	Cluster	SupervisorServices.Manage

Rechte für Aufgaben

Rechte für Aufgaben steuern die Fähigkeit von Erweiterungen, Aufgaben für vCenter Server zu erstellen und zu aktualisieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-44. Rechte für Aufgaben

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Aufgabe erstellen	Erlaubt einer Erweiterung die Erstellung einer benutzerdefinierten Aufgabe. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	Root-vCenter Server	Task.Create
Aufgabe aktualisieren	Erlaubt einer Erweiterung die Aktualisierung einer benutzerdefinierten Aufgabe. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	Root-vCenter Server	Task.Update

Mandantenmanagerrechte

Mandantenmanagerrechte steuern Aspekte des Definierens und Abrufens von Mandantenverwaltungsentitäten. (Gilt für VMware Cloud on AWS)

Tabelle 16-45. Mandantenmanagerrechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Bereitstellungsvorgänge für Mandant	Ermöglicht das Definieren eines Satzes von Ressourcen für die Mandantenverwaltung.	Root-Ordner und jede Entität, die derzeit als Dienstanbieter markiert ist.	TenantManager.Update
Abfragevorgänge für Mandant	Ermöglicht das Abrufen der Liste der Mandantenverwaltungsressourcen.	Root-Ordner und jede Entität, die derzeit als Dienstanbieter markiert ist.	TenantManager.Query

Transfer Service-Rechte

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

Rechte für VcTrusts/VcIdentity

Mit den Rechten für VcTrusts/VcIdentity wird der Zugriff auf verschiedene interne APIs und Funktionen im Zusammenhang mit der Vertrauensstellung zwischen vCenter Server-Systemen gesteuert.

Tabelle 16-46. Rechte für VcTrusts/VcIdentity

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Erstellen/Aktualisieren/ Löschen (Administratorrechte)	Ermöglicht den Vollzugriff auf Administratorebene auf verschiedene interne APIs und Funktionen im Zusammenhang mit der Vertrauensstellung zwischen vCenter Server-Systemen.	Nicht verfügbar	Trust.Administer
Erstellen/Aktualisieren/ Löschen (unter Administratorrechte)	Ermöglicht verringerten Administratorzugriff auf verschiedene interne APIs und Funktionen im Zusammenhang mit der Vertrauensstellung zwischen vCenter Server-Systemen. Mit diesem Recht wird das Erstellen/ Aktualisieren/Löschen von VcTrusts/VcIdentity so eingeschränkt, dass der Benutzer Nicht-Administratorrechte nicht eskalieren kann.	Nicht verfügbar	Trust.Manage

Rechte für „Administrator der vertrauenswürdigen Infrastruktur“

Die Rechte für „Administrator der vertrauenswürdigen Infrastruktur“ beziehen sich auf das Konfigurieren und Verwalten einer vSphere Trust Authority-Bereitstellung..

Diese Rechte bestimmen, wer Konfigurations- und Verwaltungsaufgaben für eine vSphere Trust Authority-Bereitstellung durchführen kann. Weitere Informationen zur Trust Authority-Rolle und zur Gruppe „TrustedAdmins“ finden Sie unter Voraussetzungen und notwendige Berechtigungen für vSphere Trust Authority.

Tabelle 16-47. Rechte für „Administrator der vertrauenswürdigen Infrastruktur“

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Vertrauensstellung des Schlüsselservers konfigurieren	Ermöglicht das Verwalten der Schlüsselanbieter des Schlüsselanbieterdiensts.	Root-vCenter Server	TrustedAdmin.ManageKMSTrust
TPM-Zertifikate des vertrauenswürdigen Autoritätshosts konfigurieren	Ermöglicht das Erstellen und Ändern der Einstellungen des Nachweisdiensts.	Root-vCenter Server	TrustedAdmin.ConfigureHostCertificates
Metadaten des vertrauenswürdigen Autoritätshosts konfigurieren	Ermöglicht das Bearbeiten der Basisimages, die durch den Nachweisdienst bestätigt werden.	Root-vCenter Server	TrustedAdmin.ConfigureHostMetadata
Nachweis-SSO konfigurieren	Ermöglicht das Bearbeiten der Hosts, denen die Trust Authority-Hosts vertrauen können.	Root-vCenter Server	TrustedAdmin.ManageAttestingSSO
Token-Konvertierungsrichtlinie konfigurieren	Ermöglicht die Konfiguration der Token-Konvertierungsrichtlinie.	Root-vCenter Server	TrustedAdmin.ConfigureTokenConversionPolicy
Hosts der vertrauenswürdigen Infrastruktur auflisten	Ermöglicht das Lesen von Informationen bezüglich der vertrauenswürdigen Hosts und der Trust Authority-Hosts.	Root-vCenter Server	TrustedAdmin.ReadTrustedHosts
Informationen zu STS auflisten	Ermöglicht das Exportieren der Details des vertrauenswürdigen Hosts, sodass sie in den Trust Authority-Cluster importiert werden können.	Root-vCenter Server	TrustedAdmin.ReadStsInfo

Tabelle 16-47. Rechte für „Administrator der vertrauenswürdigen Infrastruktur“ (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Hosts der vertrauenswürdigen Infrastruktur verwalten	Ermöglicht das Bearbeiten der Informationen zu den vertrauenswürdigen Hosts und den Trust Authority-Hosts.	Root-vCenter Server	TrustedAdmin.ManageTrustedHosts
Vertrauensstellung des Schlüsselservers lesen	Ermöglicht das Lesen der Schlüsselanbieter des Schlüsselanbieterdiensts.	Root-vCenter Server	TrustedAdmin.ReadKMSTrust
Nachweis-SSO lesen	Ermöglicht das Lesen, welchen Hosts die Trust Authority-Hosts vertrauen können.	Root-vCenter Server	TrustedAdmin.ReadAttestingSSO
TPM-Zertifikate des vertrauenswürdigen Autoritätshosts abrufen	Ermöglicht das Lesen der Einstellungen des Nachweisdiensts.	Root-vCenter Server	TrustedAdmin.RetrieveTPMHostCertificates
Metadaten des vertrauenswürdigen Autoritätshosts abrufen	Ermöglicht das Lesen, welche Basisimages durch den Nachweisdienst bestätigt werden können.	Root-vCenter Server	TrustedAdmin.RetrieveHostMetadata

vApp-Rechte

vApp-Rechte steuern Vorgänge im Zusammenhang mit dem Bereitstellen und Konfigurieren einer vApp.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-48. vApp-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Virtuelle Maschine hinzufügen	Ermöglicht das Hinzufügen einer virtuellen Maschine zu einer vApp.	vApps	VApp.AssignVM
Ressourcenpool zuweisen	Ermöglicht das Zuweisen eines Ressourcenpools zu einer vApp.	vApps	VApp.AssignResourcePool
vApp zuweisen	Ermöglicht das Zuweisen einer vApp zu einer anderen vApp.	vApps	VApp.AssignVApp
Klonen	Ermöglicht das Klonen einer vApp.	vApps	VApp.Clone
Erstellen	Ermöglicht das Erstellen einer vApp.	vApps	VApp.Create
Löschen	Ermöglicht das Löschen einer vApp. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	vApps	VApp.Delete
Exportieren	Ermöglicht das Exportieren einer vApp aus vSphere.	vApps	VApp.Export
Importieren	Ermöglicht das Importieren einer vApp in vSphere.	vApps	VApp.Import
Verschieben	Ermöglicht das Verschieben einer vApp an einen neuen Speicherort in der Bestandsliste.	vApps	VApp.Move
Ausschalten	Ermöglicht das Ausschalten einer vApp.	vApps	VApp.PowerOff
Einschalten	Ermöglicht das Einschalten einer vApp.	vApps	VApp.PowerOn
Von URL abrufen	Ermöglicht das Auflisten von Remote-Quelldateideskriptoren.	vApps	VApp.PullFromUrls
Umbenennen	Ermöglicht das Umbenennen einer vApp.	vApps	VApp.Rename

Tabelle 16-48. vApp-Rechte (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Anhalten	Ermöglicht das Anhalten einer vApp.	vApps	VApp.Suspend
Aufheben der Registrierung	Ermöglicht das Aufheben der Registrierung einer vApp. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	vApps	VApp.Unregister
OVF-Umgebung anzeigen	Ermöglicht das Anzeigen der OVF-Umgebung einer eingeschalteten virtuellen Maschine innerhalb einer vApp.	vApps	VApp.ExtractOvfEnvironment
vApp-Anwendungskonfiguration	Ermöglicht das Ändern der internen Struktur einer vApp (z. B. Produktinformationen und Eigenschaften).	vApps	VApp.ApplicationConfig
vApp-Instanzkonfiguration	Ermöglicht das Ändern der Konfiguration einer vApp-Instanz (z. B. Richtlinien).	vApps	VApp.InstanceConfig

Tabelle 16-48. vApp-Rechte (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
vApp-managedBy-Konfiguration	Ermöglicht einer Erweiterung oder Lösung, eine vApp so zu markieren, als würde sie von dieser Erweiterung oder Lösung verwaltet. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	vApps	VApp.ManagedByConfig
vApp-Ressourcenkonfiguration	Ermöglicht das Ändern einer vApp-Ressourcenkonfiguration. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	vApps	VApp.ResourceConfig

Rechte für VcIdentityProviders

Mit den Rechten für VcIdentityProviders wird der Zugriff auf die VcIdentityProviders-API gesteuert.

Tabelle 16-49. Rechte für VcIdentityProviders

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Erstellen	Ermöglicht den Zugriff vom Typ „Nur erstellen“ auf die VcIdentityProviders-API (vCenter Server-Identitätsanbieter).	Nicht verfügbar	VcIdentityProviders.Create
Verwalten	Ermöglicht den Schreibzugriff auf Administratorebene (Erstellen, Lesen, Aktualisieren, Löschen) auf die VcIdentityProviders-API (vCenter Server-Identitätsanbieter).	Nicht verfügbar	VcIdentityProviders.Manage
Lesen	Ermöglicht den Lesezugriff auf die VcIdentityProviders-API (vCenter Server-Identitätsanbieter).	Nicht verfügbar	VcIdentityProviders.Read

Rechte für die Konfiguration von VMware vSphere Lifecycle Manager

Mit Rechten für die Konfiguration von VMware vSphere Lifecycle Manager wird die Fähigkeit zum Konfigurieren des vSphere Lifecycle Manager-Diensts gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis Weisen Sie nur Administratoren oder vertrauenswürdigen Benutzern Rechte zu, die VMware vSphere Lifecycle Manager-APIs zum Akzeptieren von URLs verwenden.

Tabelle 16-50. Rechte für die Konfiguration von VMware vSphere Lifecycle Manager

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Konfigurieren** ■ **Dienst konfigurieren**	Ermöglicht Ihnen die Konfiguration des vSphere Lifecycle Manager-Diensts und der geplanten Aufgabe zum Herunterladen von Patches.	Root-vCenter Server	VcIntegrity.General.com.vmware.vcIntegrity.Configure

Gewünschte Rechte für die Konfigurationsverwaltung von VMware vSphere Lifecycle Manager

Mit gewünschten Rechten für die Konfigurationsverwaltung von VMware vSphere Lifecycle Manager wird die Fähigkeit zum Verwalten der vSphere Lifecycle Manager-Konfiguration gesteuert.

Tabelle 16-51. Gewünschte Rechte für die Konfigurationsverwaltung von VMware vSphere Lifecycle Manager

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Gewünschte Rechte für die Konfigurationsverwaltung** ■ **Gewünschte Clusterkonfiguration exportieren** ■ **Gewünschte Clusterkonfiguration ändern** ■ **Lesezugriff auf die gewünschte Plattform für die Konfigurationsverwaltung** ■ **Cluster auf die gewünschte Konfiguration standardisieren**	**Gewünschte Clusterkonfiguration exportieren** ermöglicht das Exportieren der Konfiguration oder des Konfigurationsschemas. **Gewünschte Clusterkonfiguration ändern** ermöglicht das Importieren einer Konfiguration oder das Extrahieren der Konfiguration aus einem Referenzhost. **Lesezugriff auf die gewünschte Plattform für die Konfigurationsverwaltung** ermöglicht die Überprüfung der Konformität, das Ausführen der Standardisierungsvorabprüfung, das Anzeigen der Konformität und die Revision der Ergebnisse der Vorabprüfung. **Cluster auf die gewünschte Konfiguration standardisieren** ermöglicht die Standardisierung eines Clusters und den Übergang zu vSphere Configuration Profiles.	Root-vCenter Server	VcIntegrity.ClusterConfiguration.Export VcIntegrity.ClusterConfiguration.Modify VcIntegrity.ClusterConfiguration.View VcIntegrity.ClusterConfiguration.Remediate

Rechte für ESXi-Integritätsperspektiven für VMware vSphere Lifecycle Manager

Mit Rechten für ESXi-Integritätsperspektiven für VMware vSphere Lifecycle Manager wird die Möglichkeit gesteuert, die Integrität von ESXi-Hosts und -Clustern zu überprüfen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-52. Rechte für ESXi-Integritätsperspektiven für VMware vSphere Lifecycle Manager

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **ESXi-Integritätsperspektiven** ■ **Lesen** ■ **Schreiben**	**Lesen** ermöglicht das Abfragen des Zustands von ESXi-Hosts und -Clustern. **Schreiben** wird derzeit nicht verwendet.	Hosts Cluster	VcIntegrity.lifecycleHealth.Read VcIntegrity.lifecycleHealth.Write

Rechte für VMware vSphere Lifecycle Manager-Depots

Mit Rechten für VMware vSphere Lifecycle Manager-Depots wird die Fähigkeit zur Verwaltung von Depots gesteuert.

Tabelle 16-53. Rechte für VMware vSphere Lifecycle Manager-Depots

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Lifecycle Manager: Rechte für Depots** ■ **Löschen**	Ermöglicht das Löschen eines vSphere Lifecycle Manager-Depots.	Root-vCenter Server	VcIntegrity.lifecycleDepots.Delete

Allgemeine Rechte für VMware vSphere Lifecycle Manager

Mit den allgemeinen Rechten für VMware vSphere Lifecycle Manager wird die Fähigkeit zum Lesen und Schreiben von Lifecyle Manager-Ressourcen gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-54. Allgemeine Rechte für VMware vSphere Lifecycle Manager

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Lifecycle Manager: Allgemeine Rechte** ■ **Lesen** ■ **Schreiben**	**Lesen** ermöglicht das Lesen der vSphere Lifecycle Manager-Ressourcen. Diese Berechtigung ist erforderlich, um Aufgabeninformationen zu erhalten. **Schreiben** ermöglicht das Schreiben der vSphere Lifecycle Manager-Ressourcen. Dieses Recht ist erforderlich, um eine vSphere Lifecycle Manager-Aufgabe abzubrechen.	Root-vCenter Server	VcIntegrity.lifecycleGeneral.Read VcIntegrity.lifecycleGeneral.Write

Rechte für die Hardwarekompatibilität von VMware vSphere Lifecycle Manager

Mit Rechten für die Hardwarekompatibilität von VMware vSphere Lifecycle Manager wird die Fähigkeit gesteuert, potenzielle Hardwarekompatibilitätsprobleme zu erkennen und zu beheben.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-55. Rechte für die Hardwarekompatibilität von VMware vSphere Lifecycle Manager

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Lifecycle Manager: Berechtigungen für die Hardwarekompatibilität** ■ **Kompatibilität für den Zugriff auf Hardware** ■ **Schreiben**	**Kompatibilität für den Zugriff auf Hardware** und **Schreiben** ermöglichen den Zugriff auf die Hardwarekompatibilitätsdaten und das Beheben potenzieller Hardwarekompatibilitätsprobleme.	Hosts	VcIntegrity.HardwareCompatibility.Read VcIntegrity.HardwareCompatibility.Write

Rechte für VMware vSphere Lifecycle Manager-Images

Mit Rechten für VMware vSphere Lifecycle Manager-Images wird die Fähigkeit zur Verwaltung von Images gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis Weisen Sie nur Administratoren oder vertrauenswürdigen Benutzern Rechte zu, die VMware vSphere Lifecycle Manager-APIs zum Akzeptieren von URLs verwenden.

Tabelle 16-56. Rechte für VMware vSphere Lifecycle Manager-Images

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Lifecycle Manager: Image-Rechte** ■ **Lesen** ■ **Schreiben**	**Lesen** ermöglicht das Lesen von vSphere Lifecycle Manager-Images. Dieses Recht ist für Folgendes erforderlich: ■ Auflisten aller Entwürfe für einen Cluster ■ Erhalten weiterer Informationen zu einem Entwurf ■ Durchführen einer Prüfung für einen Entwurf ■ Validieren eines Entwurfs ■ Abrufen des Inhalts eines Entwurfs ■ Ermitteln der Liste der effektiven Komponenten ■ Erhalten der Inhalte des Dokuments mit dem aktuellen gewünschten Zustand ■ Starten einer Prüfung in einem Cluster ■ Erhalten des Konformitätsergebnisses ■ Erhalten einer Empfehlung ■ Exportieren des aktuellen gewünschten Zustands als Depot, JSON-Datei oder ISO **Schreiben** ermöglicht das Verwalten von vSphere Lifecycle Manager-Images. Dieses Recht ist für Folgendes erforderlich: ■ Erstellen, Löschen oder Übergeben eines Entwurfs ■ Importieren des gewünschten Zustands ■ Generieren von Empfehlungen	Root-vCenter Server	VcIntegrity.lifecycleSettings.Read VcIntegrity.lifecycleSettings.Write

Tabelle 16-56. Rechte für VMware vSphere Lifecycle Manager-Images

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
	■ Festlegen oder Löschen verschiedener Teile eines Entwurfs		

Rechte für die Standardisierung von VMware vSphere Lifecycle Manager-Images

Mit Rechten für VMware vSphere Lifecycle Manager-Images wird die Fähigkeit zur Standardisierung von Images gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-57. Rechte für die Standardisierung von VMware vSphere Lifecycle Manager-Images

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Lifecycle Manager: Image-Standardisierungsrechte** ■ **Lesen** ■ **Schreiben**	**Lesen** ermöglicht die Ausführung der Vorabprüfung für die Standardisierung. **Schreiben** ermöglicht die Ausführung der Standardisierung.	Cluster	VcIntegrity.lifecycleSoftwareRemediation.Read VcIntegrity.lifecycleSoftwareRemediation.Write

Rechte für VMware vSphere Lifecycle Manager-Einstellungen

Mit Rechten für VMware vSphere Lifecycle Manager-Einstellungen wird die Fähigkeit zur Verwaltung von Depots und Standardisierungsrichtlinien gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis Weisen Sie nur Administratoren oder vertrauenswürdigen Benutzern Rechte zu, die VMware vSphere Lifecycle Manager-APIs zum Akzeptieren von URLs verwenden.

Tabelle 16-58. Rechte für VMware vSphere Lifecycle Manager-Einstellungen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Lifecycle Manager: Rechte für Einstellungen** ■ **Lesen** ■ **Schreiben**	**Lesen** ermöglicht das Lesen von vSphere Lifecycle Manager-Depots und Standardisierungsrichtlinien. **Schreiben** ermöglicht das Schreiben von vSphere Lifecycle Manager-Depots und Standardisierungsrichtlinien.	Root-vCenter Server	VcIntegrity.lifecycleSoftwareSpecification.Read VcIntegrity.lifecycleSoftwareSpecification.Write

Rechte für die Verwaltung von VMware vSphere Lifecycle Manager-Baselines

Mit Rechten für die Verwaltung von VMware vSphere Lifecycle Manager-Baselines wird die Fähigkeit gesteuert, Baselines und Baselinegruppen zu verwalten.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-59. Rechte für die Verwaltung von VMware vSphere Lifecycle Manager-Baselines

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Baseline verwalten** ■ **Baseline anhängen** ■ **Baseline verwalten**	**Baseline anhängen** ermöglicht das Anhängen von Baselines und Baselinegruppen an Objekte in der vSphere-Bestandsliste. **Baseline verwalten** ermöglicht das Erstellen, Bearbeiten oder Löschen von Baselines und Baselinegruppen.	Root-vCenter Server	VcIntegrity.Baseline.com.vmware.vcIntegrity.AssignBaselines VcIntegrity.Baseline.com.vmware.vcIntegrity.ManageBaselines

Rechte zum Verwalten von Patches und Upgrades für VMware vSphere Lifecycle Manager

Mit den Rechten zum Verwalten von Patches und Upgrades für VMware vSphere Lifecycle Manager wird die Fähigkeit zum Anzeigen, Prüfen und Standardisieren anwendbarer Patches, Erweiterungen oder Upgrades gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-60. Rechte zum Verwalten von Patches und Upgrades für VMware vSphere Lifecycle Manager

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Patches und Upgrades verwalten** ■ **Standardisieren zum Übernehmen von Patches, Erweiterungen und Upgrades** ■ **Auf passende Patches, Erweiterungen und Upgrades prüfen** ■ **Patches und Erweiterungen bereitstellen** ■ **Konformitätsstatus anzeigen**	**Standardisieren zum Übernehmen von Patches, Erweiterungen und Upgrades** ermöglicht die Standardisierung von virtuellen Maschinen und Hosts, um Patches, Erweiterungen oder Upgrades anzuwenden, wenn Sie Baselines verwenden. Mit diesem Recht können Sie außerdem den Konformitätsstatus anzeigen. **Auf passende Patches, Erweiterungen und Upgrades prüfen** ermöglicht das Prüfen von virtuellen Maschinen und Hosts, um nach anwendbaren Patches, Erweiterungen oder Upgrades zu suchen, wenn Sie Baselines verwenden. **Patches und Erweiterungen bereitstellen** ermöglicht das Staging von Patches oder Erweiterungen auf ESXi-Hosts, wenn Sie Baselines verwenden. Außerdem ermöglicht Ihnen dieses Recht die Anzeige des Konformitätsstatus der ESXi-Hosts. **Konformitätsstatus anzeigen** ermöglicht die Anzeige der Baseline-Konformitätsinformationen für ein Objekt in der vSphere-Bestandsliste.	Root-vCenter Server	VcIntegrity.Updates.com.vmware.vcIntegrity.Remediate VcIntegrity.Updates.com.vmware.vcIntegrity.Scan VcIntegrity.Updates.com.vmware.vcIntegrity.Stage VcIntegrity.Updates.com.vmware.vcIntegrity.ViewStatus

Rechte zum Hochladen von Dateien für VMware vSphere Lifecycle Manager

Mit Rechten zum Hochladen von Dateien für VMware vSphere Lifecycle Manager wird die Fähigkeit gesteuert, Updates in das vSphere Lifecycle Manager-Depot zu importieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis Weisen Sie nur Administratoren oder vertrauenswürdigen Benutzern Rechte zu, die VMware vSphere Lifecycle Manager-APIs zum Akzeptieren von URLs verwenden.

Tabelle 16-61. Rechte zum Hochladen von Dateien für VMware vSphere Lifecycle Manager

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Datei hochladen** ■ **Upgrade-Images und Offline-Pakete hochladen**	Ermöglicht das Hochladen von Upgrade-ISO und Offline-Patchpaketen.	Root-vCenter Server	VcLifecycle.Upgrade

Rechte zum Ändern der VM-Konfiguration

Rechte zum Ändern der VM-Konfiguration steuern die Fähigkeit, Optionen und Geräte für virtuelle Maschinen zu konfigurieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-62. Rechte zum Ändern der VM-Konfiguration

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Konfiguration ändern** ■ **Festplatten-Lease abrufen**	Ermöglicht Festplatten-Lease-Vorgänge für eine virtuelle Maschine.	virtuelle Maschinen	VirtualMachine.Config.DiskLease
■ **Konfiguration ändern** ■ **Vorhandene Festplatte hinzufügen**	Ermöglicht das Hinzufügen einer vorhandenen virtuellen Festplatte zu einer virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Config.AddExistingDisk
■ **Konfiguration ändern** ■ **Neue Festplatte hinzufügen**	Ermöglicht das Erstellen einer neuen virtuellen Festplatte für eine virtuelle Maschine.	virtuelle Maschinen	VirtualMachine.Config.AddNewDisk

Tabelle 16-62. Rechte zum Ändern der VM-Konfiguration (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Konfiguration ändern** ■ **Gerät hinzufügen oder entfernen**	Ermöglicht das Hinzufügen oder Entfernen von Geräten (ausgenommen Festplatten).	virtuelle Maschinen	VirtualMachine.Config.AddRemoveDevice
■ **Konfiguration ändern** ■ **Erweiterte Konfiguration**	Ermöglicht das Hinzufügen oder Ändern erweiterter Parameter in der Konfigurationsdatei der virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Config.AdvancedConfig
■ **Konfiguration ändern** ■ **CPU-Anzahl ändern**	Ermöglicht das Ändern der Anzahl virtueller CPUs.	virtuelle Maschinen	VirtualMachine.Config.CPUCount
■ **Konfiguration ändern** ■ **Arbeitsspeicher ändern**	Ermöglicht das Ändern der Größe des Arbeitsspeichers, der der virtuellen Maschine zugeteilt ist.	virtuelle Maschinen	VirtualMachine.Config.Memory
■ **Konfiguration ändern** ■ **Einstellungen ändern**	Ermöglicht das Ändern der allgemeinen Einstellungen der virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Config.Settings
■ **Konfiguration ändern** ■ **Platzierung der Auslagerungsdatei ändern**	Ermöglicht das Ändern der Richtlinie zur Platzierung der Auslagerungsdatei für eine virtuelle Maschine.	virtuelle Maschinen	VirtualMachine.Config.SwapPlacement
■ **Konfiguration ändern** ■ **Ressource ändern**	Ermöglicht das Ändern der Ressourcenkonfiguration für eine Gruppe von VM-Knoten in einem vorgegebenen Ressourcenpool.	virtuelle Maschinen	VirtualMachine.Config.Resource

Tabelle 16-62. Rechte zum Ändern der VM-Konfiguration (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Konfiguration ändern** ■ **Host-USB-Gerät konfigurieren**	Ermöglicht das Verbinden eines hostbasierten USB-Geräts mit einer virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Config.HostUSBDevice
■ **Konfiguration ändern** ■ **Rohgerät konfigurieren**	Ermöglicht das Hinzufügen oder Entfernen einer Raw-Festplattenzuordnung oder eines SCSI-Passthrough-Geräts. Wenn dieser Parameter gesetzt wird, werden alle weiteren Rechte zum Ändern von Raw-Geräten außer Kraft gesetzt, einschließlich des Verbindungsstatus.	virtuelle Maschinen	VirtualMachine.Config.RawDevice
■ **Konfiguration ändern** ■ **managedBy konfigurieren**	Gestattet es einer Erweiterung oder Lösung, eine virtuelle Maschine als von dieser Erweiterung oder Lösung verwaltet zu markieren.	virtuelle Maschinen	VirtualMachine.Config.ManagedBy
■ **Konfiguration ändern** ■ **Verbindungseinstellungen anzeigen**	Ermöglicht die Konfiguration von Optionen für Remotekonsolen virtueller Maschinen.	virtuelle Maschinen	VirtualMachine.Config.MksControl
■ **Konfiguration ändern** ■ **Virtuelle Festplatte erweitern**	Ermöglicht das Vergrößern einer virtuellen Festplatte.	virtuelle Maschinen	VirtualMachine.Config.DiskExtend

Tabelle 16-62. Rechte zum Ändern der VM-Konfiguration (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Konfiguration ändern** ■ **Verbindungseinstellungen ändern**	Ermöglicht das Ändern der Eigenschaften eines vorhandenen Geräts.	virtuelle Maschinen	VirtualMachine.Config.EditDevice
■ **Konfiguration ändern** ■ **Kompatibilität der Fault Tolerance abfragen**	Ermöglicht das Prüfen, ob eine virtuelle Maschine mit Fault Tolerance kompatibel ist.	virtuelle Maschinen	VirtualMachine.Config.QueryFTCompatibility
■ **Konfiguration ändern** ■ **Dateien ohne Besitzer abfragen**	Ermöglicht das Abfragen von Dateien ohne Besitzer.	virtuelle Maschinen	VirtualMachine.Config.QueryUnownedFiles
■ **Konfiguration ändern** ■ **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	VirtualMachine.Config.ReloadFromPath
■ **Konfiguration ändern** ■ **Festplatte entfernen**	Ermöglicht das Entfernen eines virtuellen Festplattengeräts.	virtuelle Maschinen	VirtualMachine.Config.RemoveDisk

Tabelle 16-62. Rechte zum Ändern der VM-Konfiguration (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Konfiguration ändern** ■ **Umbenennen**	Ermöglicht das Umbenennen einer virtuellen Maschine oder das Ändern zugeordneter Anmerkungen für eine virtuelle Maschine.	virtuelle Maschinen	VirtualMachine.Config.Rename
■ **Konfiguration ändern** ■ **Gastinformationen zurücksetzen**	Ermöglicht das Bearbeiten der Gastbetriebssystem-Informationen für eine virtuelle Maschine.	virtuelle Maschinen	VirtualMachine.Config.ResetGuestInfo
■ **Konfiguration ändern** ■ **Anmerkung festlegen**	Ermöglicht das Hinzufügen oder Bearbeiten einer Anmerkung für eine virtuelle Maschine.	virtuelle Maschinen	VirtualMachine.Config.Annotation
■ **Konfiguration ändern** ■ **Festplattenänderungsverfolgung aktivieren bzw. deaktivieren**	Ermöglicht das Aktivieren bzw. Deaktivieren der Änderungsverfolgung für Festplatten der virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Config.ChangeTracking
■ **Konfiguration ändern** ■ **Verzweigtes übergeordnetes Element umschalten**	Ermöglicht das Aktivieren bzw. Deaktivieren eines übergeordneten vmfork.	virtuelle Maschinen	VirtualMachine.Config.ToggleForkParent
■ **Konfiguration ändern** ■ **Kompatibilität der virtuellen Maschine aktualisieren**	Ermöglicht das Upgrade der Kompatibilitätsversion der virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Config.UpgradeVirtualHardware

Rechte für Vorgänge als Gast auf virtuellen Maschinen

Rechte für Gastvorgänge auf virtuellen Maschinen steuern die Fähigkeit zur Interaktion der Daten und Anwendungen innerhalb des Gastbetriebssystems einer virtuellen Maschine mit der API.

Weitere Informationen zu diesen Vorgängen finden Sie in der Dokumentation *vSphere Web Services-API-Referenz*.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-63. Vorgänge als Gast auf virtuelle Maschinen

Rechtename im vSphere Client	Beschreibung	Gültig für Objekt	Rechtename in der API
■ **Gastvorgänge** ■ **Aliasspeicher im Gast ändern**	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die das Ändern des Alias für die virtuelle Maschine beinhalten.	virtuelle Maschinen	VirtualMachine.GuestOperations.ModifyAliases
■ **Gastvorgänge** ■ **Aliasspeicher im Gast abfragen**	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die das Abfragen des Alias für die virtuelle Maschine beinhalten.	virtuelle Maschinen	VirtualMachine.GuestOperations.QueryAliases
■ **Gastvorgänge** ■ **Gastvorgangsänderungen**	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die Änderungen am Gastbetriebssystem einer virtuellen Maschine einschließen, wie z. B. das Übertragen einer Datei auf eine virtuelle Maschine. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	virtuelle Maschinen	VirtualMachine.GuestOperations.Modify

Tabelle 16-63. Vorgänge als Gast auf virtuelle Maschinen (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Gültig für Objekt	Rechtename in der API
■ **Gastvorgänge** ■ **Gastvorgang-Programmausführung**	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die das Ausführen einer Anwendung auf der virtuellen Maschine einschließen. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	virtuelle Maschinen	VirtualMachine.GuestOperations.Execute
■ **Gastvorgänge** ■ **Gastvorgangsabfragen**	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die Abfragen des Gastbetriebssystems einschließen, wie z. B. das Auflisten von Dateien im Gastbetriebssystem. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	virtuelle Maschinen	VirtualMachine.GuestOperations.Query

Rechte für die Interaktion virtueller Maschinen

Rechte für die Interaktion virtueller Maschinen steuern die Fähigkeit, mit der Konsole einer virtuellen Maschine zu interagieren, Medien zu konfigurieren, Betriebsvorgänge auszuführen und VMware Tools zu installieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-64. Interaktion virtueller Maschinen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Interaktion** ■ **Frage beantworten**	Ermöglicht die Behebung von Problemen beim Statuswechsel virtueller Maschinen und bei Laufzeitfehlern.	virtuelle Maschinen	VirtualMachine.Interact.AnswerQuestion
■ **Interaktion** ■ **Sicherungsvorgang der virtuellen Maschine**	Ermöglicht die Ausführung von Sicherungsvorgängen bei virtuellen Maschinen.	virtuelle Maschinen	VirtualMachine.Interact.Backup
■ **Interaktion** ■ **CD-Medien konfigurieren**	Ermöglicht die Konfiguration eines virtuellen DVD- oder CD-ROM-Laufwerks.	virtuelle Maschinen	VirtualMachine.Interact.SetCDMedia
■ **Interaktion** ■ **Diskettenmedien konfigurieren**	Ermöglicht die Konfiguration eines virtuellen Diskettenlaufwerks.	virtuelle Maschinen	VirtualMachine.Interact.SetFloppyMedia
■ **Interaktion** ■ **Konsoleninteraktion**	Ermöglicht die Interaktion mit der virtuellen Maus, der virtuellen Tastatur und dem virtuellen Bildschirm der virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Interact.ConsoleInteract
■ **Interaktion** ■ **Screenshot erstellen**	Ermöglicht die Erstellung eines Screenshots einer virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Interact.CreateScreenshot
■ **Interaktion** ■ **Alle Festplatten defragmentieren**	Ermöglicht Defragmentierungsvorgänge für alle Festplatten der virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Interact.DefragmentAllDisks
■ **Interaktion** ■ **Geräteverbindung**	Ermöglicht die Änderung des Verbindungsstatus der virtuellen Geräte einer virtuellen Maschine, die getrennt werden können.	virtuelle Maschinen	VirtualMachine.Interact.DeviceConnection
■ **Interaktion** ■ **Drag & Drop**	Ermöglich das Ziehen und Ablegen von Dateien zwischen einer virtuellen Maschine und einem Remoteclient.	virtuelle Maschinen	VirtualMachine.Interact.DnD

Tabelle 16-64. Interaktion virtueller Maschinen (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Interaktion** ■ **Verwaltung des Gastbetriebssystems durch VIX API**	Ermöglicht die Verwaltung des Betriebssystems der virtuellen Maschine über die VIX-API.	virtuelle Maschinen	VirtualMachine.Interact.GuestControl
■ **Interaktion** ■ **USB HID-Scancodes einfügen**	Ermöglicht das Einfügen von USB HID-Scancodes.	virtuelle Maschinen	VirtualMachine.Interact.PutUsbScanCodes
■ **Interaktion** ■ **Anhalten oder Wiederaufnehmen**	Ermöglicht das Anhalten oder Fortsetzen der virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Interact.Pause
■ **Interaktion** ■ **Zurücksetzungs- oder Verkleinerungsvorgänge ausführen**	Ermöglicht die Ausführung von Zurücksetzungs- oder Verkleinerungsvorgängen auf der virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Interact.SESparseMaintenance
■ **Interaktion** ■ **Ausschalten**	Ermöglicht das Ausschalten einer eingeschalteten virtuellen Maschine. Dabei wird das Gastbetriebssystem heruntergefahren.	virtuelle Maschinen	VirtualMachine.Interact.PowerOff
■ **Interaktion** ■ **Einschalten**	Ermöglicht das Einschalten einer ausgeschalteten virtuellen Maschine und die Wiederaufnahme des Betriebs einer angehaltenen virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Interact.PowerOn
■ **Interaktion** ■ **Sitzung auf virtueller Maschine aufzeichnen**	Ermöglicht die Aufzeichnung einer Sitzung auf einer virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Interact.Record
■ **Interaktion** ■ **Wiedergabe sitzung auf der virtuellen Maschine**	Ermöglicht die Wiedergabe einer aufgezeichneten Sitzung auf einer virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Interact.Replay

Tabelle 16-64. Interaktion virtueller Maschinen (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Interaktion** ■ **Zurücksetzen**	Ermöglicht das Zurücksetzen einer virtuellen Maschine und den Neustart des Gastbetriebssystems.	virtuelle Maschinen	VirtualMachine.Interact.Reset
■ **Interaktion** ■ **Fault Tolerance fortsetzen**	Ermöglicht die Fortsetzung von Fault Tolerance für eine virtuelle Maschine.	virtuelle Maschinen	VirtualMachine.Interact.EnableSecondary
■ **Interaktion** ■ **Anhalten**	Ermöglicht das Anhalten einer eingeschalteten virtuellen Maschine. Dabei wird das Gastsystem in den Standby-Modus versetzt.	virtuelle Maschinen	VirtualMachine.Interact.Suspend
■ **Interaktion** ■ **Fault Tolerance anhalten**	Ermöglicht die Unterbrechung von Fault Tolerance für eine virtuelle Maschine.	virtuelle Maschinen	VirtualMachine.Interact.DisableSecondary
■ **Interaktion** ■ **Anhalten und in Arbeitsspeicher verschieben**	Ermöglicht das Aussetzen des Arbeitsspeichers für eine virtuelle Maschine.	virtuelle Maschinen	VirtualMachine.Interact.SuspendToMemory
■ **Interaktion** ■ **Failover testen**	Ermöglicht das Testen des Fault Tolerance-Failovers, indem die sekundäre virtuelle Maschine als primäre virtuelle Maschine festgelegt wird.	virtuelle Maschinen	VirtualMachine.Interact.MakePrimary
■ **Interaktion** ■ **Neustart sekundärer VM testen**	Ermöglicht das Beenden einer sekundären virtuellen Maschine für eine virtuelle Maschine mit Fault Tolerance.	virtuelle Maschinen	VirtualMachine.Interact.DisableSecondary
■ **Interaktion** ■ **Fault Tolerance ausschalten**	Ermöglicht die Deaktivierung von Fault Tolerance für eine virtuelle Maschine.	virtuelle Maschinen	VirtualMachine.Interact.TurnOffFaultTolerance

Tabelle 16-64. Interaktion virtueller Maschinen (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Interaktion** ■ **Fault Tolerance einschalten**	Ermöglicht die Aktivierung von Fault Tolerance für eine virtuelle Maschine.	virtuelle Maschinen	VirtualMachine.Interact.CreateSecondary
■ **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	VirtualMachine.Interact.ToolsInstall

Rechte zum Bearbeiten der Bestandsliste einer virtuellen Maschine

Rechte zum Bearbeiten der Bestandsliste steuern das Hinzufügen, Verschieben und Entfernen von virtuellen Maschinen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-65. Rechte zum Bearbeiten der Bestandsliste einer virtuellen Maschine

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Bestandsliste bearbeiten** ■ **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	VirtualMachine.Inventory.CreateFromExisting
■ **Bestandsliste bearbeiten** ■ **Neue erstellen**	Ermöglicht das Erstellen einer virtuellen Maschine und die Zuteilung von Ressourcen für ihre Ausführung.	Cluster, Hosts, Ordner für virtuelle Maschinen	VirtualMachine.Inventory.Create

Tabelle 16-65. Rechte zum Bearbeiten der Bestandsliste einer virtuellen Maschine (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Bestandsliste bearbeiten** ■ **Verschieben**	Ermöglicht das Verlagern einer virtuellen Maschine in der Hierarchie. Die Berechtigung muss für Quelle und Ziel vorhanden sein.	virtuelle Maschinen	VirtualMachine.Inventory.Move
■ **Bestandsliste bearbeiten** ■ **Registrieren**	Ermöglicht das Hinzufügen einer vorhandenen virtuellen Maschine zu einer vCenter Server- oder Host-Bestandsliste.	Cluster, Hosts, Ordner für virtuelle Maschinen	VirtualMachine.Inventory.Register
■ **Bestandsliste bearbeiten** ■ **Entfernen**	Ermöglicht das Löschen einer virtuellen Maschine. Durch das Löschen werden die zugrunde liegenden Dateien der virtuellen Maschine von der Festplatte entfernt. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	virtuelle Maschinen	VirtualMachine.Inventory.Delete
■ **Bestandsliste bearbeiten** ■ **Registrierung aufheben**	Ermöglicht das Aufheben der Registrierung einer virtuellen Maschine in einer vCenter Server- oder Host-Bestandsliste. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	virtuelle Maschinen	VirtualMachine.Inventory.Unregister

Rechte für das Bereitstellen virtueller Maschinen

Rechte für das Bereitstellen virtueller Maschinen steuern Aktivitäten im Bezug auf das Bereitstellen und Anpassen von virtuelle Maschinen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-66. Rechte für das Bereitstellen virtueller Maschinen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **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	VirtualMachine.Provisioning.DiskRandomAccess
■ **Bereitstellung** ■ **Dateizugriff zulassen**	Ermöglicht Vorgänge für Dateien, die einer virtuellen Maschine zugeordnet sind, einschließlich VMX, Festplatten, Protokollen und NVRAM.	virtuelle Maschinen	VirtualMachine.Provisioning.FileRandomAccess
■ **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	VirtualMachine.Provisioning.DiskRandomRead

Tabelle 16-66. Rechte für das Bereitstellen virtueller Maschinen (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **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	VirtualMachine.Provisioning.GetVmFiles
■ **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	VirtualMachine.Provisioning.PutVmFiles
■ **Bereitstellung** ■ **Vorlage klonen**	Ermöglicht das Klonen einer Vorlage.	Vorlagen	VirtualMachine.Provisioning.CloneTemplate
■ **Bereitstellung** ■ **Virtuelle Maschine klonen**	Ermöglicht das Klonen einer vorhandenen virtuellen Maschine und das Zuweisen von Ressourcen.	virtuelle Maschinen	VirtualMachine.Provisioning.Clone
■ **Bereitstellung** ■ **Vorlage aus virtueller Maschine erstellen**	Ermöglicht das Erstellen einer neuen Vorlage anhand einer virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Provisioning.CreateTemplateFromVM
■ **Bereitstellung** ■ **Gast anpassen**	Ermöglicht die benutzerdefinierte Anpassung des Gastbetriebssystems einer virtuellen Maschine ohne sie zu verschieben.	virtuelle Maschinen	VirtualMachine.Provisioning.Customize

Tabelle 16-66. Rechte für das Bereitstellen virtueller Maschinen (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Bereitstellung** ■ **Vorlage bereitstellen**	Ermöglicht das Bereitstellen einer virtuellen Maschine anhand einer Vorlage.	Vorlagen	VirtualMachine.Provisioning.DeployTemplate
■ **Bereitstellung** ■ **Als Vorlage markieren**	Ermöglicht das Kennzeichnen einer vorhandenen, ausgeschalteten virtuellen Maschine als Vorlage.	virtuelle Maschinen	VirtualMachine.Provisioning.MarkAsTemplate
■ **Bereitstellung** ■ **Als virtuelle Maschine markieren**	Ermöglicht das Kennzeichnen einer vorhandenen Vorlage als virtuelle Maschine.	Vorlagen	VirtualMachine.Provisioning.MarkAsVM
■ **Bereitstellung** ■ **Anpassungsspezifikation ändern**	Ermöglicht das Erstellen, Ändern oder Löschen von Anpassungsspezifikationen.	Root-vCenter Server	VirtualMachine.Provisioning.ModifyCustSpecs
■ **Bereitstellung** ■ **Festplatten heraufstufen**	Ermöglicht das Heraufstufen von Vorgängen auf den Festplatten einer virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.Provisioning.PromoteDisks
■ **Bereitstellung** ■ **Anpassungsspezifikationen lesen**	Ermöglicht das Lesen einer Anpassungsspezifikation.	virtuelle Maschinen	VirtualMachine.Provisioning.ReadCustSpecs

Rechte für die Dienstkonfiguration der virtuellen Maschine

Rechte für die Dienstkonfiguration der virtuellen Maschine bestimmen, wer die Überwachungs- und Verwaltungsaufgaben für die Dienstkonfiguration ausführen kann.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-67. Rechte für die Dienstkonfiguration der virtuellen Maschine

Rechtename im vSphere Client	Beschreibung	Rechtename in der API
■ **Dienstkonfiguration** ■ **Benachrichtigungen zulassen**	Ermöglicht das Erstellen und Nutzen von Benachrichtigungen zum Dienststatus.	VirtualMachine.Namespace.Event
■ **Dienstkonfiguration** ■ **Abrufen globaler Ereignisbenachrichtigungen zulassen**	Ermöglicht die Abfrage, ob Benachrichtigungen vorhanden sind.	VirtualMachine.Namespace.EventNotify
■ **Dienstkonfiguration** ■ **Dienstkonfiguration verwalten**	Ermöglicht das Erstellen, Ändern und Löschen von VM-Diensten.	VirtualMachine.Namespace.Management
■ **Dienstkonfiguration** ■ **Dienstkonfiguration ändern**	Ermöglicht das Ändern der bestehenden Dienstkonfiguration der virtuellen Maschine.	VirtualMachine.Namespace.ModifyContent
■ **Dienstkonfiguration** ■ **Dienstkonfigurationen abfragen**	Ermöglicht das Abrufen einer Liste der VM-Dienste.	VirtualMachine.Namespace.Query
■ **Dienstkonfiguration** ■ **Dienstkonfiguration lesen**	Ermöglicht das Abrufen der bestehenden Dienstkonfiguration der virtuellen Maschine.	VirtualMachine.Namespace.ReadContent

Rechte für die Snapshot-Verwaltung von virtuellen Maschinen

Rechte in Bezug auf die Snapshot-Verwaltung von virtuellen Maschinen steuern die Fähigkeit, Snapshots aufzunehmen, zu löschen, umzubenennen und wiederherzustellen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-68. Rechte für die Snapshot-Verwaltung von virtuellen Maschinen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Snapshot-Verwaltung** ■ **Snapshot erstellen**	Ermöglicht das Erstellen eines neuen Snapshots vom aktuellen Status der virtuellen Maschine.	virtuelle Maschinen	VirtualMachine.State.CreateSnapshot
■ **Snapshot-Verwaltung** ■ **Snapshot entfernen**	Ermöglicht das Entfernen eines Snapshots aus dem Snapshotverlauf.	virtuelle Maschinen	VirtualMachine.State.RemoveSnapshot

Tabelle 16-68. Rechte für die Snapshot-Verwaltung von virtuellen Maschinen (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Snapshot-Verwaltung** ■ **Snapshot umbenennen**	Ermöglicht das Umbenennen eines Snapshots durch Zuweisen eines neuen Namens und/oder einer neuen Beschreibung.	virtuelle Maschinen	VirtualMachine.State.RenameSnapshot
■ **Snapshot-Verwaltung** ■ **Snapshot wiederherstellen**	Ermöglicht das Zurücksetzen der virtuellen Maschine auf den Status, der in einem bestimmten Snapshot vorgelegen hat.	virtuelle Maschinen	VirtualMachine.State.RevertToSnapshot

vSphere Replication-Rechte der VM

vSphere Replication-Rechte der VM steuern die Verwendung der Replizierung durch VMware vCenter Site Recovery Manager™ für virtuelle Maschinen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-69. vSphere Replication-Rechte der VM

Rechtename im	Beschreibung	Erforderlich bei	Rechtename in der API
■ **vSphere Replication** ■ **Replizierung konfigurieren**	Ermöglicht die Konfiguration der vSphere Replication der VM.	virtuelle Maschinen	VirtualMachine.Hbr.ConfigureReplication
■ **vSphere Replication** ■ **Replizierung verwalten**	Ermöglicht das Auslösen der Online-, Offline- oder Vollsynchronisierung bei einer vSphere Replication der VM.	virtuelle Maschinen	VirtualMachine.Hbr.ReplicaManagement
■ **vSphere Replication** ■ **Replizierung überwachen**	Ermöglicht die Überwachung einer vSphere Replication der VM.	virtuelle Maschinen	VirtualMachine.Hbr.MonitorReplication

Rechte für VM-Klassen

Rechte für VM-Klassen steuern, wer VM-Klassen in einem Kubernetes-Namespace hinzufügen und entfernen kann.

Tabelle 16-70. Rechte für VM-Klassen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Klassen virtueller Maschinen verwalten	Ermöglicht die Verwaltung von VM-Klassen in Kubernetes-Namespaces in einem Supervisor-Cluster.	Cluster	VirtualMachineClasses.Manage

vSAN-Rechte

vSAN-Rechte steuern, wer flache Vorgänge zur erneuten Schlüsselerstellung durchführen und Clientinformationen aktualisieren darf.

Tabelle 16-71. vSAN-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
■ **Cluster** ■ **ShallowRekey**	Ermöglicht die Durchführung einer flachen erneuten Schlüsselerstellung für einen Cluster.	Cluster	Vsan.Cluster.ShallowRekey
■ **Xvc** ■ **UpdateClientInfo**	Intern verwendet.	Dienstbenutzer	Vsan.Xvc.UpdateClientInfo

Rechte für vSAN-Statistiken

vSphere Stats-Rechte steuern die Fähigkeit, auf vSAN-Metriken zuzugreifen.

Tabelle 16-72. Rechte für vSAN-Statistiken

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Zugriff auf Dienstermittlungs-Endpoint der vSAN-Statistiken	Ermöglicht den Zugriff auf den Dienstermittlungs-Endpoint `https://` *vCenterServer-IP* `/vsan/metrics/serviceDiscovery`.	Dienstkontorolle.	vSANStats.Access

vSphere-Zonen-Rechte

vSphere-Zonen-Rechte steuern, wer vSphere-Zonen auf vSphere with Tanzu erstellen und verwalten kann.

Tabelle 16-73. vSphere-Zonen-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Anhängen und Trennen von vSphere-Objekten für vSphere-Zonen	Ermöglicht die Zuordnung von Objekten zu einer vSphere-Zone.	Cluster	Zone.ObjectAttachable
vSphere-Zonen und deren Zuordnungen erstellen, aktualisieren und löschen	Ermöglicht das Erstellen und Löschen einer vSphere-Zone.	Cluster	Zone.Manage

vService-Rechte

vService-Rechte steuern den Zugriff virtueller Maschinen und vApps auf Funktionen zum Erstellen, Konfigurieren und Aktualisieren von vService-Abhängigkeiten.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-74. vService-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Abhängigkeit erstellen	Ermöglicht das Erstellen einer vService-Abhängigkeit für virtuelle Maschinen oder vApps.	vApps und virtuelle Maschinen	vService.CreateDependency
Abhängigkeit löschen	Ermöglicht das Entfernen einer vService-Abhängigkeit für eine virtuelle Maschine oder vApp.	vApps und virtuelle Maschinen	vService.DestroyDependency
Abhängigkeitskonfiguration neu konfigurieren	Ermöglicht die Neukonfiguration einer Abhängigkeit, um den Anbieter oder die Bindung zu aktualisieren.	vApps und virtuelle Maschinen	vService.ReconfigureDependency
Abhängigkeit aktualisieren	Ermöglicht Aktualisierungen einer Abhängigkeit, um den Namen oder die Beschreibung zu konfigurieren.	vApps und virtuelle Maschinen	vService.UpdateDependency

vSphere-Tag-Berechtigungen

Die vSphere-Tag-Berechtigungen bestimmen, ob Tags und Tag-Kategorien erstellt und gelöscht und ob Tags in vCenter Server-Bestandslistenobjekten zugewiesen und entfernt werden können.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-75. vSphere-Tag-Berechtigungen

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
vSphere Tag zuweisen oder Zuweisung aufheben	Ermöglicht das Zuweisen oder das Aufheben der Zuweisung eines Tags für ein Objekt in der vCenter Server-Bestandliste.	Beliebiges Objekt	InventoryService.Tagging.AttachTag
Zuweisen eines vSphere Tags zu einem Objekt bzw. Aufheben der Zuweisung eines vSphere Tags zu einem Objekt	Lässt zu, dass Objekten Tags zugewiesen oder nicht zugewiesen werden. Verwenden Sie dieses Recht, um zu begrenzen, welchen Objekten Benutzer Tags zuweisen oder deren Zuweisung entfernen können.	Beliebiges Objekt	InventoryService.Tagging.ObjectAttachable
vSphere Tag erstellen	Ermöglicht das Erstellen eines Tags.	Beliebiges Objekt	InventoryService.Tagging.CreateTag
vSphere Tag-Kategorie erstellen	Ermöglicht das Erstellen einer Tag-Kategorie.	Beliebiges Objekt	InventoryService.Tagging.CreateCategory
vSphere Tag löschen	Ermöglicht das Löschen eines Tags.	Beliebiges Objekt	InventoryService.Tagging.DeleteTag
vSphere Tag-Kategorie löschen	Ermöglicht das Löschen einer Tag-Kategorie.	Beliebiges Objekt	InventoryService.Tagging.DeleteCategory
vSphere Tag bearbeiten	Ermöglicht das Bearbeiten eines Tags.	Beliebiges Objekt	InventoryService.Tagging.EditTag
vSphere Tag-Kategorie bearbeiten	Ermöglicht das Bearbeiten einer Tag-Kategorie.	Beliebiges Objekt	InventoryService.Tagging.EditCategory

Tabelle 16-75. vSphere-Tag-Berechtigungen (Fortsetzung)

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
UsedBy-Feld für Kategorie ändern	Ermöglicht das Ändern des UsedBy-Felds für eine Tag-Kategorie.	Beliebiges Objekt	InventoryService.Tagging.ModifyUsedByForCategory
UsedBy-Feld für Tag ändern	Ermöglicht das Ändern des UsedBy-Felds für ein Tag.	Beliebiges Objekt	InventoryService.Tagging.ModifyUsedByForTag

vSphere Client-Rechte

vSphere Client-Rechte steuern den Offlinezugriff auf den vCenter Server.

Diese Rechte gelten nur für VMware Cloud.

vSphere Data Protection-Rechte

vSphere Data Protection-Rechte steuern die Fähigkeit zum Verwalten der VMware vSphere® Data Protection™-Sicherungs- und Wiederherstellungslösung.

Tabelle 16-76. vSphere Data Protection-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Schutz	Ermöglicht die Durchführung von Datenschutzvorgängen, wie z. B. das Erstellen und Verwalten von Backups.	vCenter Server	vSphereDataProtection.Protection
Wiederherstellung	Ermöglicht die Durchführung von Datenschutzvorgängen, wie z. B. das Wiederherstellen von Backups.	vCenter Server	vSphereDataProtection.Recovery

vSphere Stats-Rechte

vSphere Stats-Rechte steuern die Fähigkeit, auf vStats-Status- und Statistikdaten für Objekte wie virtuelle Maschinen und Hosts zuzugreifen.

Tabelle 16-77. vSphere Stats-Rechte

Rechtename im vSphere Client	Beschreibung	Erforderlich bei	Rechtename in der API
Statistikdaten erfassen	Ermöglicht das Erstellen und Aktualisieren von Übernahmespezifikationen in vStats.	Das Objekt, für das Statistikdaten erfasst werden.	vStats.CollectAny
Statistikkonfiguration ändern	Ermöglicht die Verwaltung der Konfigurationseinstellungen des vStats-Diensts.	vCenter Server	vStats.Settings
Statistikdaten abfragen	Ermöglicht das Aufzählen von Statistikanbietern sowie Metriken und Indikatoren, die Anbieter offenlegen, für die Anbieter Statistikdaten erfassen können.	Das Objekt, für das Statistikdaten abgefragt werden.	vStats.QueryAny

vSphere Hardening und Übereinstimmung

17

Organisationen erwarten, dass ihre Daten geschützt werden, indem das Risiko von Datendiebstahl, Cyberangriffen oder nicht autorisiertem Zugriff verringert wird. Häufig müssen Organisationen auch diverse Vorschriften aus Regierungs- oder privaten Standards einhalten, wie diejenigen des National Institute of Standards and Technology (NIST) und der Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG). Wenn sichergestellt werden soll, dass Ihre vSphere-Umgebung diese Standards erfüllt, muss ein Verständnis breiter gefasster Kriterien gegeben sein, die Mitarbeiter, Prozesse und Technologie einschließen.

Eine Übersicht über die verschiedenen Sicherheits- und Übereinstimmungsthemen, die Sie beachten sollten, unterstützt Sie beim Planen der Übereinstimmungsstrategie. Darüber hinaus finden Sie auf der VMware-Website zusätzliche Ressourcen zur Übereinstimmung.

Lesen Sie als Nächstes die folgenden Themen:

- Sicherheit vs. Übereinstimmung in der vSphere-Umgebung
- Referenz zu vSphere-Sicherheitskontrollen
- Informationen zum National Institute of Standards and Technology
- Informationen zu DISA STIGs
- Über NERC CIP
- Informationen zu VMware Security Development Lifecycle
- Überwachungsprotokollierung in vSphere
- Grundlegendes zur Sicherheit und Übereinstimmung – nächste Schritte
- vCenter Server und FIPS

Sicherheit vs. Übereinstimmung in der vSphere-Umgebung

Die Begriffe Sicherheit und Übereinstimmung werden häufig wie Synonyme verwendet. Es handelt sich jedoch um eindeutige und unterschiedliche Konzepte.

Sicherheit, womit häufig Informationssicherheit gemeint ist, wird in der Regel als ein Satz technischer, physischer und administrativer Kontrollen definiert, die Sie implementieren, um für Vertraulichkeit, Integrität und Verfügbarkeit zu sorgen. Sie sichern beispielsweise einen Host, indem Sie eingrenzen, welche Konten sich bei ihm auf welchen Wegen (SSH, direkte Konsole usw.) anmelden können. Übereinstimmung ist im Gegensatz dazu eine Reihe von Anforderungen, die erforderlich sind, um die minimalen Kontrollen zu erfüllen, die von verschiedenen Vorschriftenrahmen festgelegt wurden und eingeschränkte Leitlinien für jeden spezifischen Technologie-, Anbieter- oder Konfigurationstyp bereitstellen. Zum Beispiel hat die Zahlungskartenbranche (Payment Card Industry, PCI) Sicherheitsrichtlinien festgelegt, damit die Organisationen ihre Kundenkontodaten proaktiv besser schützen können.

Sicherheit verringert das Risiko von Datendiebstahl, Cyberangriffen oder nicht autorisiertem Zugriff, während die Übereinstimmung nachweist, dass eine Sicherheitskontrolle eingerichtet wurde, in der Regel innerhalb eines bestimmten Zeitrahmens. Sicherheit wird hauptsächlich in den Designentscheidungen aufgeführt und zeigt sich in den Technologiekonfigurationen. Übereinstimmung konzentriert sich auf die Zuordnung des Bezugs zwischen Sicherheitskontrollen und spezifischen Anforderungen. Eine Übereinstimmungszuordnung bietet eine zentrale Ansicht zur Auflistung vieler der erforderlichen Sicherheitskontrollen. Diese Kontrollen werden durch die jeweiligen Übereinstimmungsanforderungen der einzelnen Sicherheitskontrollen detaillierter aufgeführt, die von einer Domäne vorgegeben werden, wie NIST, PCI, FedRAMP, HIPAA usw.

Effektive Cybersicherheits- und Übereinstimmungsprogramme basieren auf drei Grundlagen: Mitarbeitern, Prozessen und Technologie. Oft wird fälschlicherweise angenommen, dass Technologie allein ausreicht, um alle Cybersicherheitsbedürfnisse zu erfüllen. Technologie spielt in der Tat eine umfassende und wichtige Rolle bei der Entwicklung und Ausführung eines Informationssicherheitsprogramms. Technologie ohne Prozesse und Verfahren, Sensibilisierung und Schulung führt allerdings zu einer Schwachstelle in Ihrer Organisation.

Beim Definieren Ihrer Sicherheits- und Übereinstimmungsstrategien müssen Sie Folgendes beachten:

- Alle Mitarbeiter benötigen allgemeine Sensibilisierung und Schulung, die IT-Mitarbeiter darüber hinaus spezifische Schulung.
- Der Prozess definiert, wie Aktivitäten, Rollen und Dokumentation innerhalb einer Organisation zur Risikominderung verwendet werden. Prozesse sind nur wirksam, wenn die Mitarbeiter sie ordnungsgemäß befolgen.
- Anhand von Technologie können die Auswirkungen eines Cybersicherheitsrisikos für Ihre Organisation verhindert oder reduziert werden. Die zu verwendende Technologie hängt von der Risikoakzeptanzebene innerhalb einer Organisation ab.

VMware bietet Compliance-Kits an, die sowohl einen Audit-Leitfaden als auch einen Leitfaden zur Produktanwendbarkeit enthalten und so die Lücke zwischen den Compliance- und gesetzlichen Anforderungen und den Implementierungsleitfäden schließen. Weitere Informationen finden Sie unter https://core.vmware.com/compliance.

Glossar für Übereinstimmungsbegriffe

Übereinstimmung führt bestimmte wichtige Begriffe und Definitionen ein.

Tabelle 17-1. Übereinstimmungsbegriffe

Begriff	Definition
CJIS	Criminal Justice Information Services (Informationsdienst Strafrechtspflege). Im Kontext der Übereinstimmung stellt der CJIS eine Sicherheitsrichtlinie zusammen, die vorgibt, welche Sicherheitsvorkehrungen lokale, bundesstaatliche und nationale Strafrechts- und Vollzugsbehörden treffen müssen, um sensible Informationen wie Fingerabdrücke und Angaben zu Vorstrafen zu schützen.
DISA STIG	Defense Information Systems Agency Security Technical Implementation Guide (Verteidigungsinformationssystembehörde – technisches Sicherheitsimplementierungshandbuch). Die Defense Information Systems Agency (DISA) ist die Behörde, die für die Aufrechterhaltung des Sicherheitsstatus der IT-Infrastruktur des Verteidigungsministeriums (Department of Defense, DoD) verantwortlich ist. DISA führt diese Aufgabe durch Entwicklung und Einsatz von Security Technical Implementation Guides (STIGs) aus.
FedRAMP	Federal Risk and Authorization Management Program (Bundesprogramm für Risiko- und Autorisierungsmanagement). FedRAMP ist ein US-Regierungsprogramm, das einen standardisierten Ansatz für die Sicherheitsbeurteilung, Autorisierung und fortlaufende Überwachung von Cloudprodukten und -services bereitstellt.
HIPAA	Health Insurance Portability and Accountability Act (Gesetz zur Übertragbarkeit und Rechenschaftspflicht für Gesundheitsversicherungen). Der HIPAA wurde 1996 vom US-Kongress verabschiedet und legt Folgendes fest: ■ Er gibt Millionen von amerikanischen Arbeitnehmern und deren Familien die Möglichkeit, Gesundheitsversicherungen zu übertragen und weiter zu unterhalten, wenn sie ihre Arbeitsstelle wechseln oder verlieren. ■ Er verringert Betrug und Missbrauch im Gesundheitswesen ■ Er gibt branchenweite Standards für Informationen im Gesundheitswesen zur elektronischen Abrechnung und anderen Prozessen vor ■ Er schreibt den Schutz und die vertrauliche Handhabung geschützter Gesundheitsdaten vor Dieser letzte Punkt ist für die Dokumentation von *vSphere-Sicherheit* besonders wichtig.

Tabelle 17-1. Übereinstimmungsbegriffe (Fortsetzung)

Begriff	Definition
NCCoE	National Cybersecurity Center of Excellence (Nationales Kompetenzzentrum für Cybersicherheit). NCCoE ist eine Organisation der US-Regierung, die Lösungen für Cybersicherheitsprobleme von US-Unternehmen entwickelt und öffentlich bereitstellt. Das Zentrum stellt ein Team aus Mitarbeitern von Cybersicherheit-Technologieunternehmen, anderen Bundesbehörden und Akademikern zusammen, um die einzelnen Probleme zu bearbeiten.
NIST	National Institute of Standards and Technology (Nationales Institut für Standards und Technologie). Das NIST ist eine nichtregulatorische Bundesbehörde, die 1901 innerhalb des US-Handelsministeriums gegründet wurde. Das NIST hat die Aufgabe, die Innovation und industrielle Wettbewerbsfähigkeit der USA zu fördern, indem Messtechniken, Standards und Technologie so vorangetrieben werden, dass sie die wirtschaftliche Sicherheit erhöhen und unsere Lebensqualität verbessern.
PAG	Product Applicability Guide (Produktanwendbarkeitshandbuch). Ein Dokument, das den Organisationen allgemeine Leitlinien an die Hand gibt, wenn sie die Lösungen eines Unternehmens zur Einhaltung der Übereinstimmungsanforderungen erwägen.
PCI DSS	Payment Card Industry Data Security Standard (Datensicherheitsstandard der Zahlungskartenindustrie). Eine Reihe von Sicherheitsstandards, mit denen sichergestellt werden soll, dass alle Unternehmen, die Kreditkarteninformationen annehmen, verarbeiten, speichern oder übertragen, eine sichere Umgebung bereitstellen.
VVD/VCF-Übereinstimmungslösungen	VMware Validated Design/VMware Cloud Foundation. Die VMware Validated Designs stellen umfangreiche und umfassend getestete Entwürfe bereit, um ein softwaredefiniertes Datencenter errichten und betreiben zu können. Anhand von VVD/VCF-Übereinstimmungslösungen können Kunden die Übereinstimmungsanforderungen zahlreicher Regierungs- und Branchenbestimmungen erfüllen.

Referenz zu vSphere-Sicherheitskontrollen

VMware Security Hardening-Handbücher bieten eine aussagekräftige Anleitung zum sicheren Bereitstellen und Nutzen von VMware-Produkten. Für vSphere ist dieses Handbuch der *vSphere Security Configuration Guide* (Handbuch für die vSphere-Sicherheitskonfiguration, früher als *Handbuch für „Hardening“* bezeichnet). Ab vSphere 8.0 Update 3 sind die Informationen aus

dem *vSphere Security Configuration Guide*, die als Sicherheitskontrollen bezeichnet werden, in diesem Handbuch enthalten.

Sicherheitskontrollen bieten Best Practices in Bezug auf die Sicherheit für vSphere. Die Sicherheitskontrollen entsprechen nicht direkt den regulatorischen Richtlinien oder Frameworks. Verwenden Sie sie daher nicht als Mittel zur Erreichung von Konformität. Außerdem sind die Sicherheitskontrollen nicht für die Verwendung als Sicherheitscheckliste vorgesehen.

Beim Thema Sicherheit muss man immer einen Kompromiss eingehen. Bei der Umsetzung von Sicherheitskontrollen kann sich dies negativ auf Benutzerfreundlichkeit, Leistung oder andere operative Aufgaben auswirken. Berücksichtigen Sie Ihre Arbeitslasten, Nutzungsmuster, die Organisationsstruktur usw. sorgfältig, bevor Sie Sicherheitsänderungen vornehmen, unabhängig davon, ob der Hinweis von VMware oder aus anderen Branchenquellen stammt.

Wenn Ihre Organisation der Einhaltung behördlicher Auflagen unterliegt, lesen Sie https://core.vmware.com/compliance. Diese Site enthält Compliance Kits und Produktüberwachungshandbücher, die vSphere-Administratoren und regulatorische Auditoren dabei unterstützen, die virtuelle Infrastruktur für regulatorische Frameworks zu sichern und zu bestätigen, wie z. B. NIST 800-53v4, NIST 800-171, PCI DSS, HIPAA, CJIS, ISO 27001 und mehr.

In diesen vSphere-Sicherheitskontrollen werden die folgenden Elemente nicht erörtert:

- Software, die innerhalb der virtuellen Maschine ausgeführt wird, wie z. B. das Gastbetriebssystem und Anwendungen
- Datenverkehr über Netzwerke der virtuellen Maschinen
- Sicherheit der Add-on-Produkte

Diese vSphere-Sicherheitskontrollen sind nicht als Tool für die „Konformität“ gedacht. Diese Sicherheitskontrollen unterstützen Sie bei den ersten Schritten auf dem Weg zur Konformität, stellen aber für sich allein nicht sicher, dass Ihre Bereitstellung konform ist. Weitere Informationen zur Übereinstimmung finden Sie unter Sicherheit vs. Übereinstimmung in der vSphere-Umgebung.

Wenden Sie Sicherheitskontrollen nicht wahllos auf Ihre Umgebung an. Nehmen Sie sich die Zeit, jede Einstellung zu bewerten und eine informierte Entscheidung zu treffen, ob Sie sie anwenden möchten. Als Minimum können Sie die Anweisungen in den Beurteilungsabschnitten nutzen, um die Sicherheit Ihrer Bereitstellung zu überprüfen.

Diese Sicherheitskontrollen sind eine Hilfestellung für die ersten Schritte bei der Konformitätsimplementierung in Ihrer Bereitstellung. Wenn Sie ihn zusammen mit den Richtlinien der Defense Information Systems Agency (DISA) und anderen Konformitätsrichtlinien verwenden, können Sie vSphere-Sicherheitskontrollen an den Konformitätsanforderungen der jeweiligen Richtlinie ausrichten.

Definitionen für die Begriffe der Sicherheitskontrollen

In den folgenden Abschnitten für die Sicherheitskontrollen werden die folgenden Begriffe und Definitionen verwendet.

Tabelle 17-2. Definitionen von Sicherheitskontrollen

Begriff der Steuerung	Definition
Installationsstandardwert	Darauf wird die Steuerung in dieser Version von vSphere standardmäßig festgelegt, wenn Sie das Produkt erstmals installieren.
Vorgeschlagener Baseline-Wert	Eine vernünftige Empfehlung für die Konfiguration dieser Steuerung, wenn keine anderen Anleitungen vorhanden sind. Diese Empfehlungen können beispielsweise durch Richtlinien zur Einhaltung behördlicher Auflagen ersetzt werden.
Aktion erforderlich	Die vorgeschlagene Aktion für eine bestimmte Steuerung. Ändern: Nehmen Sie die Änderung vor. Für vSphere-externe Steuerungen, etwa Hardwareeinstellungen, wird in dieser Dokumentation immer davon ausgegangen, dass die Steuerung standardmäßig unsicher festgelegt ist, und es wird empfohlen, die Konfiguration zu ändern. Überwachung: Stellen Sie sicher, dass der Standardwert verwendet wird, der erwartete Wert vorhanden ist oder Ausnahmen an der Steuerung dokumentiert sind. Bei der Prüfung einer Steuerung, deren Standardwert der vorgeschlagene Wert ist, sind zwei Ansätze möglich. Erstens: Nur wenn die Parameter explizit festgelegt werden, können sie überwacht werden und bekannt sein. Zweitens: Alle Konfigurationsänderungen müssen im Laufe der Zeit „gepflegt und gefüttert“ werden, sodass Sie, wenn es einen sicheren Standard gibt, diese verwenden können, um eine Umgebung zu vereinfachen. In dieser Dokument findet der zweite Ansatz Anwendung. Sie können jedoch Ihren eigenen Ansatz auswählen. Nicht implementierte Steuerungen haben keine Auswirkungen auf die Sicherheit. Sie werden in dieser Dokumentation als „Überwachung“ aufgeführt, können aber entfernt werden.
Mögliche funktionale Auswirkungen einer Änderung des Standardwerts	Verursacht diese Änderung möglicherweise Probleme? Die meisten Sicherheitskontrollen stellen auf irgendeine Weise Kompromisse dar. Was wäre im Gegenzug erforderlich, wenn diese Steuerung geändert wird?
PowerCLI-Befehlsbeurteilung	Ein PowerCLI-Beispielbefehl, um zu bestimmen, wie die Steuerung festgelegt ist.
Beispiel für PowerCLI-Befehlsstandardisierung	Ein PowerCLI-Beispielbefehl, um die Steuerung auf die Empfehlung festzulegen.

vSphere-Systemdesign-Sicherheitskontrollenreferenz

Diese Sicherheitskontrollen stellen einen Baseline-Satz von Best Practices für vSphere-Systemdesigns bereit.

Eliminieren von vCenter Server-Plug-Ins von Drittanbietern

Reduzieren oder eliminieren Sie vCenter Server-Plug-Ins von Drittanbietern.

Die Installation von Plug-Ins und anderen Drittanbieter-Querverbindungen zwischen Systemen kann die Grenzen zwischen verschiedenen Infrastruktursystemen verwischen. Dadurch können Angreifer, die ein System kompromittiert haben, lateral zu einem anderen wechseln. Da vSphere eng an andere Systeme gekoppelt ist, ergeben sich auch Hindernisse in Bezug auf rechtzeitige Patches und Upgrades. Stellen Sie sicher, dass Plug-Ins oder Add-Ons von Drittanbietern für vSphere-Komponenten einen Mehrwert schaffen. Wenn Sie Plug-Ins anstelle einzelner Verwaltungskonsolen verwenden möchten, stellen Sie sicher, dass ihre Verwendung die von ihnen verursachten Risiken ausgleicht.

Vorsicht bei Infrastrukturverwaltungsschnittstellen

Gehen Sie vorsichtig vor, wenn Sie Infrastrukturverwaltungsschnittstellen mit allgemeinen Allzweckauthentifizierungs- und -autorisierungsquellen verbinden.

Zentrale Unternehmensverzeichnisse sind aufgrund ihrer Rolle bei der Autorisierung im gesamten Unternehmen Ziele für Angreifer. Sobald dieses Verzeichnis kompromittiert ist, kann ein Angreifer sich innerhalb einer Organisation frei bewegen. Die Verbindung der IT-Infrastruktur mit zentralisierten Verzeichnissen hat sich als erhebliches Risiko für Ransomware und andere Angriffe erwiesen. Isolieren Sie die Authentifizierung und Autorisierung aller Infrastruktursysteme.

Für ESXi:

- Gesamte Hostverwaltung über vCenter Server durchführen
- Deaktivieren der ESXi Shell
- ESXi in den normalen Sperrungsmodus versetzen
- ESXi-Root-Kennwort auf ein komplexes Kennwort festlegen

Aktivieren von vSphere Distributed Resource Scheduler

Aktivieren Sie vSphere Distributed Resource Scheduler (DRS) im vollautomatisierten Modus.

vSphere DRS verwendet vMotion zum Verschieben von Arbeitslasten zwischen physischen Hosts, um Leistung und Verfügbarkeit zu gewährleisten. Der vollautomatisierte Modus stellt sicher, dass der vSphere Lifecycle Manager mit DRS arbeiten kann, um Patch- und Aktualisierungsvorgänge zu aktivieren.

Wenn bestimmte VM-zu-Host-Zuordnungen erforderlich sind, verwenden Sie DRS Regeln. Verwenden Sie nach Möglichkeit „Sollte“-Regeln anstelle von „muss“, damit Sie die Regel beim Anwenden des Patches und der Wiederherstellung mit Hochverfügbarkeit vorübergehend anhalten können.

Aktivieren von vSphere High Availability

vSphere High Availability (HA) startet Arbeitslasten auf anderen ESXi-Hosts in einem Cluster neu, wenn ein ESXi-Host plötzlich ausfällt. Stellen Sie sicher, dass die Einstellungen für HA für Ihre Umgebung ordnungsgemäß konfiguriert sind.

Aktivieren von Enhanced vMotion Compatibility

vSphere Enhanced vMotion Compatibility (EVC) stellt sicher, dass Arbeitslasten live migriert werden können, indem vMotion zwischen ESXi-Hosts in einem Cluster verwendet wird, auf dem verschiedene CPU-Generationen ausgeführt werden. EVC hilft auch in Situationen mit CPU-Schwachstellen, in denen neue Microcode-Anweisungen für CPUs eingeführt werden können, wodurch sie vorübergehend miteinander inkompatibel sind.

Schutz von Systemen vor Manipulationen

Stellen Sie sicher, dass ESXi-Hosts und die verwandten Speicher- und Netzwerkkomponenten vor Manipulation, nicht autorisiertem Zugriff und nicht autorisierter Entfernung geschützt sind. Schützen Sie die Hosts auch vor Umweltfaktoren, etwa Überschwemmungen, extremen Temperaturen (niedrig oder hoch) sowie Staub und Schmutz.

Die Verwendung von Sicherheitsfunktionen, etwa vSphere Native Key Provider und ESXi-Schlüsselpersistenz, kann dazu führen, dass sicheres Material lokal auf ESXi-Hosts gespeichert wird, sodass Angreifer anderweitig geschützte Cluster starten und entsperren können. Es ist wichtig, die physische Sicherheit und die entsprechenden Bedrohungen wie Diebstahl zu berücksichtigen.

Abgesehen von Diebstahl bedeutet sicherheitsorientiertes Denken auch, sich selbst und Ihrer Organisation Fragen zu stellen, beispielsweise:

- Was könnte schief gehen?
- Wo finde ich heraus, ob ein Fehler aufgetreten ist?

Diese Fragen gewinnen im Umgang mit nicht besetzten Datencenter-Standorten und Kollokationsanlagen an Bedeutung. Stellen Sie in Bezug auf Datencenter- und Rack-Konfigurationen die folgenden Fragen:

- Werden die Türen zum Datencenter von selbst automatisch geschlossen und entsprechend verriegelt?
- Würden angelehnte Türen eine proaktive Warnung nach sich ziehen?
- Ist es bei verriegelten Türen immer noch möglich, von der Seite oder von oben in das Rack zu gelangen und ein Kabel zu trennen? Kann eine nicht autorisierte Person ein Kabel an einen Netzwerk-Switch anschließen?
- Ist es möglich, ein Gerät, etwa ein Speichergerät, oder sogar einen ganzen Server zu entfernen? Was würde in einem solchen Szenario geschehen?

Weitere relevante Fragen:

- Könnte jemand Informationen über Ihre Umgebung oder Ihr Unternehmen aus Informationen, die auf den Servern angezeigt werden, etwa LCD-Panels oder Konsolen, erhalten?
- Wenn diese Informationsanzeigen inaktiv sind, könnten sie von außerhalb des Racks ausgelöst werden, etwa durch Verwendung eines steifen Metalldrahtes?

- Gibt es andere Schalter, etwa den Ein-/Ausschalter, der gedrückt werden könnte, um eine Dienstunterbrechung in Ihrem Unternehmen zu verursachen?

Gibt es andere physische Bedrohungen, etwa die Möglichkeit von Überschwemmungen, Einfrieren oder hoher Hitze oder Staub und Schmutz aus der Umwelt, die sich auf die Verfügbarkeit auswirken würden?

Aussagekräftige Benennung von vSphere-Objekten

Benennen Sie vSphere-Objekte aussagekräftig, und ändern Sie die Standardnamen der Objekte, um Genauigkeit zu gewährleisten und Verwirrung zu reduzieren.

Verwenden Sie gute Benennungspraktiken für vSphere-Objekte. Ändern Sie dazu Standardnamen wie „Datencenter“, „vSAN-Datenspeicher“, „DSwitch“, „VM-Netzwerk“ usw., um zusätzliche Informationen aufzunehmen. Dies trägt zur Verbesserung der Genauigkeit und Reduzierung von Fehlern bei der Entwicklung, Implementierung und Überwachung von Sicherheitsrichtlinien und betrieblichen Prozessen bei.

Portgruppen, die 802.1Q VLAN-Tagging verwenden, könnten die VLAN-Nummer enthalten. Datencenter- und Clusternamen können Speicherorte und Zwecke umfassen. Datenspeicher- und Virtual Distributed Switch-Namen können die Namen des Datencenters und der Cluster umfassen, an die sie angehängt sind. Schlüsselanbieternamen sind besonders wichtig, insbesondere beim Schutz verschlüsselter virtueller Maschinen mit Replizierung auf alternative Sites. Vermeiden Sie potenzielle „Namenskollisionen“ mit Objekten in anderen Datencentern und Clustern.

Einige Organisationen benennen Systeme nicht mit Bezeichnern des physischen Standorts, etwa Straßenadressen. Stattdessen ziehen es vor, den physischen Standort von Datencentern durch die Verwendung von Begriffen wie „Site A“, „Site B“ usw. zu verschleiern. Dies hilft auch, wenn Standorte verlagert werden. Dadurch wird verhindert, dass alles umbenannt werden muss oder falsche Informationen verbleiben.

Beachten Sie bei der Entscheidung für ein Benennungsschema, dass viele Objekte ähnliche Eigenschaften aufweisen können. Beispielsweise könnten zwei Portgruppen dasselbe VLAN zugewiesen sein, aber unterschiedliche Regeln zum Filtern und Markieren des Datenverkehrs. Es kann für eindeutige Objekte dieses Typs hilfreich sein, einen Projektnamen oder eine Kurzbeschreibung in den Namen aufzunehmen.

Abschließend sollten Sie die Automatisierung bei der Entwicklung eines Benennungsschemas in Betracht ziehen. Namen, die programmgesteuert abgeleitet werden können, sind oft hilfreich bei der Skripterstellung und Automatisierung von Aufgaben.

Isolieren von Infrastrukturverwaltungsschnittstellen

Stellen Sie sicher, dass IT-Infrastrukturverwaltungsschnittstellen in ihrem eigenen Netzwerksegment oder als Teil eines isolierten Verwaltungsnetzwerks isoliert sind.

Stellen Sie sicher, dass sich alle für Virtualisierungskomponenten konfigurierten Verwaltungsschnittstellen in einem Netzwerksegment (VLAN usw.) befinden, das nur für die Virtualisierungsverwaltung reserviert und frei von Arbeitslasten und nicht verwandten Systemen ist. Stellen Sie sicher, dass Verwaltungsschnittstellen mit Perimetersicherheitssteuerungen gesteuert werden, sodass nur autorisierte vSphere-Administratoren von autorisierten Arbeitsstationen aus auf diese Schnittstellen zugreifen können.

Einige Systemdesigns setzen vCenter Server und andere Verwaltungstools auf ihre eigenen, von ESXi isolierten Netzwerksegmente ein, da sie eine bessere Überwachung dieser Systeme bieten. Andere Designs setzen vCenter Server mit ESXi-Verwaltung ein, da die Beziehung zwischen den beiden Produkten und die Möglichkeit besteht, dass Firewall-Konfigurationsfehler oder -ausfälle den Dienst unterbrechen. Geben Sie bei der Auswahl des Designs mit Bedacht vor.

Ordnungsgemäßes Verwenden von vMotion

Stellen Sie sicher, dass vMotion die Verschlüsselung in Übertragung begriffener Daten verwendet (für virtuelle Maschinen auf „Erforderlich“ festgelegt) oder dass für vMotion verwendete VMkernel-Netzwerkschnittstellen in ihren eigenen Netzwerksegmenten isoliert sind, die über Perimetersteuerungen verfügen.

vMotion und Storage vMotion kopieren Arbeitsspeicher- und Speicherdaten der virtuellen Maschine über das Netzwerk. Die Sicherstellung, dass die Daten bei der Übertragung verschlüsselt sind, gewährleistet die Vertraulichkeit. Die Isolierung auf ein dediziertes Netzwerksegment mit geeigneten Perimetersteuerungen kann eine mehrschichtige Verteidigung (Defense in Depth, DiD) und die Verwaltung des Netzwerkdatenverkehrs ermöglichen.

Wie bei allen Verschlüsselungsformen führt die vMotion-Verschlüsselung zu Leistungseinbußen. Aber diese Leistungsänderung tritt im vMotion-Hintergrundprozess auf und wirkt sich nicht auf den Betrieb der virtuellen Maschine aus.

Ordnungsgemäßes Verwenden von vSAN

Stellen Sie sicher, dass vSAN die Verschlüsselung in Übertragung begriffener Daten verwendet oder dass für vSAN verwendete VMkernel-Netzwerkschnittstellen in ihren eigenen Netzwerksegmenten isoliert sind, die über Perimetersteuerungen verfügen.

vSAN bietet Verschlüsselung in Übertragung begriffener Daten, die bei der Kommunikation von vSAN-Knoten zur Aufrechterhaltung der Vertraulichkeit beitragen kann. Wie bei vielen Sicherheitskontrollen muss bei der Leistung ein Kompromiss eingegangen werden. Überwachen Sie die Speicherlatenz und -leistung, wenn die Verschlüsselung in Übertragung begriffener Daten aktiviert ist. Organisationen, die die vSAN-Verschlüsselung in Übertragung begriffener Daten nicht aktivieren oder nicht aktivieren können, sollten den Netzwerkdatenverkehr zu einem dedizierten Netzwerksegment mit entsprechenden Perimetersteuerungen isolieren.

Aktivieren von Network I/O Control

Stellen Sie sicher, dass Sie widerstandsfähig gegenüber Netzwerk-Denial-of-Service-Angriffen sind, indem Sie Network I/O Control (NIOC) aktivieren.

vSphere Network I/O Control (NIOC) ist eine Datenverkehrsverwaltungs-Technologie, die Quality of Service auf Hypervisorebene bietet und die Netzwerkleistung verbessert, indem Ressourcen in Cloud-Umgebungen mit mehreren Mandanten und gemeinsam genutzten Arbeitslastumgebungen priorisiert werden. NIOC wird in vSphere Distributed Switch (vDS) integriert und partitioniert die Bandbreite von Netzwerkadaptern in „Netzwerkressourcenpools“, die verschiedenen Datenverkehrstypen entsprechen, etwa vMotion- und Verwaltungsdatenverkehr. Mithilfe von NIOC können Benutzer diesen Pools Anteile, Grenzwerte und Reservierungen zuteilen.

NIOC behält die Netzwerkverfügbarkeit für wichtige Dienste bei und verhindert eine Überlastung, indem weniger kritischer Datenverkehr begrenzt wird. Dies wird erreicht, indem die Erstellung von Netzwerksteuerungsrichtlinien pro Geschäftsanforderungen ermöglicht, die Isolierung des Datenverkehrstyps sichergestellt und eine dynamische Neuzuteilung von Ressourcen basierend auf Priorität und Nutzung ermöglicht wird.

Nicht konfigurieren der vom Anbieter reservierten VLANs

Stellen Sie sicher, dass die Uplinks des physischen Switches von ESXi-Hosts nicht mit vom Anbieter reservierten VLANs konfiguriert sind.

Einige Netzwerkanbieter reservieren bestimmte VLAN-IDs für interne oder spezifische Zwecke. Stellen Sie sicher, dass ihre vSphere-Netzwerkkonfigurationen diese Werte nicht enthalten.

Konfigurieren von ESXi-Uplinks als Zugriffsports

Stellen Sie sicher, dass die Uplinks des physischen Switches von ESXi-Hosts als „Zugriffsports“ konfiguriert sind, die einem einzelnen VLAN zugewiesen sind, oder als gekennzeichnete 802.1Q-VLAN-Trunks ohne natives VLAN. Stellen Sie sicher, dass vSphere-Portgruppen keinen Zugriff auf VLAN 1 oder nicht gekennzeichnete native VLANs zulassen.

Netzwerkverbindungen, bei denen ein „natives“ VLAN konfiguriert ist, um nicht gekennzeichneten Datenverkehr zu akzeptieren, oder die Zugriff auf VLAN 1 haben, bieten Angreifern möglicherweise die Möglichkeit, spezielle Pakete zu erstellen, die die Netzwerksicherheitskontrollen beeinträchtigen. VLAN 1 ist die Standardeinstellung, die häufig für die Netzwerkverwaltung und -kommunikation verwendet wird und von Arbeitslasten isoliert werden sollte. Stellen Sie sicher, dass Portgruppen nicht für den Zugriff auf native VLANs konfiguriert sind. Stellen Sie sicher, dass VLAN-Trunk-Ports mit bestimmten Definitionen von VLANs (nicht „alle“) konfiguriert sind. Stellen Sie schließlich sicher, dass Portgruppen entsprechend konfiguriert sind, damit Angreifer eine virtualisierte Umgebung nicht verwenden können, um die Netzwerksicherheitskontrollen zu umgehen.

Ordnungsgemäßes Konfigurieren von Speicher-Fabric-Verbindungen

Stellen Sie sicher, dass die Speicher-Fabric-Verbindungen die Verschlüsselung in Übertragung begriffener Daten verwenden oder auf ihren eigenen Netzwerksegmenten oder SANs isoliert sind, die über Perimetersteuerungen verfügen.

Der Schutz von Speicherdaten während der Übertragung trägt zur Gewährleistung der Vertraulichkeit der Daten bei. Verschlüsselung ist für viele Speichertechnologien keine Option, häufig aufgrund von Verfügbarkeits- oder Leistungsproblemen. In diesen Fällen kann die Isolierung auf ein dediziertes Netzwerksegment mit den entsprechenden Perimetersteuerungen eine effektive Ausgleichssteuerung sein und für eine mehrschichtige Verteidigung sorgen.

Verwenden der LUN-Maskierung auf Speichersystemen

Stellen Sie sicher, dass die Speichersysteme LUN-Maskierung, Zonenzuweisung und andere speicherseitige Sicherheitstechniken einsetzen, damit Speicherzuteilungen nur für den vSphere-Cluster sichtbar sind, in dem sie verwendet werden sollen.

Durch die LUN-Maskierung auf dem Speicher-Controller und die SAN-Zonenzuweisung wird sichergestellt, dass der Speicherdatenverkehr für nicht autorisierte Hosts nicht sichtbar ist und dass nicht autorisierte Hosts die Datenspeicher nicht mounten können, um damit andere Sicherheitskontrollen zu umgehen.

Begrenzen von Verbindungen zu autorisierten Systemen

Ziehen Sie die Verwendung der vCenter Server Appliance-Firewall in Betracht, um Verbindungen zu autorisierten Systemen und Administratoren zu begrenzen.

Die vCenter Server Appliance enthält eine einfache Firewall. Mit ihr können Sie eingehende Verbindungen auf vCenter Server begrenzen. In Kombination mit Perimetersicherheitssteuerungen kann dies für eine effektive mehrschichtige Verteidigung sorgen.

Stellen Sie wie immer vor dem Hinzufügen von Regeln zum Blockieren von Verbindungen sicher, dass Regeln vorhanden sind, die den Zugriff von administrativen Arbeitsstationen aus ermöglichen.

Kein Speichern von Verschlüsselungsschlüsseln ohne Absicherung des physischen Zugriffs auf ESXi-Hosts

Die Umgebung darf keine Verschlüsselungsschlüssel auf ESXi-Hosts speichern, ohne auch den physischen Zugriff auf die Hosts zu schützen.

Zum Verhindern von Abhängigkeitsschleifen speichert vSphere Native Key Provider Entschlüsselungsschlüssel direkt auf den ESXi-Hosts, entweder in einem Trusted Platform Module (TPM) oder als Teil der verschlüsselten ESXi-Konfiguration. Wenn Sie jedoch einen Host nicht physisch schützen und ein Angreifer den Host stiehlt, könnte der Angreifer verschlüsselte Arbeitslasten entsperren und ausführen. Daher ist es wichtig, physische Sicherheit zu gewährleisten (siehe Schutz von Systemen vor Manipulationen) oder sich für die Verwendung eines Standardschlüsselanbieters zu entscheiden (siehe Definition eines Standardschlüsselanbieters), der zusätzliche Netzwerksicherheitskontrollen enthält.

Verwenden von dauerhaften Nicht-USB-Geräten ohne SD mit ausreichender Größe für ESXi-Startvolumes

Die Umgebung muss dauerhafte Nicht-USB-Geräten ohne SD mit ausreichender Größe für ESXi-Startvolumes verwenden.

Flash-Arbeitsspeicher ist eine Komponente, die sich im Laufe der Zeit abnutzt, wobei jeder Datenschreibvorgang seine Lebensdauer verkürzt. SSDs und NVMe-Geräte verfügen über integrierte Funktionen, um diese Abnutzung zu reduzieren und sie zuverlässiger zu machen. SD-Karten und die meisten USB-Flashlaufwerke verfügen jedoch nicht über diese Funktionen und können oft ohne erkennbare Anzeichen im Laufe der Zeit Zuverlässigkeitsprobleme aufweisen, etwa fehlerhafte Sektoren.

Sie können beim Installieren von ESXi auf diesen Geräten Überwachungs- und Systemprotokolle auf einer RAM-Disk speichern, anstatt sie dauerhaft auf dem Gerät zu schreiben. Auf diese Weise sorgen Sie dafür, dass die Abnutzung abgemildert wird und USB-Geräte länger halten. Dies bedeutet, dass Sie neue langfristige Speicherorte für diese Protokolle einrichten und die Protokollausgabe ändern müssen, um an diese neuen Speicherorte zu gelangen.

Die Auswahl eines zuverlässigen Startgeräts entfernt diese zusätzlichen Schritte und hilft ESXi automatisch, Sicherheitsüberwachungen zu bestehen.

Ordnungsgemäßes Konfigurieren des vSAN iSCSI-Ziels

Stellen Sie sicher, dass das vSAN iSCSI-Ziel seine eigenen VMkernel-Netzwerkschnittstellen verwendet, die in seinem eigenen Netzwerksegment isoliert sind und separate Perimetersteuerungen mithilfe von Filterung und Markierung des verteilten Portgruppendatenverkehrs, NSX oder externer Netzwerksicherheitskontrollen verwendet.

Da sich die iSCSI-Zielclients außerhalb des Clusters befinden, isolieren Sie sie auf ihren eigenen Netzwerkschnittstellen. Auf diese Weise können Sie andere, ausschließlich interne Netzwerkkommunikationen separat einschränken. Die Isolierung dieses Typs hilft auch bei der Diagnose und Verwaltung der Leistung.

Referenz zu vSphere-Hardware-Sicherheitskontrollen

Diese Sicherheitskontrollen stellen einen Baseline-Satz von Best Practices für die Sicherheit der vSphere-Hardware bereit. Sie sind dahingehend gegliedert, dass die Vor- und Nachteile der Implementierung der Kontrolle verdeutlicht werden.

Verwendete Variable

Die in diesem Abschnitt vorgestellten PowerCLI-Befehle verwenden folgende Variable:

- $ESXi = "*host_name*"

Verwenden von Intel Trusted Execution Technology

Stellen Sie sicher, dass Intel Trusted Execution Technology (TXT) aktiviert ist, sofern in der System-Firmware verfügbar.

Plattformen mit skalierbaren Intel Xeon-Prozessoren verfügen über TXT, das die Authentizität einer Plattform und des zugehörigen Betriebssystems bietet. Bei Aktivierung nutzt ESXi die Sicherheitsvorteile dieser Technologie.

Vorgeschlagener Wert

Aktiviert

Potenzielle Auswirkung infolge der Änderung des Standardwerts

Frühzeitige Implementierungen von TXT führten gelegentlich dazu, dass das System plötzlich heruntergefahren wurde oder Nachweisalarme in vCenter Server ausgelöst wurden oder. Oder es kam zu Startfehlern. Ein Systemneustart behebt diese Probleme, während ein Update der System-Firmware dies in der Regel dauerhaft behebt. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/78243.

PowerCLI-Befehlsbeurteilung

```
(Get-VMHost -Name $ESXi | Get-View).Capability.TxtEnabled
```

Konfigurieren von UEFI Secure Boot

Stellen Sie sicher, dass UEFI Secure Boot aktiviert ist.

Das Aktivieren von UEFI Secure Boot auf der Hardware eines ESXi-Hosts hilft dabei, Malware und nicht vertrauenswürdige Konfigurationen zu verhindern.

Vorgeschlagener Wert

Aktiviert

Potenzielle Auswirkung infolge der Änderung des Standardwerts

Die Aktivierung von UEFI Secure Boot nach der Installation verhindert möglicherweise, dass ein ESXi-Host gestartet wird. Führen Sie `/usr/lib/vmware/secureboot/bin/secureBoot.py -c` auf einem Beispielhost aus, um zu ermitteln, ob Sie Secure Boot sicher aktivieren können.

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Verwenden von TPM 2.0

Stellen Sie sicher, dass ein Trusted Platform Module (TPM) 2.0 auf Ihren ESXi-Hosts installiert und ordnungsgemäß konfiguriert ist.

ESXi kann mithilfe eines TPM erweiterte Sicherheitsfunktionen aktivieren, die Malware verhindern, Abhängigkeiten entfernen und Hardware-Lebenszyklusvorgänge schützen. Konfigurieren Sie nach Möglichkeit Ihre Hosts für die Verwendung von TPM 2.0, und aktivieren Sie das TPM in der System-Firmware.

Vorgeschlagener Wert

TPM 2.0 installiert und aktiviert (SHA-256-Hashing, TIS/FIFO-Schnittstelle)

Potenzielle Auswirkung infolge der Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
(Get-VMHost -Name $ESXi | Get-View).Capability.TpmSupported
(Get-VMHost -Name $ESXi | Get-View).Capability.TpmVersion
```

Stetiges Verwenden der aktuellen Hardware-Firmware

Stellen Sie sicher, dass Sie die neuesten Firmware-Updates auf alle Komponenten Ihrer Systeme anwenden und dass die Firmware authentifiziert und von Ihrem Hardwarehersteller bereitgestellt wird.

Hardware-Firmware ist nicht immun gegen schwerwiegende Probleme, die die Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigen. Angreifer können anfällige Systemverwaltungs-Controller und Management-Engines verwenden, um Persistenz herzustellen und Hosts nach Neustarts und Updates zu infizieren und wieder zu kompromittieren.

Vorgeschlagener Wert

Nicht verfügbar

Potenzielle Auswirkung infolge der Änderung des Standardwerts

Wenn Sie vSAN verwenden, stellen Sie sicher, dass die Versionen des Speichergeräts und der Controller-Firmware zertifiziert sind.

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Sichere integrierte Hardwareverwaltungs-Controller

Stellen Sie sicher, dass integrierte Hardwareverwaltungs-Controller vollständig geschützt sind.

Viele Server verfügen über integrierte Hardwareverwaltungs-Controller, die bei der Überwachung und Aktualisierung von Hardware, Einstellungen und Firmware äußerst hilfreich sein können. Für diese Controller:

- Deaktivieren Sie alle nicht verwendeten Funktionen.
- Deaktivieren Sie alle nicht verwendeten Zugriffsmethoden.
- Legen Sie Kennwörter und Kennwortsteuerungen fest.
- Setzen Sie Firewalls und Zugriffssteuerung ein, sodass der Zugriff nur von autorisierten Arbeitsstationen für das Virtualisierungsverwaltungsteam erfolgt.

Deaktivieren Sie alle Konfigurationsoptionen für den ersten Start, insbesondere diejenigen, die das System von einem eingesteckten USB-Gerät aus neu konfigurieren. Deaktivieren oder schützen Sie außerdem USB-Ports, die an Verwaltungs-Controller angeschlossen sind. Legen Sie nach Möglichkeit USB-Ports so fest, dass nur Tastaturen zulässig sind.

Ändern Sie Standardkennwörter für Konten.

Sichere externe Informationen werden angezeigt, um zu verhindern, dass Informationen durchsickern. Schützen Sie Schaltflächen zum Ein-/Ausschalten und für Informationen vor unbefugter Nutzung.

Viele Hardwareverwaltungs-Controller bieten Warnungsmechanismen, wenn Hardwarefehler und Konfigurationsänderungen auftreten. Sie sollten diese verwenden, wenn Sie keine andere Methode für die Hardwareüberwachung verwenden.

Vorgeschlagener Wert

Nicht verfügbar

Potenzielle Auswirkung infolge der Änderung des Standardwerts

Das Deaktivieren von Verbindungsmethoden kann zu künftigen Überwachungs- und Verwaltungsänderungen an den Hardwareverwaltungs-Controller-Konfigurationen auf Ihren bereitgestellten Servern führen. Verwenden Sie nach Möglichkeit CLI- und API-Verwaltungsmethoden, die Sie per Skript erstellen können, anstatt zusätzliche Verwaltungssoftware oder -anwendungen zu verwenden. Das Erlernen dieser Techniken spart Zeit, vermeidet den zusätzlichen Aufwand für die Installation und Wartung zusätzlicher Tools und ermöglicht rechtzeitige Konfigurationsänderungen.

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Synchronisieren der Uhrzeit auf integrierten Hardwareverwaltungs-Controllern

Stellen Sie sicher, dass Sie die Uhrzeit auf integrierten Hardwareverwaltungs-Controllern synchronisieren.

Kryptografie, Überwachungsprotokollierung, Clustervorgänge und Reaktion auf Vorfälle hängen von der synchronisierten Uhrzeit ab. Diese Empfehlung gilt für alle Geräte in Ihrer Infrastruktur. Für NTP (Network Time Protocol) müssen mindestens vier Quellen verfügbar sein. Wenn Sie sich zwischen zwei Quellen oder einer Quelle entscheiden müssen, sollten Sie eine Quelle vorziehen.

Vorgeschlagener Wert

Standortspezifisch oder:

0.vmware.pool.ntp.org,

1.vmware.pool.ntp.org,

2.vmware.pool.ntp.org,

3.vmware.pool.ntp.org

Potenzielle Auswirkung infolge der Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Schützen der Art und Weise der Verwendung von Active Directory durch integrierte Hardwareverwaltungs-Controller

Stellen Sie sicher, dass Sie weder eine Abhängigkeitsschleife noch einen Angriffsvektor erstellen, wenn integrierte Hardwareverwaltungs-Controller Active Directory verwenden.

Deaktivieren Sie Verbindungen mit Active Directory, oder betrachten Sie sie mindestens als Angriffsvektoren und Abhängigkeitsschleifen (für Authentifizierung, Autorisierung, DNS, DHCP und Uhrzeit). Ziehen Sie in Erwägung, lokale Konten auf diesen Geräten über APIs und CLIs zu verwalten. Wenn Sie Active Directory für die Authentifizierung verwenden müssen, verwenden Sie die lokale Autorisierung, damit Angreifer mit Zugriff auf Active Directory sich nicht selbst über die Gruppenmitgliedschaft heraufstufen können.

Vorgeschlagener Wert

Nicht verfügbar

Potenzielle Auswirkung infolge der Änderung des Standardwerts

Wenn Hardwareverwaltungscontroller nicht mit zentralen Authentifizierungs- und Autorisierungsquellen verbunden werden, ist eine zusätzliche Verwaltung erforderlich. Die meisten Hardwareverwaltungs-Controller verfügen über CLI-Toolkits oder APIs, um den Prozess zu automatisieren.

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Deaktivieren von virtuellen integrierten Hardwareverwaltungs-Controllern

Stellen Sie sicher, dass integrierte Hardwareverwaltungs-Controller mit internen, emulierten oder virtuellen Netzwerkschnittstellen deaktiviert sind.

Einige Hardwareverwaltungs-Controller haben die Möglichkeit, ESXi virtuelle Netzwerkschnittstellen als Verwaltungsschnittstelle zu präsentieren. Diese Ansätze schaffen potenzielle Hintertüren für den Zugriff, die Angreifer verwenden können, um netzwerkbasierte Firewalls und Perimeter-Firewalls in beide Richtungen zu umgehen und die Beobachtung durch IDS, IPS und Bedrohungsanalysetools zu vermeiden. In vielen Fällen ist diese Funktionalität für die Verwaltung von Hosts nicht unbedingt erforderlich.

Vorgeschlagener Wert

Nicht verfügbar

Potenzielle Auswirkung infolge der Änderung des Standardwerts

Das Deaktivieren interner Netzwerke kann die Effektivität des Anbieterverwaltungstools einschränken.

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Aktivieren von AMD Secure Encrypted Virtualization-Encrypted State

Stellen Sie sicher, dass AMD Secure Encrypted Virtualization-Encrypted State (SEV-ES) aktiviert ist, sofern in der System-Firmware verfügbar. Stellen Sie sicher, dass der Wert für Mindestanzahl SEV-Nicht-ES-ASID der Anzahl an virtuellen SEV-ES-Maschinen plus eins entspricht.

AMD EPYC-Plattformen unterstützen SEV-ES, eine Technologie zum Verschlüsseln des Arbeitsspeicher- und CPU-Registerstatus und zur Einschränkung der Sichtbarkeit auf den Hypervisor, um die Sicherheit der Arbeitslast zu erhöhen und die Offenlegung gegenüber bestimmten Arten von Angriffen zu verringern. Bei ordnungsgemäßer Konfiguration bietet SEV-ES erweiterte Sicherheit für das Gastbetriebssystem auf virtuellen Maschinen und Containern unter vSphere und vSphere with Tanzu. Die Aktivierung von SEV-ES in der System-Firmware erleichtert die künftige Aktivierung innerhalb virtueller Maschinen, Container und Gastbetriebssysteme.

Vorgeschlagener Wert

Aktiviert (Wert für Mindestanzahl SEV-Nicht-ES-ASID entspricht der Anzahl an virtuellen SEV-ES-Maschinen plus eins)

Potenzielle Auswirkung infolge der Änderung des Standardwerts

Das Gastbetriebssystem für eine virtuelle Maschine muss SEV-ES unterstützen und schränkt daher einige Funktionen wie vMotion, Snapshots usw. ein. Weitere Informationen zu diesen Kompromissen finden Sie unter Nicht unterstützte VMware-Funktionen in SEV-ES.

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Aktivieren von Virtual Intel Software Guard Extensions (vSGX)

Stellen Sie sicher, dass Virtual Intel® Software Guard Extensions (vSGX) aktiviert ist, sofern in der System-Firmware verfügbar.

Plattformen mit skalierbaren Intel Xeon-Prozessoren verfügen über Software Guard Extensions (SGX), eine Technologie, mit der Anwendungen Daten im Systemspeicher schützen können. Bei ordnungsgemäßer Konfiguration unterstützt vSphere die Verwendung von SGX innerhalb virtueller Maschinen. Die Aktivierung von SGX in der System-Firmware erleichtert die künftige Aktivierung innerhalb virtueller Maschinen und Gastbetriebssysteme.

Vorgeschlagener Wert

Vorgeschlagen: Aktiviert (Software, entsperrt)

Potenzielle Auswirkung infolge der Änderung des Standardwerts

Das Gastbetriebssystem für eine virtuelle Maschine muss vSGX unterstützen und schränkt daher einige Funktionen wie vMotion, Snapshots usw. ein. Weitere Informationen zu diesen Kompromissen finden Sie unter Nicht unterstützte VMware-Funktionen auf vSGX.

PowerCLI-Befehlsbeurteilung

```
(Get-VMHost -Name $ESXi | Get-View).Capability.SgxRegistrationSupported
```

Deaktivieren von externen Ports

Stellen Sie sicher, dass nicht verwendete externe Ports deaktiviert oder vor unbefugter Nutzung geschützt sind.

Nicht verwendete Ports, insbesondere USB, können von Angreifern zum Anhängen von Speicher, Netzwerken und Tastaturen verwendet werden. Ergreifen Sie angemessene Schritte, um den Zugriff auf diese Ports durch Deaktivierung und Zugriffssteuerung zu kontrollieren. Verwenden Sie nach Möglichkeit andere Mittel wie stabile Rack-Türen, Rack-Seitenverkleidungen und Bodenbeläge, um die Ports außerhalb des Racks unzugänglich zu machen, wenn die Rack-Tür geschlossen ist. Beachten Sie, dass Kabel leicht durch viele Lücken in und um Racks und Rack-Türen passen. Zudem können steife Drähte verwendet werden, um Kabel von außerhalb des Racks in Steckdosen zu schieben und Kabel zu trennen, um eine Unterbrechung des Betriebs zu verursachen.

Legen Sie nach Möglichkeit USB-Ports so fest, dass nur Tastaturen zulässig sind.

Beachten Sie bei der Deaktivierung dieser Art von Funktionalität, dass Sie möglicherweise während eines Ausfalls oder als Teil von Lebenszyklusvorgängen mithilfe einer USB-Tastatur auf einen Server zugreifen müssen, und planen Sie dies entsprechend.

Vorgeschlagener Wert

Nicht verfügbar

Potenzielle Auswirkung infolge der Änderung des Standardwerts

Beim Thema Sicherheit muss man immer einen Kompromiss eingehen. Wenn Sie eine Sicherheitskontrolle in Betracht ziehen, etwa die Deaktivierung externer Ports, sollten Sie auch eine einfache Wiederherstellung nach einem Ausfall oder Vorfall berücksichtigen. In

diesem Fall beeinträchtigt die Deaktivierung externer Ports die Möglichkeit, im Notfall die ESXi-Konsole zu verwenden.

Einige Server können bestimmte USB-Ports für die Verwaltung dynamisch deaktivieren und aktivieren. Stellen Sie sicher, dass Ihre Auswahl für diese Sicherheitskontrolle den Anforderungen Ihrer Organisation entspricht und dass Sie diese Methoden testen, bevor Sie sie implementieren.

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Referenz der ESXi-Sicherheitskontrollen

Diese Sicherheitskontrollen stellen einen grundlegenden Satz bewährter Methoden für die ESXi-Sicherheit bereit. Sie sind dahingehend gegliedert, dass die Vor- und Nachteile der Implementierung der Kontrolle verdeutlicht werden. Die meisten Kontrollen stellen erweiterte Systemeinstellungen dar. Erweiterte Systemeinstellungen können Sie entweder über die bereitgestellte PowerCLI ändern oder unter vSphere Client (**Host > Konfigurieren > System > Erweiterte Systemeinstellungen**).

Verwendete Variable

Die in diesem Abschnitt aufgeführten PowerCLI-Befehle verwenden folgende Variablen:

- $ESXi = "*host_name*"
- $vmkernel_interface = "*vmkernel_adapter*"

Verweigern des Zugriffs des DCUI-Kontos

Der ESXi-Host muss dem DCUI-Benutzerkonto den Shell-Zugriff verweigern.

Das DCUI-Benutzerkonto wird zur Prozessisolierung für die DCUI selbst verwendet. Um die Angriffsfläche zu verringern, deaktivieren Sie für das DCUI-Benutzerkonto den Shell-Zugriff.

Werte

Standardwert der Installation: True.

Empfohlener Baseline-Wert: False

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.account.list.Invoke() | Where-Object { $_.UserID -eq 'dcui' } | Select-
Object -ExpandProperty Shellaccess
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.account.set.CreateArgs()
$arguments.id = "dcui"
$arguments.shellaccess = "false"
$ESXcli.system.account.set.Invoke($arguments)
```

Annotations.WelcomeMessage

Konfiguriert den Text der Anmeldenachricht, die auf dem VMware Host Client und der DCUI angezeigt wird.

ESXi bietet die Möglichkeit, eine Anmeldenachricht anzuzeigen. Die Anmeldenachricht wird beispielsweise dazu verwendet, Eindringlinge über die Rechtswidrigkeit ihrer Aktivitäten zu informieren und autorisierten Benutzern mitzuteilen, welche Erwartungen und Verpflichtungen sie bei der Verwendung des Systems erfüllen und akzeptieren müssen.

Werte

Standardwert der Installation: Nicht definiert

Empfohlener Baseline-Wert: Erkundigen Sie sich bei den Rechtsabteilung Ihrer Organisation nach dem für Ihre Umgebung passenden Text.

Beispielnachricht: Nur für autorisierte Benutzer. Die vollzogene oder versuchte unbefugte Nutzung dieses Systems ist verboten und kann straf-, zivil-, sicherheits- oder verwaltungsrechtliche Konsequenzen und/oder Sanktionen nach sich ziehen. Durch die Nutzung dieses Informationssystems erklären Sie sich mit der Überwachung und Aufzeichnung ohne vorherige Ankündigung oder Genehmigung einverstanden. Bei der Nutzung dieses Systems haben Benutzer keinen Anspruch auf Privatsphäre. Sämtliche auf diesem System gespeicherten oder über dieses System übertragenen oder durch Überwachung und/oder Aufzeichnung erlangten Informationen können für Strafverfolgungsbehörden offengelegt und/oder gemäß Bundes- und Landesgesetzen sowie den Richtlinien der Organisation verwendet werden. Verlassen Sie jetzt das System, wenn Sie kein autorisierter Benutzer dieses Systems sind.

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Maskiert die „F2/F12“- und IP-Adressinformationen auf der DCUI. Möglicherweise erfordert Ihre Umgebung auch eine Dokumentation und Schulung.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Annotations.WelcomeMessage
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Annotations.WelcomeMessage | Set-
AdvancedSetting -Value "your_message"
```

Config.HostAgent.vmacore.soap.sessionTimeout

Konfiguriert für die vSphere API eine Zeitüberschreitung für die Sitzung.

Diese trägt dazu bei, potenzielle Sicherheitsrisiken zu verringern, indem sichergestellt wird, dass unbeaufsichtigte Sitzungen nicht unbefristet offen bleiben, wodurch sie von nicht autorisierten Benutzern oder Schadsoftware ausgenutzt werden könnten.

Werte

Standardwert der Installation: 30

Empfohlener Baseline-Wert: 30

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.vmacore.soap.sessionTimeout
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.vmacore.soap.sessionTimeout
| Set-AdvancedSetting -Value 30
```

Config.Etc.issue

Konfiguriert den Text des Banners, das angezeigt wird, wenn ein Benutzer mittels SSH eine Verbindung zu einem ESXi-Host herstellt.

ESXi bietet die Möglichkeit, Banner für SSH-Verbindungen anzuzeigen. Ein Banner wird beispielsweise verwendet, um Eindringlinge über die Rechtswidrigkeit ihrer Aktivitäten zu informieren und autorisierten Benutzern mitzuteilen, welche Erwartungen und Verpflichtungen sie bei der Nutzung des Systems einhalten und akzeptieren müssen. Lassen Sie den SSH-Dienst deaktiviert, solange Sie keine Fehlerbehebung durchführen. Eine Inkonsistenz der Implementierung von ESXi und vCenter Server erfordert, dass „issue“ in `Config.Etc.issue` klein geschrieben wird, damit beide Szenarien funktionieren.

Werte

Standardwert der Installation: Nicht definiert

Empfohlener Baseline-Wert: Erkundigen Sie sich bei den Rechtsabteilung Ihrer Organisation nach dem für Ihre Umgebung passenden Text.

Beispielnachricht: Nur für autorisierte Benutzer. Die vollzogene oder versuchte unbefugte Nutzung dieses Systems ist verboten und kann straf-, zivil-, sicherheits- oder verwaltungsrechtliche Konsequenzen und/oder Sanktionen nach sich ziehen. Durch die Nutzung dieses Informationssystems erklären Sie sich mit der Überwachung und Aufzeichnung ohne vorherige Ankündigung oder Genehmigung einverstanden. Bei der Nutzung dieses Systems haben Benutzer keinen Anspruch auf Privatsphäre. Sämtliche auf diesem System gespeicherten oder über dieses System übertragenen oder durch Überwachung und/oder Aufzeichnung erlangten Informationen können für Strafverfolgungsbehörden offengelegt und/oder gemäß Bundes- und Landesgesetzen sowie den Richtlinien der Organisation verwendet werden. Verlassen Sie jetzt das System, wenn Sie kein autorisierter Benutzer dieses Systems sind.

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.Etc.issue
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.Etc.issue | Set-AdvancedSetting
-Value "**************************************************************************`n*
Authorized users only. Actual or attempted unauthorized use of this      *`n* system
is prohibited and may result in criminal, civil, security, or     *`n* administrative
proceedings and/or penalties. Use of this information     *`n* system indicates consent to
monitoring and recording, without notice     *`n* or permission. Users have no expectation
of privacy. Any information     *`n* stored on or transiting this system, or obtained
by monitoring and/or    *`n* recording, may be disclosed to law enforcement and/or used
in accordance *`n* with Federal law, State statute, and organization policy. If you
```

```
are not *`n* an authorized user of this system, exit the system at this time.
*`n**************************************************************************`n"
```

Deaktivieren des Shell-Zugriffs für vpxuser

Der ESXi-Host muss den Shell-Zugriff für das vpxuser-Konto verweigern.

vCenter Server erstellt das vpxuser-Konto, wenn ein ESXi-Host erstmalig angehängt wird. Das vpxuser-Konto wird anschließend für die privilegierte Authentifizierung bei ESXi verwendet. Während vCenter Server das Kennwort für das vpxuser-Konto automatisch in einem mit der Option `VirtualCenter.VimPasswordExpirationInDays` festgelegten Intervall rotiert, verfügt das vpxuser-Konto auch über Shell-Zugriff. Deaktivieren Sie das vpxuser-Konto, um die Angriffsfläche zu verringern.

Werte

Standardwert der Installation: True.

Empfohlener Baseline-Wert: False

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Benutzerkonten ohne Shell-Zugriff können den Shell-Zugriff anderer Benutzer nicht neu konfigurieren. Dies gilt unabhängig von ihrer Berechtigungsstufe. Da vCenter Server eine Verbindung mit einem ESXi-Host über das vpxuser-Konto herstellt, kann dieses nach dem Deaktivieren des Shell-Zugriffs für vpxuser nicht mehr verwendet werden, um diese Kontoeinstellungen für andere Konten zu ändern. Weitere Neukonfigurationen müssen für jeden Host einzeln bei Verwendung eines autorisierten Kontos erfolgen.

ESXi 8.0 und höher unterstützt keine herkömmlichen Kennwort- oder Kontowiederherstellungen mehr, wie das Starten von einem Medium oder das Ändern von „init“ in eine Shell beim Starten.

Stellen Sie sicher, dass auf dem ESXi-Host mindestens ein Benutzerkonto mit vollständigen Berechtigungen erhalten bleibt und schützen Sie dieses Konto entsprechend.

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.account.list.Invoke() | Where-Object { $_.UserID -eq 'vpxuser' } | Select-
Object -ExpandProperty Shellaccess
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.account.set.CreateArgs()
$arguments.id = "vpxuser"
```

```
$arguments.shellaccess = "false"
$ESXcli.system.account.set.Invoke($arguments)
```

vCenter Server muss den vSphere Authentication Proxy verwenden, um das Speichern von Active Directory-Anmeldedaten zu vermeiden

Mit dem vSphere Authentication Proxy kann vCenter Server eine Verbindung mit Active Directory-Entitäten herstellen und diese verwalten, ohne dass Active Directory-Anmeldedaten direkt gespeichert werden müssen. Dies verringert das Risiko einer Offenlegung oder eines Missbrauchs von Anmeldedaten.

Werte

Standardwert der Installation: Nicht konfiguriert

Empfohlener Baseline-Wert: Konfigurieren, wenn die Funktion verwendet wird

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-VMHostAuthentication | Select-Object
VMHost,Domain,DomainMembershipStatus
```

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar

DCUI.Access

Der ESXi-Host muss über eine exakte DCUI.Access-Liste verfügen.

Legt die Liste der Benutzerausnahmen für den Sperrmodus so fest, dass diese eine exakte Liste von Benutzern enthält, und stellt sicher, dass nur autorisierte Benutzer direkten DCUI-Zugriff auf den ESXi-Host haben, wenn der Sperrmodus aktiviert ist.

Der Root-Benutzer kann nicht aus der Liste entfernt werden.

Verwenden Sie die Liste der Benutzerausnahmen für den Sperrmodus, um den Zugriff auf die ESXi Shell und SSH zu kontrollieren. Weitere Informationen hierzu finden Sie unter Vorhandenseins einer exakten Liste der ausgenommenen Benutzer auf dem ESXi-Host.

Werte

Standardwert der Installation: root

Empfohlener Baseline-Wert: root

Aktion erforderlich

Überprüfen Sie die Liste.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Potenzieller Verlust des Administratorzugriffs auf Hosts. Stellen Sie vor dem Konfigurieren des Sperrmodus sicher, dass ESXi-Hosts an vCenter Server angehängt sind und dass Zugriffslisten und Ausnahmelisten konfiguriert werden.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting DCUI.Access
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting DCUI.Access | Set-AdvancedSetting -Value root
```

Vorhandenseins einer exakten Liste der ausgenommenen Benutzer auf dem ESXi-Host

Der ESXi-Host muss über eine exakte Liste der ausgenommenen Benutzer verfügen.

In der Liste „Benutzerausnahmen für den Sperrmodus“ aufgeführte Benutzer verlieren ihre Berechtigungen nicht, wenn der Host in den Sperrmodus wechselt. Diese Situation kann gegebenenfalls den Zweck des Sperrmodus zunichte machen.

Werte

Standardwert der Installation: Null

Empfohlener Baseline-Wert: Null

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Potenzieller Verlust des Administratorzugriffs auf ESXi-Hosts. Stellen Sie vor dem Konfigurieren des Sperrmodus sicher, dass ESXi-Hosts an vCenter Server angehängt sind und dass Zugriffslisten und Ausnahmelisten konfiguriert werden.

PowerCLI-Befehlsbeurteilung

```
(Get-View (Get-VMHost -Name $ESXi | Get-
View).ConfigManager.HostAccessManager).QueryLockdownExceptions()
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
(Get-View (Get-VMHost -Name $ESXi | Get-
View).ConfigManager.HostAccessManager).UpdateLockdownExceptions($NULL)
```

Aktivieren des normalen Sperrmodus zur Beschränkung des Zugriffs auf ESXi

Die Aktivierung des Sperrmodus deaktiviert den direkten Zugriff auf einen ESXi-Host. Der Sperrmodus erfordert, dass vCenter Server den ESXi-Host direkt verwaltet.

Eine Beschränkung des Zugriffs auf diesem Weg stellt sicher, dass vCenter Server Rollen und Berechtigungen erzwingt. Benutzer können diese Rollen und Berechtigungen auch nicht umgehen, indem sie sich direkt bei einem ESXi-Host anmelden. Indem sämtliche Interaktionen über vCenter Server erfolgen müssen, verringert sich das Risiko, dass Benutzer versehentlich erhöhte Berechtigungen erlangen oder Aufgaben ausführen, für die sie nicht ordnungsgemäß überwacht werden.

Benutzer, die in der Liste „Ausnahme für Benutzer“ der einzelnen ESXi-Hosts aufgeführt sind, sind berechtigt, den Sperrmodus außer Kraft zu setzen und sich anzumelden. Standardmäßig sind in der Liste der ausgenommenen Benutzer keine Benutzer enthalten.

Mögliche Einstellungen für den Sperrmodus sind „Deaktiviert“, „Normal“ und „Streng“. Wenn der Sperrmodus auf „Streng“ festgelegt ist und der ESXi-Host den Kontakt zu vCenter Server verliert, können Sie diesen erst wieder verwalten, nachdem die Verbindung wiederhergestellt wurde. Wenn Sie die Verbindung nicht wiederherstellen können, müssen Sie den ESXi-Host neu erstellen. In der Regel geht der Sperrmodus „Streng“ über die Anforderungen der meisten Bereitstellungen hinaus. Der Sperrmodus „Normal“ ist in den meisten Fällen ausreichend.

Werte

Standardwert der Installation: lockdownDisabled

Empfohlener Baseline-Wert: lockdownNormal

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Potenzieller Verlust des Administratorzugriffs auf Hosts. Stellen Sie vor dem Konfigurieren des Sperrmodus sicher, dass ESXi-Hosts an vCenter Server angehängt sind und dass Zugriffslisten und Ausnahmelisten konfiguriert werden.

Für einige Vorgänge, z. B. die Sicherung und Fehlerbehebung, ist ein direkter Zugriff auf den ESXi-Host erforderlich. In diesen Fällen können Sie den Sperrmodus für bestimmte Hosts vorübergehend deaktivieren und ihn erneut aktivieren, sobald Sie fertig sind.

PowerCLI-Befehlsbeurteilung

```
(Get-View (Get-VMHost -Name $ESXi | Get-View).ConfigManager.HostAccessManager).LockdownMode
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
(Get-View (Get-VMHost -Name $ESXi | Get-
View).ConfigManager.HostAccessManager).ChangeLockdownMode('lockdownNormal')
```

Syslog.global.auditRecord.storageEnable

Konfiguriert Sie den ESXi-Host für das lokale Speichern von Prüfdatensätzen.

Sie müssen auf ESXi-Hosts die Protokollierung der Überwachungsdatensätze aktivieren.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: True

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Für Protokolle wird zusätzlicher Speicherplatz benötigt.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageEnable
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageEnable | Set-
AdvancedSetting -Value TRUE
```

Syslog.global.auditRecord.storageCapacity

Auf ESXi-Hosts müssen Sie ausreichend Speicherkapazität für die Überwachungsdatensätze einer Woche aktivieren.

Wenn ein Remote-Speichergerät für Prüfdatensätze vorhanden ist, muss unbedingt sichergestellt werden, dass die lokale Speicherkapazität ausreicht, um Prüfdatensätze aufzunehmen, die sich während möglicher Unterbrechungen der Datenübermittlung auf dem Gerät ansammeln. Dadurch wird sichergestellt, dass in Zeiten, in denen der Remote-Speicher nicht verfügbar ist, keine Prüfdatensätze verloren gehen oder überschrieben werden. Dies sichert die nahtlose Kontinuität des Prüfpfads und sorgt für die Einhaltung der Compliance-Anforderungen.

Werte

Standardwert der Installation: 4

Empfohlener Baseline-Wert: 100

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Für Protokolle wird zusätzlicher Speicherplatz benötigt.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageCapacity
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageCapacity |
Set-AdvancedSetting -Value 100
```

ScratchConfig.CurrentScratchLocation and Syslog.global.auditRecord.storageDirectory

Konfiguriert einen dauerhaften Protokollspeicherort für alle lokal auf dem ESXi-Host gespeicherten Überwachungsdatensätze.

Sie können ESXi so konfigurieren, dass Prüfdatensätze in einem In-Memory-Dateisystem gespeichert werden. Dies passiert, wenn das Verzeichnis „/scratch“ des Hosts mit „/tmp/scratch“ verknüpft ist. Anschließend werden immer nur die Datensätze eines einzigen Tages gespeichert. Darüber hinaus werden Prüfdatensätze bei jedem Neustart neu initialisiert. Dies stellt ein Sicherheitsrisiko dar, da die auf dem Host protokollierte Benutzeraktivität nur temporär gespeichert wird und bei Neustarts verloren geht. Dies kann auch die Überprüfung und die Überwachung von Ereignissen sowie die Diagnose von Problemen erschweren. Konfigurieren Sie die Protokollierung von ESXi-Host-Überwachungsdatensätzen immer in einem persistenten Datenspeicher.

Sie können ermitteln, ob der Scratch-Datenträger temporär oder persistent ist, indem Sie die erweiterte Einstellung `ScratchConfig.CurrentScratchLocation` abfragen. Wenn bei der Abfrage „/tmp/scratch“ zurückgegeben wird, handelt es sich um einen temporären Datenspeicher. In diesem Fall sollten Sie den Speicher für die Prüfdatensätze erneut einem persistenten Gerät zuordnen.

Der Speicher darf kein vSAN-Datenspeicher sein. Wenn Ihr einziger lokaler, Nicht-vSAN-Speicher ein SD- oder USB-Medium ist (das bei wiederholtem Schreiben von Protokollen unzuverlässig werden kann), sollten Sie die Protokolle auf der Ramdisk belassen und stattdessen einen Host für die Remoteprotokollierung konfigurieren. Dokumentieren Sie die Entscheidung und die Gründe für zukünftige Prüfungen.

Werte

Standardwert der Installation:

`ScratchConfig.CurrentScratchLocation`: Hängt vom Startgerät ab

`Syslog.global.auditRecord.storageDirectory`: `/scratch/auditLog`

Empfohlener Baseline-Wert: Dauerhafter Speicherort

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Für Protokolle wird zusätzlicher Speicherplatz benötigt.

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.syslog.config.get.Invoke() | Select
LocalLogOutput,LocalLogOutputIsPersistent

# If your LocalLogOutput is set to a directory in /scratch, and LocalLogOutputIsPersistent
is true, that means your boot device is of a type and size that makes /scratch persistent.
Verify that your audit storage is also on /scratch, and that /scratch points to a VMFS
datastore:

Get-VMHost -Name $ESXi | Get-AdvancedSetting ScratchConfig.CurrentScratchLocation
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageDirectory
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageDirectory |
Set-AdvancedSetting -Value "/vmfs/volumes/$Datastore/audit"
```

Syslog.global.auditRecord.remoteEnable

Konfiguriert den ESXi-Host für die Übertragung von Überwachungsprotokollen auf einen Remotehost.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: True

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.remoteEnable
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.remoteEnable | Set-
AdvancedSetting -Value TRUE
```

Syslog.global.logFiltersEnable

Aktiviert die Protokollfilterung auf dem ESXi-Host.

Sie können Protokollfilter erstellen, um die Anzahl doppelter Einträge in den Protokollen zu reduzieren und bestimmte Protokollereignisse komplett zu sperren.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: False

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logFiltersEnable
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logFiltersEnable | Set-
AdvancedSetting -Value FALSE
```

LocalLogOutputIsPersistent, ScratchConfig.CurrentScratchLocation und Syslog.global.logDir

Konfiguriert die dauerhafte Protokollierung aller lokal gespeicherten Protokolle auf dem ESXi-Host.

Sie können ESXi so konfigurieren, dass Protokolldateien in einem speicherresidenten Dateisystem gespeichert werden. Dies passiert, wenn das Verzeichnis „/scratch“ des Hosts mit „/tmp/scratch“ verknüpft ist. Anschließend werden immer nur die Protokolle eines einzigen Tages gespeichert. Darüber hinaus werden Protokolldateien bei jedem Neustart neu initialisiert. Dies stellt ein Sicherheitsrisiko dar, da die auf dem Host protokollierte Benutzeraktivität nur temporär gespeichert wird und bei Neustarts verloren geht. Das kann auch die Überprüfung und die Überwachung von Ereignissen sowie die Diagnose von Problemen erschweren. Konfigurieren Sie auf dem ESXi-Host die Protokollierung immer in einem persistenten Datenspeicher.

Sie können ermitteln, ob der Scratch-Datenträger temporär oder persistent ist, indem Sie den erweiterten Parameter `ScratchConfig.CurrentScratchLocation` abfragen. Wenn bei der Abfrage „/tmp/scratch“ zurückgegeben wird, handelt es sich um einen temporären Datenspeicher. In diesem Fall sollten Sie den Speicher für die Prüfdatensätze erneut einem persistenten Gerät zuordnen.

Der Speicher darf kein vSAN-Datenspeicher sein, es sei denn, Sie legen `Syslog.global.vsanBacking` fest, was Einschränkungen und Abhängigkeiten mit sich bringt. Wenn Ihr einziger lokaler, Nicht-vSAN-Speicher ein SD- oder USB-Medium ist (das bei wiederholtem Schreiben von Protokollen unzuverlässig werden kann), sollten Sie die Protokolle auf der Ramdisk belassen und stattdessen einen Host für die Remoteprotokollierung konfigurieren. Dokumentieren Sie die Entscheidung und die Gründe für zukünftige Prüfungen.

Werte

Standardwert der Installation: `ScratchConfig.CurrentScratchLocation`: Vom Startgerät abhängig

`Syslog.global.logDir`: `/scratch/log`

Empfohlener Baseline-Wert: Dauerhafter Speicherort

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.syslog.config.get.Invoke() | Select
LocalLogOutput,LocalLogOutputIsPersistent

# If your LocalLogOutput is set to a directory in /scratch, and LocalLogOutputIsPersistent
is true, that means your boot device is of a type and size that makes /scratch persistent.
Verify that your log storage is also on /scratch, , and that /scratch points to a VMFS
datastore:
```

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting ScratchConfig.CurrentScratchLocation
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logDir
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logDir | Set-AdvancedSetting
-Value "/vmfs/volumes/$Datastore/logs"
```

Syslog.global.logHost

Konfiguriert die Remoteprotokollierung.

Wenn Sie die Remoteprotokollierung auf einem zentralen Protokoll-Host konfigurieren, stellen Sie für ESXi-Protokolle einen sicheren, zentralisierten Speicher bereit. Das Sammeln von Host-Protokolldateien auf einem zentralen Host eröffnet Ihnen die Möglichkeit, alle Hosts mit einem einzigen Tool zu überwachen. Sie können auch aggregierte Analysen durchführen und nach Elementen wie koordinierten Angriffen auf mehrere Hosts suchen. Die Protokollierung auf einem sicheren, zentralen Protokollserver unterstützt das Verhindern von Protokollmanipulation und bietet außerdem eine langfristige Prüfungsaufzeichnung.

Werte

Standardwert der Installation: Nicht definiert

Empfohlener Baseline-Wert: Standortspezifisch

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logHost
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logHost | Set-AdvancedSetting
-Value "log_collector"
```

Syslog.global.certificate.checkSSLCerts

Verifiziert Zertifikate für TLS.

Der ESXi-Host muss Zertifikate für Endpoints für die TLS-Remoteprotokollierung verifizieren. Mit TLS-Zertifikaten kann sichergestellt werden, dass ein Endpoint authentifiziert und vertrauenswürdig ist.

Werte

Standardwert der Installation: True.

Empfohlener Baseline-Wert: True

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.certificate.checkSSLCerts
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.certificate.checkSSLCerts | Set-AdvancedSetting -Value TRUE
```

Syslog.global.certificate.strictX509Compliance

Führt eine strenge x509-Verifizierung für TLS-fähige Remoteprotokollierungs-Endpoints durch.

Der ESXi-Host muss eine strenge x509-Verifizierung für TLS-fähige Remoteprotokollierungs-Endpoints anwenden. Die Einstellung `Syslog.global.certificate.strictX509Compliance` führt während der Verifizierung zusätzliche Gültigkeitsprüfungen der CA-Root-Zertifikate durch.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: True

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.certificate.strictX509Compliance
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting
Syslog.global.certificate.strictX509Compliance | Set-AdvancedSetting -Value TRUE
```

Mem.MemEagerZero

Aktiviert die Vernichtung flüchtiger Schlüssel.

Standardmäßig setzt ESXi Seiten, denen virtuelle Maschinen, Benutzerbereichsanwendungen und Kernel-Threads zugeteilt wurden, im Moment der Zuteilung auf Null. Dadurch wird sichergestellt, dass keine nicht auf Null gesetzte Seiten für virtuelle Maschinen oder Benutzerbereichsanwendungen offengelegt werden. Diese Maßnahme dient dazu, zu verhindern, dass kryptografische Schlüssel von virtuellen Maschinen oder Benutzerwelten für andere Clients offengelegt werden.

Wenn der Arbeitsspeicher jedoch nicht wiederverwendet wird, können diese Schlüssel über einen längeren Zeitraum im Arbeitsspeicher des Hosts verbleiben. Um dies zu beheben, können Sie die Einstellung `MemEagerZero` dahingehend konfigurieren, dass das Nullsetzen von Benutzerwelt- und Gast-Arbeitsspeicherseiten erzwungen wird, wenn ein Benutzerwelt-Prozess oder Gast aussteigt. Bei Kernel-Threads werden Speicherbereiche, die Schlüssel enthalten, auf Null gesetzt, sobald das Geheimnis nicht mehr benötigt wird.

Werte

Standardwert der Installation: 0

Empfohlener Baseline-Wert: 1

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Für virtuelle Maschinen ist für das Herunterfahren zusätzliche Zeit erforderlich, die dem Umfang des zugewiesenen Speichers entspricht.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Mem.MemEagerZero
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Mem.MemEagerZero | Set-AdvancedSetting -Value
1
```

Prüfung auf aktive Wartung der ESXi-Version

Stellen Sie sicher, dass die ESXi-Version nicht den VMware-Status „Ende des allgemeinen Supports“ erreicht hat.

Werte

Standardwert der Installation: Nicht verfügbar

Empfohlener Baseline-Wert: Nicht verfügbar

Aktion erforderlich

Überwachen Sie Ihre ESXi-Version in regelmäßigen Abständen.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Lesen Sie alle Versionshinweise und testen und implementieren Sie neue Softwareversionen über stufenweise Rollouts.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Select-Object Name,Version,Build
```

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar

Aktivieren von Zeitsynchronisierungsquellen

Auf dem ESXi-Host müssen die Zeitsynchronisierungsdienste aktiviert sein und ausgeführt werden.

Verschlüsselung, Überwachungsprotokollierung, Clustervorgänge sowie Reaktionen auf Vorfälle und Forensik basieren auf einer synchronisierten Uhrzeit. Um sicherzustellen, dass die Uhrzeit über Dienste und Vorgänge hinweg synchronisiert wird, aktivieren Sie zunächst auf dem Host die Dienste NTP und/oder PTP und stellen Sie sicher, dass diese ausgeführt werden.

Werte

Standardwert der Installation: Gestoppt, Manuell starten und beenden

Empfohlener Baseline-Wert: Wird ausgeführt, Mit Host beenden und starten

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHostService -VMHost $ESXi | Where-Object{$_.Key -eq "ntpd"}
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHostService -VMHost $ESXi -ErrorAction:Stop | Where-Object{$_.Key -eq "ntpd"} | Set-
VMHostService -policy "on" -Confirm:$false
Get-VMHostService -VMHost $ESXi -ErrorAction:Stop | Where-Object{$_.Key -eq "ntpd"} |
Restart-VMHostService -Confirm:$false
```

Konfigurieren zuverlässiger Zeitsynchronisierungsquellen

Für den ESXi-Host müssen zuverlässige Zeitsynchronisierungsquellen konfiguriert werden.

Verschlüsselung, Überwachungsprotokollierung, Clustervorgänge sowie Reaktionen auf Vorfälle und Forensik sind auf eine synchronisierte Uhrzeit angewiesen. Für NTP (Network Time Protocol) müssen mindestens vier Quellen verfügbar sein. Wenn Sie sich zwischen zwei Quellen oder einer Quelle entscheiden müssen, sollten Sie eine Quelle vorziehen.

PTP (Precision Time Protocol) ist eine Alternative zu NTP, die eine Zeitgenauigkeit unter einer Millisekunde bietet. Die Architektur von PTP unterscheidet sich von der von NTP und bietet nicht dieselbe Resilienz bei einem Ausfall des primären Servers. Ziehen Sie in Erwägung, NTP als Backup-Quelle für PTP zu konfigurieren, damit weiterhin eine Zeitquelle verfügbar ist, wenn auch mit geringerer Genauigkeit.

Werte

Standardwert der Installation: Nicht definiert

Empfohlener Baseline-Wert:

Standortspezifisch oder:

0.vmware.pool.ntp.org,

1.vmware.pool.ntp.org,

2.vmware.pool.ntp.org,

3.vmware.pool.ntp.org

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHostNtpServer -VMHost $ESXi
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ntp0 = "0.vmware.pool.ntp.org"
$ntp1 = "1.vmware.pool.ntp.org"
$ntp2 = "2.vmware.pool.ntp.org"
$ntp3 = "3.vmware.pool.ntp.org"

Add-VMHostNTPServer -NtpServer $ntp0 , $ntp1 , $ntp2 , $ntp3 -VMHost $ESXi -Confirm:$false
```

Verwendung der TLS-Verschlüsselung

Der ESXi-Host muss durch Aktivierung moderner TLS-Verschlüsselungen die Vertraulichkeit und Integrität der Übertragungen sicherstellen.

Ab ESXi 8.0 Update 3 konfigurieren TLS-Profile die Client- und Server-TLS-Einstellungen so, dass nur starke Verschlüsselungen verwendet werden. Mit den folgenden Befehlen können Sie die gesamte Verschlüsselungsliste und alle Verschlüsselungssuites anzeigen:

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.tls.server.get.CreateArgs()
$arguments.showprofiledefaults = $true
$arguments.showcurrentbootprofile = $true
$ESXcli.system.tls.server.get.invoke($arguments)
```

Nach Änderungen am TLS-Profil müssen Sie den ESXi-Host neu starten. (Im vSphere Client wird der Host mit dem Suffix „Neustart erforderlich“ angezeigt.)

Werte

Standardwert der Installation: COMPATIBILE

Empfohlener Baseline-Wert: NIST_2024

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Änderungen an den Verschlüsselungssuites wirken sich auf die Konnektivität mit externen Systemen aus. Sie müssen den Host neu starten, damit diese Änderung des TLS-Profils wirksam wird.

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.tls.server.get.invoke() | Select-Object -ExpandProperty Profile
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.tls.server.set.CreateArgs()
$arguments.profile = "NIST_2024"
$ESXcli.system.tls.server.set.invoke($arguments)
```

UserVars.ESXiVPsDisabledProtocols

Der ESXi-Host muss die höchste unterstützte TLS-Version aktivieren.

ESXi 8.0 aktiviert standardmäßig TLS 1.2. Im Bedarfsfall können jedoch andere Protokolle aktiviert werden. Ab ESXi 8.0 Update 3 ist standardmäßig TLS 1.3 aktiviert.

Werte

Standardwert der Installation: sslv3,tlsv1,tlsv1.1

Empfohlener Baseline-Wert: sslv3,tlsv1,tlsv1.1

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiVPsDisabledProtocols
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiVPsDisabledProtocols | Set-
AdvancedSetting -Value "sslv3,tlsv1,tlsv1.1"
```

Konfigurieren der TPM-basierten Verschlüsselung

Der ESXi-Host muss eine TPM-basierte Konfigurationsverschlüsselung erfordern.

Die Konfiguration eines ESXi-Hosts besteht aus Konfigurationsdateien für jeden Dienst, der auf dem Host ausgeführt wird. Die Konfigurationsdateien befinden sich in der Regel im Verzeichnis `/etc`, sie können sich aber auch in anderen Namespaces befinden. Die Konfigurationsdateien enthalten Laufzeitinformationen über den Status der Dienste. Im Laufe der Zeit können sich die Standardwerte in den Konfigurationsdateien ändern, z. B. wenn die Einstellungen auf dem ESXi-Host geändert werden.

Ein Cron-Auftrag sichert die ESXi-Konfigurationsdateien regelmäßig, wenn ESXi ordnungsgemäß heruntergefahren wird, oder bei Bedarf, und erstellt eine archivierte Konfigurationsdatei in der Startbank. Wenn ESXi neu startet, liest das System die archivierte Konfigurationsdatei und stellt den Zustand wird wieder her, in dem sich ESXi befand, als die Sicherung erstellt wurde.

Vor vSphere 7.0 Update 2 ist die archivierte ESXi-Konfigurationsdatei nicht verschlüsselt. In vSphere 7.0 Update 2 und höher ist die archivierte Konfigurationsdatei verschlüsselt. Wenn der ESXi-Host mit einem Trusted Platform Module (TPM) konfiguriert ist, wird das TPM zum „Versiegeln“ der Konfiguration für den Host verwendet, was eine starke Sicherheitsgarantie und zusätzlichen Schutz vor Online-Angriffen bietet.

Die Konfigurationsverschlüsselung verwendet das physische TPM, sofern es zum Zeitpunkt der Installation oder des Upgrades verfügbar ist und unterstützt wird. Wenn das TPM später hinzugefügt oder aktiviert wird, müssen Sie den ESXi-Host explizit neu konfigurieren, damit er das neu verfügbare TPM verwendet. Nachdem die TPM-Verschlüsselung der Konfiguration aktiviert wurde, kann sie nicht wieder deaktiviert werden.

Werte

Standardwert der Installation: Standortspezifisch

Empfohlener Baseline-Wert: TPM

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Die Verwendung von Secure Boot und durch TPM erzwungener Konfigurationsverschlüsselung machen herkömmliche Versuche zur Wiederherstellung des Root-Passworts unbrauchbar. Stellen Sie sicher, dass Sie den Zugriff auf ESXi-Administratorkonten nicht verlieren.

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.settings.encryption.get.Invoke() | Select Mode
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.settings.encryption.set.CreateArgs()
```

```
$arguments.mode = "TPM"
$ESXcli.system.settings.encryption.set.Invoke($arguments)
```

Prüfen der ESXi-Software auf Aktualität

Indem Sie über ESXi-Patches auf dem aktuellen Stand bleiben, reduzieren Sie Schwachstellen im Hypervisor.

Ein versierter Angreifer kann bekannte Schwachstellen ausnutzen, wenn er versucht, auf einen ESXi-Host zuzugreifen oder seine Berechtigungen zu erhöhen. Aktualisieren Sie immer zuerst vCenter Server, wenn ein Update verfügbar ist. Aktualisieren Sie danach ESXi.

Werte

Standardwert der Installation: Downlevel

Empfohlener Baseline-Wert: Aktuell

Aktion erforderlich

Überwachen Sie den ESXi-Patch-Level in regelmäßigen Abständen.

Lesen Sie alle Versionshinweise und testen und implementieren Sie neue Softwareversionen über stufenweise Rollouts.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

vSphere Update-Versionen fügen Funktionen hinzu und ändern diese. Mit Patch-Versionen werden ausschließlich Probleme behoben.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Select-Object Name,Version,Build
```

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar

VMkernel.Boot.execInstalledOnly

Führen Sie nur von einem VIB bereitgestellte Binärdateien aus.

ESXi führt Integritätsprüfungen von VIBs durch, die auf der Akzeptanzebene basieren. Indem ESXi angewiesen wird, nur solche Binärdateien auszuführen, die aus einem gültigen auf dem Host installierten VIB stammen, wird Angreifern die Verwendung vorgefertigter Toolkits für einen Angriff erschwert und die Wahrscheinlichkeit einer Erkennung verbessert.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: True

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Nicht signierte Software von Drittanbietern wird möglicherweise nicht installiert oder ausgeführt.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting VMkernel.Boot.execInstalledOnly
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting VMkernel.Boot.execInstalledOnly | Set-
AdvancedSetting -Value True
```

Deaktivieren von Verwaltungsdiensten auf VMkernel-Adaptern

Stellen Sie sicher, dass für vSAN, vMotion und andere dedizierte VMkernel-Adapter keine Verwaltungsdienste aktiviert sind.

Für spezielle Verwendungen vorgesehene VMkernel-Netzwerkschnittstellen können mit Verwaltungsfunktionen konfiguriert werden, die gegebenenfalls die Netzwerkisolierung und die Sicherheitsmaßnahmen konterkarieren. Aktivieren Sie Verwaltungsdienste nur auf VMkernel-Schnittstellen, die für die Verwaltung vorgesehen sind.

Werte

Standardwert der Installation: Standortspezifisch

Empfohlener Baseline-Wert: Standortspezifisch

Aktion erforderlich

Überwachen Sie Ihre standortspezifischen Werte.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Für einige von Drittanbietern verwaltete Lösungen ist es möglicherweise erforderlich, dass Sie die Verwaltungsdienste auf VMkernel-Adaptern aktivieren.

PowerCLI-Befehlsbeurteilung

```
Get-VMHostNetworkAdapter -VMHost $ESXi -VMKernel | Select
VMHost,Name,IP,ManagementTrafficEnabled
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHostNetworkAdapter -VMHost $ESXi -Name $vmkernel_interface | Set-
VMHostNetworkAdapter -ManagementTrafficEnabled $false
```

Konfigurieren der ESXi-Firewall für das Blockieren von Datenverkehr

Sie müssen die ESXi-Host-Firewall so konfigurieren, dass der Netzwerkdatenverkehr standardmäßig blockiert wird.

Stellen Sie sicher, dass der gesamte eingehende und ausgehende Netzwerkdatenverkehr blockiert wird, sofern er nicht ausdrücklich erlaubt ist. Das verringert die Angriffsfläche und verhindert den nicht autorisierten Zugriff auf den Host.

Werte

Standardwert der Installation: Aktiviert

Empfohlener Baseline-Wert: Aktiviert

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Eine Firewall ist recht simpel und ähnelt den ACLs von Routern. Gegebenenfalls müssen Sie reflexive Regeln neu konfigurieren.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-VMHostFirewallDefaultPolicy
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.network.firewall.set.CreateArgs()
$arguments.defaultaction = $FALSE
```

```
$arguments.enabled = $true
$ESXcli.network.firewall.set.Invoke($arguments)
```

Konfigurieren der ESXi-Firewall für autorisierte Netzwerke

Konfigurieren Sie die ESXi-Firewall so, dass nur Datenverkehr von autorisierten Netzwerken zugelassen wird.

Stellen Sie sicher, dass der gesamte eingehende und ausgehende Netzwerkdatenverkehr blockiert wird, sofern er nicht ausdrücklich erlaubt ist. Das verringert die Angriffsfläche und verhindert den nicht autorisierten Zugriff auf den ESXi-Host.

Ab vSphere 8.0 Update 2 werden Firewallregeln als Besitz von „user“ oder „system“ kategorisiert, wobei nur benutzereigene Regeln konfiguriert werden können. In vSphere 8 Update 2b und PowerCLI 13.2.1 gibt es zusätzliche abfragbare Parameter, um die Einstellung und Prüfung auf konfigurierbare Regeln zu automatisieren.

Werte

Standardwert der Installation: Verbindungen von beliebigen IP-Adressen sind zulässig

Empfohlener Baseline-Wert: Verbindungen sind nur von autorisierten Infrastruktur- und Verwaltungsarbeitsstationen zulässig

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Eine Firewall ist recht simpel und ähnelt den ACLs von Routern. Gegebenenfalls müssen Sie reflexive Regeln neu konfigurieren.

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$list = $ESXcli.network.firewall.ruleset.list.Invoke() | Where {($_.AllowedIPconfigurable
-eq $true) -and ($_.EnableDisableconfigurable -eq $true)} | Select -ExpandProperty Name

$arguments = $ESXcli.network.firewall.ruleset.allowedip.list.CreateArgs()
foreach ($rule in $list) {
    $arguments.rulesetid = $rule
    $ESXcli.network.firewall.ruleset.allowedip.list.Invoke($arguments)
}
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
# Customize this example for your environment.
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
# Deactivate firewall temporarily so we don't lose connectivity
$arguments = $ESXcli.network.firewall.set.CreateArgs()
$arguments.enabled = $false
$ESXcli.network.firewall.set.Invoke($arguments)
```

```
# Unset the "allow all" flag
$arguments = $ESXcli.network.firewall.ruleset.set.CreateArgs()
$arguments.allowedall = $false
$arguments.rulesetid = "sshServer"
$ESXcli.network.firewall.ruleset.set.Invoke($arguments)

# Add an IP range
$arguments = $ESXcli.network.firewall.ruleset.allowedip.add.CreateArgs()
$arguments.ipaddress = "192.168.0.0/16"
$arguments.rulesetid = "sshServer"
$ESXcli.network.firewall.ruleset.allowedip.add.Invoke($arguments)

# Enable the firewall
$arguments = $ESXcli.network.firewall.set.CreateArgs()
$arguments.enabled = $true
$ESXcli.network.firewall.set.Invoke($arguments)
```

Festlegen der Richtlinie für gefälschte Übertragungen auf „Ablehnen“

Legen Sie in der Richtlinie für gefälschte Übertragungen sowohl für den vSphere Standard-Switch als für dessen Portgruppen „Ablehnen“ fest.

Wenn das Betriebssystem der virtuellen Maschine die MAC-Adresse ändert, kann es jederzeit Frames mit einer imitierten Quell-MAC-Adresse senden. Durch das Imitieren einer MAC-Adresse kann ein Betriebssystem böswillige Angriffe auf die Geräte in einem Netzwerk durchführen, indem es die Identität eines vom empfangenden Netzwerk autorisierten Netzwerkadapters annimmt. Wenn die Option „Gefälschte Übertragungen“ auf „Akzeptieren“ festgelegt ist, führt ESXi keinen Vergleich zwischen der Quell-MAC-Adresse und der geltenden MAC-Adresse durch. Zum Schutz vor MAC-Imitation können Sie die Option „Gefälschte Übertragungen“ auf „Ablehnen“ einstellen. Dann 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.

Werte

Standardwert der Installation: Annehmen

Empfohlener Baseline-Wert: Ablehnen

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Einige Arbeitslasten, beispielsweise geclusterte Anwendungen sowie Netzwerkgeräte und -funktionen, nutzen diese Techniken im normalen Betrieb. Im Bedarfsfall können Sie eine

separate Portgruppe konfigurieren, die dieses Verhalten zulässt, und daran ausschließlich autorisierte virtuelle Maschinen anhängen.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | select
VirtualSwitch,ForgedTransmits
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | select
VirtualPortGroup,ForgedTransmits
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -ForgedTransmits $false
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -ForgedTransmitsInherited $true
```

Festlegen der Richtlinie „MAC-Adressänderungen“ auf „Ablehnen“

Legen Sie die Richtlinie „MAC-Adressänderungen“ auf dem vSphere Standard-Switch und den dazu gehörigen Portgruppen auf „Ablehnen“ fest.

Wenn das Betriebssystem der virtuellen Maschine die MAC-Adresse ändert, kann es Frames mit einer imitierten Quell-MAC-Adresse senden. Damit kann es böswillige Angriffe auf die Geräte in einem Netzwerk durchführen, indem es die Identität eines vom empfangenden Netzwerk autorisierten Netzwerkadapters annimmt. Um zu verhindern, dass virtuelle Maschinen ihre geltende MAC-Adresse ändern, sollten Maßnahmen ergriffen werden, die die Stabilität der MAC-Adresse erzwingen oder die Möglichkeit zum Ändern von MAC-Adressen einschränken. Dies trägt dazu bei, das Risiko einer MAC-Imitation und potenzieller böswilliger Aktivitäten zu mindern.

Werte

Standardwert der Installation: Annehmen

Empfohlener Baseline-Wert: Ablehnen

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Einige Arbeitslasten, beispielsweise geclusterte Anwendungen und Netzwerkgeräte und -funktionen, nach MAC-Adresse lizenzierte Anwendungen und das vCenter Server-Upgrade mit reduzierter Ausfallzeit nutzen diese Techniken im normalen Betrieb. Im Bedarfsfall können Sie eine separate Portgruppe konfigurieren, die dieses Verhalten zulässt, und daran ausschließlich autorisierte virtuelle Maschinen anhängen.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | select
VirtualSwitch,MacChanges
```

```
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | select
VirtualPortGroup,MacChanges
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -MacChanges $false
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -MacChangesInherited $true
```

Festlegen der Richtlinie „Promiskuitiver Modus“ auf „Ablehnen“

Legen Sie die Richtlinie „Promiskuitiver Modus“ auf dem vSphere Standard-Switch und dessen Portgruppen auf „Ablehnen“ fest.

Wenn für eine Portgruppe „Promiskuitiver Modus“ aktiviert ist, können alle mit dieser Portgruppe verbundenen virtuellen Maschinen potenziell alle über diese Portgruppe übertragenen Pakete lesen, unabhängig vom beabsichtigten Empfänger. Bedenken Sie die möglichen Auswirkungen und Designaspekte, bevor Sie den Standardwert in „Promiskuitiver Modus“ ändern.

Werte

Standardwert der Installation: Ablehnen

Empfohlener Baseline-Wert: Ablehnen

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Bestimmte Arbeitslasten und Arbeiten, z. B. DHCP-Server, Netzwerkgeräte und die Sicherheitsüberwachung, integrieren diese Techniken in ihrem regelmäßigen Betrieb. Im Bedarfsfall können Sie eine separate Portgruppe konfigurieren, die dieses Verhalten zulässt, und daran ausschließlich autorisierte virtuelle Maschinen anhängen.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | select
VirtualSwitch,AllowPromiscuous
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | select
VirtualPortGroup,AllowPromiscuous
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -AllowPromiscuous $false
```

```
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -AllowPromiscuousInherited $true
```

Beschränken von Virtual Guest Tagging (VGT) auf Standard-Switches

Der ESXi-Host muss die Verwendung von Virtual Guest Tagging (VGT) auf Standard-Switches beschränken.

Wenn eine Portgruppe auf „VLAN 4095“ festgelegt ist, übergibt der vSwitch alle Netzwerk-Frames an die angehängten virtuellen Maschinen, ohne die VLAN-Tags zu ändern. Dies wird in vSphere als VGT bezeichnet. Die virtuelle Maschine muss die VLAN-Informationen unter Verwendung eines 802.1Q-Treibers selbst im Betriebssystem verarbeiten.

VLAN 4095 darf nur implementiert werden, wenn die angehängten virtuellen Maschinen spezifisch autorisiert wurden und in der Lage sind, VLAN-Tags selbsttätig zu verwalten. Wenn VLAN 4095 nicht ordnungsgemäß aktiviert ist, kann dies zu einem Denial-of-Service führen oder einer virtuellen Maschine die Interaktion mit Datenverkehr in einem nicht autorisierten VLAN ermöglichen.

Werte

Standardwert der Installation: Nicht VLAN 4095

Empfohlener Baseline-Wert: Nicht VLAN 4095

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | select Name,VlanID
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard -Name $PG| Set-VirtualPortGroup
-VlanID "new_VLAN"
```

Aktivieren der Secure Boot-Erzwingung

Secure Boot (sicherer Start) ist Bestandteil des UEFI-Firmwarestandards. Bei aktiviertem UEFI Secure Boot lädt ein Host einen UEFI-Treiber oder ESXi-Apps nur dann, wenn der Bootloader des Betriebssystems über ein gültige digitale Signatur verfügt. Secure Boot für ESXi erfordert die Unterstützung durch die Firmware. Secure Boot für ESXi erfordert außerdem, dass alle ESXi-Kernelmodule, -Treiber und -VIBs von VMware oder einem unterstellten Partner signiert wurden.

Secure Boot wird im BIOS des physischen ESXi-Servers aktiviert und vom Hypervisor-Bootloader unterstützt. Diese Kontrolle ändert die Einstellung von ESXi von der bloßen Unterstützung von Secure Boot in die Erforderung desselben. Ohne Aktivierung dieser Einstellung und die Konfigurationsverschlüsselung ist ein ESXi-Host möglicherweise Offline-Angriffen ausgesetzt. Ein Angreifer könnte einfach das ESXi-Installationslaufwerk in einen Host ohne Secure Boot transferieren und starten.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: True

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Die Verwendung von Secure Boot und durch TPM erzwungener Konfigurationsverschlüsselung machen herkömmliche Versuche zur Wiederherstellung des Root-Passworts unbrauchbar. Stellen Sie sicher, dass Sie den Zugriff auf ESXi-Administratorkonten nicht verlieren.

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.settings.encryption.get.Invoke() | Select RequireSecureBoot
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.settings.encryption.set.CreateArgs()
$arguments.requiresecureboot = $true
$ESXcli.system.settings.encryption.set.Invoke($arguments)
```

Deaktivieren der ESXi Shell

Die ESXi Shell sollte deaktiviert sein.

Werte

Standardwert der Installation: Gestoppt, Manuell starten und beenden

Empfohlener Baseline-Wert: Gestoppt, Manuell starten und beenden

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'TSM' -and $_.Running -eq
'True'}
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'TSM' -and $_.Policy -eq 'On'}
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'TSM'} | Set-VMHostService -Policy Off
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'TSM'} | Stop-VMHostService
```

UserVars.ESXiShellInteractiveTimeOut

Legt eine Zeitüberschreitung fest, um ESXi Shell- und SSH-Sitzungen im Leerlauf automatisch zu beenden.

Wenn Benutzer vergessen, sich von ihrer SSH-Sitzung abzumelden, bleibt die Verbindung im Leerlauf unbegrenzt offen. Dies steigert die Möglichkeit, dass andere Benutzer potenziell einen privilegierten Zugriff auf den Host erhalten. Sie können Shell-Sitzungen, die sich im Leerlauf befinden, dahingehend konfigurieren, dass sie automatisch beendet werden.

Werte

Standardwert der Installation: 0

Empfohlener Baseline-Wert: 900

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiShellInteractiveTimeOut
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiShellInteractiveTimeOut | Set-
AdvancedSetting -Value 900
```

Deaktivieren des SNMP-Dienstes

Deaktivieren Sie den SNMP-Dienst, wenn Sie ihn nicht verwenden.

Werte

Standardwert der Installation: Gestoppt, Mit dem Host starten und beenden

Empfohlener Baseline-Wert: Gestoppt, Manuell starten und beenden

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'snmpd' -and $_.Running -eq
'True'}
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'snmpd' -and $_.Policy -eq 'On'}
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'snmpd'} | Set-VMHostService -Policy
Off
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'snmpd'} | Stop-VMHostService
```

Deaktivieren des SNMP-Dienstes

Deaktivieren Sie SSH und aktivieren Sie es nur für die Fehlerbehebung.

ESXi ist kein UNIX-ähnliches Multiuser-Betriebssystem. ESXi ist ein speziell entwickelter Hypervisor, der durch den VMware Host Client, den vSphere Client, die CLIs und die APIs verwaltet wird. Auf ESXi dient SSH als Schnittstelle für die Fehlerbehebung und den Support und wird standardmäßig angehalten und deaktiviert. Die Aktivierung dieser Schnittstelle birgt Risiken.

Werte

Standardwert der Installation: Gestoppt, Manuell starten und beenden

Empfohlener Baseline-Wert: Gestoppt, Manuell starten und beenden

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'TSM-SSH' -and $_.Running -eq
'True'}
```

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'TSM-SSH' -and $_.Policy -eq
'On'}
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'TSM-SSH'} | Set-VMHostService -Policy
Off
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'TSM-SSH'} | Stop-VMHostService
```

Verwenden von Entropie für kryptografische Vorgänge

Der ESXi-Host muss für kryptografische Vorgänge ausreichende Entropie verwenden.

In vSphere 8.0 und höher unterstützt die ESXi-Entropie-Implementierung die Zertifizierungen FIPS 140-3 und EAL4. Kernel-Startoptionen steuern, welche Entropiequellen auf einem ESXi-Host aktiviert werden sollen.

Werte

Standardwert der Installation:

disableHwrng = FALSE

entropySources = 0

Empfohlener Baseline-Wert:

disableHwrng = FALSE

entropySources = 0

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.settings.kernel.list.Invoke() | Where {$_.Name -eq "disableHwrng" -or
$_.Name -eq "entropySources"}
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.settings.kernel.set.CreateArgs()
$arguments.setting = "disableHwrng"
$arguments.value = "FALSE"
$ESXcli.system.settings.kernel.set.invoke($arguments)
$arguments.setting = "entropySources"
```

```
$arguments.value = "0"
$ESXcli.system.settings.kernel.set.invoke($arguments)
```

Überprüfen von Image-Profil- und VIB-Akzeptanzebenen

Die Akzeptanzebene des ESXi-Host-Image-Profils muss mindestens „PartnerSupported“ lauten.

Die Akzeptanzebene steuert, welche Installationen ESXi zulässt. Informationen zu den VIB-Ebenen finden Sie unter Verwalten der Akzeptanzebenen von ESXi-Hosts und vSphere-Installationspaketen.

Weder VMware noch VMware-Partner testen CommunitySupported-VIBs. CommunitySupported-VIBs enthalten außerdem keine digitale Signatur. Gehen Sie daher bei der Installation von CommunitySupported-VIBs äußerst vorsichtig vor.

Werte

Standardwert der Installation: PartnerSupported

Empfohlener Baseline-Wert: PartnerSupported oder höher

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

CommunitySupported-Pakete sind nicht signiert und können nicht installiert werden.

PowerCLI-Befehlsbeurteilung

```
(Get-EsxCli -VMHost $ESXi -V2).software.acceptance.get.Invoke()
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.software.acceptance.set.CreateArgs()
$arguments.level = "PartnerSupported" # VMwareCertified, VMwareAccepted, PartnerSupported,
CommunitySupported
$ESXcli.software.acceptance.set.Invoke($arguments)
```

Security.AccountUnlockTime

Der ESXi-Host muss Konten nach einer bestimmten Zeit entsperren.

`Security.AccountUnlockTime` stellt sicher, dass Benutzerkonten auf dem ESXi-Host nach einem festgelegten Zeitraum der Inaktivität automatisch entsperrt werden. Durch das Erzwingen des automatischen Entsperrens von Konten können Organisationen ein Gleichgewicht zwischen Sicherheit und Benutzerfreundlichkeit erzielen. Dieses stellt sicher, dass Konten, die sich im Leerlauf befinden, sofort wieder aktiviert werden können, während gleichzeitig das Potenzial für den nicht autorisierten Zugriff minimiert wird.

Werte

Standardwert der Installation: 900 Sekunden

Empfohlener Baseline-Wert: 900 Sekunden

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountUnlockTime
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountUnlockTime | Set-
AdvancedSetting -Value 900
```

Security.AccountLockFailures

Legt die maximale Anzahl fehlgeschlagener Anmeldeversuche fest, nach denen ein Konto gesperrt wird.

Dies schützt vor Brute-Force-Angriffen und nicht autorisierten Zugriffsversuchen, indem das betroffene Konto vorübergehend deaktiviert wird, was bis zum Ablaufen der Sperrzeit oder das manuelle Zurücksetzen des Kontos durch einen Administrator weitere Anmeldeversuche verhindert. Das Entsperren eines gesperrten Kontos erfordert entweder ein administratives Eingreifen oder eine Wartezeit bis das Konto automatisch entsperrt wird, sofern diese Einstellung `Security.AccountUnlockTime` verwendet wird.

Werte

Standardwert der Installation: 5

Empfohlener Baseline-Wert: 5

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Ein niedriger Schwellenwert für Anmeldefehler kann potenziell eine Zunahme beabsichtigter oder unbeabsichtigter Denial-of-Service-Angriffe bewirken, z. B. durch erneute Versuche eine SSH-Verbindung herzustellen.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountLockFailures
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountLockFailures | Set-
AdvancedSetting -Value 5
```

Security.PasswordHistory

Lässt keine erneute Verwendung von Kennwörtern zu.

Diese Einstellung verhindert die erneute Verwendung vorheriger Kennwörter. Dies verhindert potenzielle Angriffe mit alten, kompromittierten Anmeldedaten.

Werte

Standardwert der Installation: 5

Empfohlener Baseline-Wert: 5

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordHistory
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordHistory | Set-
AdvancedSetting -Value 5
```

Security.PasswordMaxDays

Legt die maximale Anzahl an Tagen zwischen Kennwortänderungen fest.

Moderne Best Practices für Kennwörter, wie sie in NIST 800-63B Abschnitt 5.1.1.2 und anderen relevanten Anleitungen beschrieben werden, besagen, dass die Erzwingung regelmäßiger Kennwortänderungen die Sicherheit nicht verbessert, wenn Kennwörter bereits über eine angemessene Entropie verfügen.

Werte

Standardwert der Installation: 99999

Empfohlener Baseline-Wert: 99999

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordMaxDays
```

PowerCLI-Befehl

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordMaxDays | Set-
AdvancedSetting -Value 99999
```

Security.PasswordQualityControl

Erzwingt komplexe Kennwörter.

Empfehlungen wie in NIST 800-63B Abschnitt 5.1.1.2 legen nahe, dass Erstellungsregeln, z. B. das Festlegen einer Mischung aus Zeichenklassen, auf Systemen nicht erzwungen werden sollten, da sie die Kennwortsicherheit häufig nicht verbessern und die Akzeptanz für sicherere Passphrasen verringern.

Regeln für die Stärke und Komplexität von Kennwörtern gelten für alle ESXi-Benutzer, einschließlich des Root-Benutzers. Wenn der ESXi-Host jedoch einer Domäne beitritt, gelten diese Regeln nicht für Active Directory (AD)-Benutzer, da Kennwortrichtlinien für AD-Benutzer vom AD-System erzwungen werden.

Werte

Standardwert der Installation: retry=3 min=disabled,disabled,disabled,7,7

Empfohlener Baseline-Wert: retry=3 min=disabled,15,15,15,15 max=64 similar=deny passphrase=3

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Andere Produkte und Dienste innerhalb des VMware-Ökosystems erwarten möglicherweise keine Änderungen der Anforderungen an die Komplexität von Kennwörtern, weshalb möglicherweise die Installation fehlschlägt.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordQualityControl
```

PowerCLI-Befehl

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordQualityControl | Set-
AdvancedSetting -Value "retry=3 min=disabled,15,15,15,15 max=64 similar=deny passphrase=3"
```

UserVars.SuppressHyperthreadWarning

Unterdrückt die Warnung vor einer potenzielle Sicherheitslücke aufgrund von Hyper-Threading.

Sicherheitswarnungen aufgrund von Hyper-Threading resultieren aus nicht behobenen CPU-Schwachstellen im System. Wenn diese Warnungen ignoriert werden, bleiben potenzielle Risiken möglicherweise unerkannt. Stellen Sie sicher, dass Korrekturen von Hardwareproblemen gemäß dem in Ihrem Unternehmen akzeptablen Risikos erfolgen. Sofern Sie eine Warnung unterdrücken, dokumentieren Sie die Entscheidung und geben Sie eine Begründung an.

Werte

Standardwert der Installation: 0

Empfohlener Baseline-Wert: 0

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.SuppressHyperthreadWarning
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.SuppressHyperthreadWarning | Set-
AdvancedSetting -Value 0
```

UserVars.DcuiTimeOut

Legt eine Zeitbeschränkung fest, nach deren Ablauf im Leerlauf befindliche DCUI-Sitzungen automatisch beendet werden.

DCUI ermöglicht eine direkte Anmeldung beim ESXi-Host für Verwaltungsaufgaben. Um eine unbeabsichtigte DCUI-Nutzung über noch laufende Anmeldesitzungen zu verhindern, beenden Sie Verbindungen im Leerlauf.

Werte

Standardwert der Installation: 600

Empfohlener Baseline-Wert: 600

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.DcuiTimeOut
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.DcuiTimeOut | Set-AdvancedSetting
-Value 600
```

CIM-Dienst deaktivieren

Der ESXi-CIM-Dienst sollte deaktiviert sein.

Dienste, die nicht verwendet werden und für den Betrieb nicht erforderlich sind, sollten deaktiviert werden.

Werte

Standardwert der Installation: Gestoppt, Mit dem Host starten und beenden

Empfohlener Baseline-Wert: Gestoppt, Manuell starten und beenden

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'sfcbd-watchdog' -and
$_.Running -eq 'True'}
```

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'sfcbd-watchdog' -and $_.Policy
-eq 'On'}
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'sfcbd-watchdog'} | Set-VMHostService
-Policy Off
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'sfcbd-watchdog'} | Stop-VMHostService
```

Config.HostAgent.log.level

Legt die Protokollierungsebene fest.

Stellen Sie beim Festlegen der Protokollierungsebene sicher, dass in den Überwachungsprotokollen ausreichend Informationen vorhanden sind, um Diagnosen und forensische Untersuchungen durchzuführen.

Werte

Standardwert der Installation: Info

Empfohlener Baseline-Wert: Info

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Für Protokolle wird zusätzlicher Speicherplatz benötigt.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.log.level
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.log.level | Set-
AdvancedSetting -Value info
```

Syslog.global.logLevel

Protokolliert ausreichende Informationen für Ereignisse.

Ohne ausreichende Protokolldaten können kritische Indikatoren für eine Kompromittierung unbemerkt bleiben, was bei der effektiven Reaktion auf Cybersicherheitsvorfälle zu einer erhöhten Angreifbarkeit und potenziellen Ausfällen führt.

Werte

Standardwert der Installation: Fehler

Empfohlener Baseline-Wert: Info

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Für Protokolle wird zusätzlicher Speicherplatz benötigt.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logLevel
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logLevel | Set-AdvancedSetting
-Value info
```

Config.HostAgent.plugins.solo.enableMob

Deaktiviert den Managed Object Browser (MOB).

Dienste, die nicht verwendet werden und für den Betrieb nicht erforderlich sind, sollten deaktiviert werden.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: False

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.plugins.solo.enableMob
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.plugins.solo.enableMob | Set-
AdvancedSetting -Value False
```

Net.BlockGuestBPDU

Blockiert BPDU (Bridge Protocol Data Unit)-Übertragungen des Gastbetriebssystems.

BPDUs werden genutzt, um Spanning-Tree-Protocol (STP)-Informationen zu übertragen und Netzwerkschleifen zu erkennen. BPDU Guard und Portfast werden normalerweise auf dem physischen Switch aktiviert, der direkt mit dem ESXi-Host verbunden ist, um die Verzögerung bei der Spanning-Tree-Konvergenz zu reduzieren.

Wenn jedoch ein BPDU-Paket von einer virtuellen Maschine auf dem ESXi-Host an den konfigurierten physischen Switch gesendet wird, kann dies zu einer kaskadierenden Sperrung aller Uplink-Schnittstellen vom ESXi-Host führen. Um solche Sperren zu verhindern, können Sie den BPDU-Filter auf dem ESXi-Host aktivieren, damit alle BPDU-Pakete verworfen werden, die an den physischen Switch gesendet werden.

Standard-Switches und Distributed Virtual Switches unterstützen kein STP und generieren keine BPDUs.

Werte

Standardwert der Installation: 1

Empfohlener Baseline-Wert: 1

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Einige netzwerkorientierte Arbeitslasten können legitime BPDU-Pakete generieren. Stellen Sie vor der Aktivierung des BPDU-Filters sicher, dass von virtuellen Maschinen auf dem ESXi-Host keine legitimen BPDU-Pakete generiert werden. Wenn der BPDU-Filter in dieser Situation aktiviert ist, bietet die Aktivierung der Funktion „Gefälschte Übertragungen“ mittels „Ablehnen“ in der Portgruppe des virtuellen Switches zusätzlichen Schutz vor Spanning Tree-Schleifen.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.BlockGuestBPDU
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.BlockGuestBPDU | Set-AdvancedSetting
-Value 1
```

Net.DVFilterBindIpAddress

Schränkt die Verwendung der dvFilter-Netzwerk-APIs ein.

Wenn Sie kein Produkt wie VMware NSX verwenden, das die dvFilter-Netzwerk-API nutzt, konfigurieren Sie den ESXi-Host nicht so, dass er Netzwerkinformationen an eine IP-Adresse sendet. Das Aktivieren der API und der Verweis auf eine kompromittierte IP-Adresse kann möglicherweise einen unbefugten Zugriff auf das Netzwerk anderer virtueller Maschinen auf dem ESXi-Host ermöglichen.

Wenn Sie ein Produkt verwenden, das auf diese API angewiesen ist, müssen Sie unbedingt prüfen, ob der ESXi-Host korrekt konfiguriert wurde, um eine sichere Netzwerkkommunikation zu gewährleisten.

Werte

Standardwert der Installation: ""

Empfohlener Baseline-Wert: ""

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.DVFilterBindIpAddress
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.DVFilterBindIpAddress | Set-
AdvancedSetting -Value ""
```

UserVars.ESXiShellTimeOut

Legt eine Zeitüberschreitung fest, um zu begrenzen, wie lange ESXi Shell- und SSH-Dienste ausgeführt werden dürfen.

Diese erweiterte Systemeinstellung definiert ein Zeitfenster, nach dessen Ablauf die ESXi Shell- und SSH-Dienste automatisch beendet werden.

Werte

Standardwert der Installation: 0

Empfohlener Baseline-Wert: 600

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiShellTimeOut
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiShellTimeOut | Set-
AdvancedSetting -Value 600
```

UserVars.SuppressShellWarning

Unterdrückt die Warnung für Support- und Fehlerbehebungsschnittstellen.

Der ESXi-Host darf keine Warnungen unterdrücken, die melden, dass die ESXi Shell aktiviert ist.

Warnungen, dass SSH oder die ESXi Shell aktiviert ist, können ein Hinweis auf einen laufenden Angriff sein. Dabei ist es wichtig, sicherzustellen, dass SSH und die ESXi Shell deaktiviert sind und dass diese erweiterte Systemeinstellung nicht aktiviert ist.

Werte

Standardwert der Installation: 0

Empfohlener Baseline-Wert: 0

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.SuppressShellWarning
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.SuppressShellWarning | Set-
AdvancedSetting -Value 0
```

Konfigurieren des ESXi Secure Shell-Daemons für FIPS

Der Secure Shell (SSH)-Daemon des ESXi-Hosts muss so konfiguriert werden, dass er nur gemäß FIPS 140-2/140-3 validierte Verschlüsselungen verwendet. Sie müssen Systemdienste härten und sichern, wenn diese aktiviert werden.

Werte

Standardwert der Installation: aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

Empfohlener Baseline-Wert: aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq 'ciphers'} |
Select-Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'ciphers'
$arguments.value = 'aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-
ctr,aes128-ctr'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Konfigurieren des ESXi SSH-Daemon für FIPS

Der SSH-Daemon des ESXi-Hosts muss gemäß FIPS 140-2/140-3 validierte kryptografische Module verwenden.

OpenSSH auf dem ESXi-Host wird mit einem nach FIPS 140-2/140-3 validierten Kryptografiemodul ausgeliefert, das standardmäßig aktiviert ist. Zum Erzielen von Abwärtskompatibilität können Sie dieses Modul deaktivieren. Überwachen und korrigieren Sie dies gegebenenfalls.

Werte

Standardwert der Installation: True.

Empfohlener Baseline-Wert: True

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.security.fips140.ssh.get.Invoke()
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.security.fips140.ssh.set.CreateArgs()
$arguments.enable = $true
$ESXcli.system.security.fips140.ssh.set.Invoke($arguments)
```

Konfigurieren des ESXi Secure Shell-Daemons für das Nicht-Zulassen von Gateway-Ports

Der Secure Shell (SSH)-Daemon des ESXi-Hosts muss so konfiguriert sein, dass er keine Gateway-Ports zulässt.

Sie müssen Systemdienste härten und sichern, wenn diese aktiviert werden.

Werte

Standardwert der Installation: Nein

Empfohlener Baseline-Wert: Nein

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq 'gatewayports'}
| Select-Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'gatewayports'
```

```
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Konfigurieren des ESXi Secure Shell-Daemons, damit er keine hostbasierte Authentifizierung zulässt

Der Secure Shell (SSH)-Daemon des ESXi-Hosts darf keine hostbasierte Authentifizierung zulassen.

Sie müssen Systemdienste härten und sichern, wenn diese aktiviert werden.

Werte

Standardwert der Installation: Nein

Empfohlener Baseline-Wert: Nein

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'hostbasedauthentication'} | Select-Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'hostbasedauthentication'
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Konfigurieren des ESXi Secure Shell-Daemons für das Festlegen eines Timeout-Zählers

Der Secure Shell (SSH)-Daemon des ESXi-Hosts muss für Sitzungen im Leerlauf einen Timeout-Zähler festlegen.

Sie müssen Systemdienste härten und sichern, wenn diese aktiviert werden. Der Timeout-Zähler-Wert multipliziert mit dem Wert des Zeitüberschreitungsintervalls im Leerlauf ergibt die Gesamtzahl der Sekunden, während der eine Sitzung bis zur Trennung inaktiv sein kann.

Werte

Standardwert der Installation: 3

Empfohlener Baseline-Wert: 3

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'clientalivecountmax'} | Select-Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'clientalivecountmax'
$arguments.value = '3'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Konfigurieren des ESXi Secure Shell-Daemons für das Festlegen eines Zeitüberschreitungsintervalls

Der Secure Shell (SSH)-Daemon des ESXi-Hosts muss für Sitzungen im Leerlauf einen Timeout-Zähler festlegen.

Sie müssen Systemdienste härten und sichern, wenn diese aktiviert werden. Der Timeout-Zähler-Wert multipliziert mit dem Wert des Zeitüberschreitungsintervalls im Leerlauf ergibt die Gesamtzahl der Sekunden, während der eine Sitzung bis zur Trennung inaktiv sein kann.

Werte

Standardwert der Installation: 200

Empfohlener Baseline-Wert: 200

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'clientaliveinterval'} | Select-Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'clientaliveinterval'
$arguments.value = '200'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Konfigurieren des ESXi Secure Shell Daemons für die Anzeige eines Anmelde-Banners

Der Secure Shell (SSH)-Daemon des ESXi-Hosts muss das Anmelde-Banner des Systems anzeigen, bevor der Zugriff auf das System gewährt wird.

Sie müssen Systemdienste härten und sichern, wenn diese aktiviert werden. Sie müssen außerdem die Einstellung `Config.Etc.issue` festlegen, um Text für dieses Banner anzugeben.

Werte

Standardwert der Installation: `/etc/issue`

Empfohlener Baseline-Wert: `/etc/issue`

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq 'banner'} |
Select-Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'banner'
```

```
$arguments.value = '/etc/issue'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Konfigurieren des ESXi Secure Shell-Daemons für das Ignorieren von .rhosts-Dateien

Der Secure Shell (SSH)-Daemon des ESXi-Hosts muss `.rhosts` -Dateien ignorieren.

Sie müssen Systemdienste härten und sichern, wenn diese aktiviert werden.

Werte

Standardwert der Installation: Ja

Empfohlener Baseline-Wert: Ja

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq 'ignorerhosts'}
| Select-Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'ignorerhosts'
$arguments.value = 'yes'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Konfigurieren des ESXi Secure Shell-Daemons für die Deaktivierung der lokalen Stream-Weiterleitung

Der Secure Shell (SSH)-Daemon des ESXi-Hosts muss die lokale Stream-Weiterleitung deaktivieren.

Sie müssen Systemdienste härten und sichern, wenn diese aktiviert werden.

Werte

Standardwert der Installation: Nein

Empfohlener Baseline-Wert: Nein

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'allowstreamlocalforwarding'} | Select-Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'allowstreamlocalforwarding'
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Konfigurieren des ESXi Secure Shell-Daemons für die Deaktivierung der TCP-Weiterleitung

Der Secure Shell (SSH)-Daemon des ESXi-Hosts muss die TCP-Weiterleitung deaktivieren.

Sie müssen Systemdienste härten und sichern, wenn diese aktiviert werden.

Werte

Standardwert der Installation: Nein

Empfohlener Baseline-Wert: Nein

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'allowtcpforwarding'} | Select-Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'allowtcpforwarding'
```

```
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Konfigurieren des ESXi Secure Shell-Daemons für das Nicht-Zulassen von Tunnels

Der Secure Shell (SSH)-Daemon des ESXi-Hosts darf keine Tunnel zulassen.

Sie müssen Systemdienste härten und sichern, wenn diese aktiviert werden.

Werte

Standardwert der Installation: Nein

Empfohlener Baseline-Wert: Nein

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq 'permittunnel'}
| Select-Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'permittunnel'
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Konfigurieren des ESXi Secure Shell-Daemons für das Nicht-Zulassen von Benutzerumgebungseinstellungen

Der Secure Shell (SSH)-Daemon des ESXi-Hosts darf keine Benutzerumgebungseinstellungen zulassen.

Sie müssen Systemdienste härten und sichern, wenn diese aktiviert werden.

Werte

Standardwert der Installation: Nein

Empfohlener Baseline-Wert: Nein

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'permituserenvironment'} | Select-Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'permituserenvironment'
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Deaktivieren des Service Location Protocol-Dienstes

Deaktivieren Sie den Service Location Protocol (SLP)-Dienst, wenn er nicht verwendet werden.

Werte

Standardwert der Installation: Gestoppt, Manuell starten und beenden

Empfohlener Baseline-Wert: Gestoppt, Manuell starten und beenden

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'slpd' -and $_.Running -eq
'True'}
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'slpd' -and $_.Policy -eq 'On'}
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'slpd'} | Set-VMHostService -Policy Off
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'slpd'} | Stop-VMHostService
```

Mem.ShareForceSalting

Beschränkt die transparente gemeinsame Seitennutzung auf virtuelle Maschinen, die mit `sched.mem.pshare.salt` konfiguriert sind.

Die transparente gemeinsame Seitennutzung (Transparent Page Sharing, TPS) ist eine Methode zur Verringerung des Arbeitsspeicherbedarfs virtueller Maschinen. Unter streng kontrollierten Bedingungen können Angreifer mithilfe von TPS unbefugten Zugriff auf Daten auf benachbarten virtuellen Maschinen erlangen. Virtuelle Maschinen, für die die Einstellung `sched.mem.pshare.salt` nicht konfiguriert ist, können Speicher nicht mit anderen virtuellen Maschinen gemeinsam nutzen. Große Seitenformate, eine Leistungsoptimierung im Hypervisor auf vielen modernen CPUs, sind nicht mit TPS kompatibel.

Werte

Standardwert der Installation: 2

Empfohlener Baseline-Wert: 2

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Mem.ShareForceSalting
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Mem.ShareForceSalting | Set-AdvancedSetting
-Value 2
```

UserVars.HostClientSessionTimeout

Legt eine Zeitüberschreitung fest, um im Leerlauf befindliche ESXi-Host-Clientsitzungen automatisch zu beenden.

Der ESXi-Host muss im Leerlauf befindliche Clientsitzungen automatisch beenden. Diese trägt dazu bei, potenzielle Sicherheitsrisiken zu verringern, indem sichergestellt wird, dass unbeaufsichtigte Sitzungen nicht unbefristet offen bleiben, wodurch sie von nicht autorisierten Benutzern oder Schadsoftware ausgenutzt werden könnten.

Werte

Standardwert der Installation: 900

Empfohlener Baseline-Wert: 900

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.HostClientSessionTimeout
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.HostClientSessionTimeout | Set-
AdvancedSetting -Value 900
```

Net.BMCNetworkEnable

Deaktiviert die Netzwerkschnittstellen für die Verwaltung virtueller Hardware.

Controller für die Hardwareverwaltung stellen dem ESXi-Host häufig virtuelle oder USB-NICs bereit. Da diese als Hintertüren verwendet werden können, sollten sie sowohl in der Hardwarekonfiguration als auch in der ESXi-Konfiguration deaktiviert werden.

Werte

Standardwert der Installation: 1

Empfohlener Baseline-Wert: 0

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Diese Funktionalität ist möglicherweise für einige verwaltete Lösungen von Drittanbietern erforderlich.

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.BMCNetworkEnable
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.BMCNetworkEnable | Set-AdvancedSetting
-Value 0
```

Aktivieren der bidirektionalen/gegenseitigen CHAP-Authentifizierung für iSCSI-Datenverkehr

Legen Sie für die Authentifizierung des iSCSI-Speicheradapters „Bidirektionales CHAP verwenden“ fest und geben Sie die Anmeldedaten an.

Gegenseitiges CHAP bietet eine zusätzliche Schutzebene, da sowohl der Initiator (Client) als auch das Ziel (Server) gegenseitig ihre Identität bestätigen müssen. Dies verhindert, dass zwischen den beiden Instanzen übertragene Daten durch nicht autorisierte Entitäten abgefangen oder geändert werden.

Werte

Standardwert der Installation: Nicht konfiguriert

Empfohlener Baseline-Wert: Aktiviert

Aktion erforderlich

Ändern Sie den Standardwert der Installation, wenn Sie diese Funktion verwenden.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VMHost -Name $ESXi | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Select VMHost,
Device, ChapType, @{N="CHAPName";E={$_.AuthenticationProperties.ChapName}}
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VMHost -Name $ESXi | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Set-VMHostHba
parameters
```

Informationen zu Parametern finden Sie unter *ESXCLI – Referenz*.

Kein Speichern von Verschlüsselungsschlüsseln ohne Absicherung des physischen Zugriffs auf ESXi-Hosts

Der ESXi-Host darf keine Verschlüsselungsschlüssel auf dem ESXi-Host selbst speichern, wenn der Host nicht vor physischem Zugriff geschützt ist.

Schlüsselpersistenz ist ein Mechanismus, der ein lokales Trusted Platform Module (TPM) verwendet, um Schlüssel des Standardschlüsselanbieters zu speichern, die sich normalerweise nur in einem externen Schlüsselverwaltungssystem (Key Management System, KMS) befinden. Zwar kann dieses Setup die Verwaltung von Abhängigkeiten verbessern, durch die Verwendung der Schlüsselpersistenz ändern sich jedoch die Verschlüsselungsrisiken. Wenn ein Angreifer den Host stiehlt, hat er Zugriff auf die Verschlüsselungsschlüssel für die Daten auf diesem Host und umgeht die Zugriffskontrollen des externen KMS. Nutzen Sie Schlüsselpersistenz daher nur, wenn Sie die physische Sicherheit Ihrer Hosts gewährleisten können. Wenn die physischen Hosts nicht sicher sind und ein Angreifer den Host stehlen kann, kann der Angreifer auch auf verschlüsselte Arbeitslasten zugreifen und diese verwenden.

Schlüsselpersistenz und vSphere Native Key Provider werden häufig verwechselt, da beide Verschlüsselungsdaten auf Hosts speichern. Der vSphere Native Key Provider verwendet jedoch keine Schlüsselpersistenz. Das Deaktivieren der Schlüsselpersistenz wirkt sich daher nicht auf ihn aus. Wie bei der Schlüsselpersistenz muss auch beim vSphere Native Key Provider sorgfältig auf die physische Sicherheit geachtet werden. Weitere Informationen hierzu finden Sie unter vSphere-Systemdesign-Sicherheitskontrollenreferenz.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: False

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

„Standard“ ist das gewünschte Verhalten. Eine Abweichung von der Standardeinstellung kann sich negativ auf die Vertraulichkeit in Umgebungen auswirken, in denen ein physischer Zugriff durch Angreifer möglich ist.

PowerCLI-Befehlsbeurteilung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.security.keypersistence.get.invoke() | Select-Object -ExpandProperty Enabled
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.security.keypersistence.disable.CreateArgs()
$arguments.removeallstoredkeys = $true
$ESXcli.system.security.keypersistence.disable.Invoke($arguments)
```

Referenz der vCenter Server-Sicherheitskontrollen

Diese Sicherheitskontrollen stellen einen grundlegenden Satz bewährter Methoden für die vCenter Server-Sicherheit bereit. Sie sind dahingehend gegliedert, dass die Vor- und Nachteile der Implementierung der Kontrolle verdeutlicht werden. Zum Vornehmen von Änderungen können Sie je nach Steuerung vSphere Client, PowerCLI oder die vCenter Server-Verwaltungsschnittstelle verwenden.

Verwendete PowerCLI und Variablen

Für einige der hier verwendeten PowerCLI-Beispiele muss das Modul „VMware.vSphere.SsoAdmin“ installiert werden.

Die in diesem Abschnitt aufgeführten PowerCLI-Befehle verwenden folgende Variablen:

- $VC="*vcenter_server_name*"

- $VDS="*vsphere_distributed_switch_name*"
- $VDPG="*vsphere_distributed_port_group*"

Festlegen der Zeitüberschreitung bei Inaktivität von vSphere Client

vCenter Server muss vSphere Client-Sitzungen nach 15 Minuten Inaktivität beenden.

Im Leerlauf befindliche vSphere Client-Sitzungen können unbegrenzt geöffnet bleiben, wenn ein Benutzer vergisst, sich abzumelden. Dadurch wird das Risiko eines nicht autorisierten privilegierten Zugriffs erhöht.

Werte

Installationsstandardwert: 120 Minuten

Vorgeschlagener Baseline-Wert: 15 Minuten

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Nicht verfügbar (keine öffentliche API verfügbar)

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar (keine öffentliche API verfügbar)

Festlegen des Standorts in vSphere Client

Verwaltung > Clientkonfiguration > Zeitüberschreitung der Sitzung

Festlegen des Intervalls für fehlgeschlagene Anmeldeversuche

vCenter Server muss das Intervall für die Erfassung fehlgeschlagener Anmeldeversuche auf mindestens 15 Minuten festlegen.

Durch die Begrenzung der Anzahl an fehlgeschlagenen Anmeldeversuchen wird das Risiko eines Brute-Force-Angriffs reduziert, bei dem es durch Erraten von Benutzerkennwörtern zu unbefugten Zugriffen kommt.

Werte

Installationsstandardwert: 180

Empfohlener Baseline-Wert: 900

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-SsoLockoutPolicy | Select FailedAttemptIntervalSec
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-SsoLockoutPolicy | Set-SsoLockoutPolicy -FailedAttemptIntervalSec 900
```

Festlegen des Standorts in vSphere Client

Verwaltung > Single Sign-On > Konfiguration > Lokale Konten > Sperrrichtlinie

Konfigurieren der maximalen Versuche der vSphere-SSO-Sperrrichtlinie

vCenter Server muss nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche ein Konto sperren.

Wiederholte fehlgeschlagene Anmeldungen für ein Konto können Sicherheitsprobleme signalisieren. Sperren Sie zum Begrenzen von Brute-Force-Versuchen das Konto nach einem bestimmten Schwellenwert, um den Ausgleich zwischen der Vermeidung automatischer Verbindungsversuche und potenziellen Denial-of-Service-Angriffen zu erreichen.

Werte

Standardwert der Installation: 5

Empfohlener Baseline-Wert: 5

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-SsoLockoutPolicy | Select MaxFailedAttempts
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-SsoLockoutPolicy | Set-SsoLockoutPolicy -MaxFailedAttempts 5
```

Festlegen des Standorts in vSphere Client

Verwaltung > Single Sign-On > Konfiguration > Lokale Konten > Sperrrichtlinie

Konfigurieren der Entsperrzeit der vSphere-SSO-Sperrrichtlinie

vCenter Server muss Konten nach einem bestimmten Zeitraum entsperren.

Wiederholte fehlgeschlagene Anmeldungen können auf Sicherheitsbedrohungen hinweisen. vCenter Server-Konten sollten nicht automatisch entsperrt werden, wenn sie aufgrund mehrerer fehlgeschlagener Anmeldungen gesperrt wurden. Stellen Sie sicher, dass Sie über Ihre administrator@vsphere.local-Informationen verfügen und dass sie gültig sind.

Werte

Installationsstandardwert: 300

Empfohlener Baseline-Wert: 0

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Wenn Konten nicht automatisch entsperrt werden, kann es zum Denial-of-Service kommen.

PowerCLI-Befehlsbeurteilung

```
Get-SsoLockoutPolicy | Select AutoUnlockIntervalSec
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-SsoLockoutPolicy | Set-SsoLockoutPolicy -AutoUnlockIntervalSec 0
```

Festlegen des Standorts in vSphere Client

Verwaltung > Single Sign-On > Konfiguration > Lokale Konten > Sperrrichtlinie

Erzwingen der Kennwortkomplexität

vCenter Server muss Kennwortkomplexität erzwingen.

Moderne Best Practices für Kennwörter (siehe u. a. NIST 800-63B, Abschnitt 5.1.1.2) zeigen, dass bei angemessener Kennwortentropie die Sicherheit nicht dadurch verbessert wird, dass Benutzer willkürlich zur Änderung ihrer Kennwörter in bestimmten Intervallen aufgefordert werden. Viele automatisierte Sicherheitstools und Frameworks für die Einhaltung behördlicher Auflagen berücksichtigen diese Orientierungshilfe nicht und setzen diese Empfehlung möglicherweise außer Kraft.

Regeln für die Kennwortstärke und -komplexität gelten für Konten, die in vSphere SSO erstellt wurden, einschließlich administrator@vsphere.local (oder administrator@*mydomain*, wenn Sie bei der Installation eine andere Domäne angegeben haben). Diese Regeln gelten nicht für Active Directory-Benutzer, wenn vCenter Server einer Domäne beigetreten ist, da AD diese Kennwortrichtlinien erzwingt.

Werte

Standardwert der Installation:

Maximale Länge: 20

Minimale Länge: 8

Mindestens 1 Sonderzeichen

Mindestens 2 Buchstaben

Mindestens 1 Großbuchstabe

Mindestens 1 Kleinbuchstabe

Mindestens 1 Zahl

3 identische Nachbarn

Empfohlener Baseline-Wert:

Maximale Länge: 64

Minimale Länge: 15

Mindestens 1 Sonderzeichen

Mindestens 2 Buchstaben

Mindestens 1 Großbuchstabe

Mindestens 1 Kleinbuchstabe

Mindestens 1 Zahl

3 identische Nachbarn

Empfohlene Aktion

Ändern Sie die Installationsstandardwerte.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Von anderen Produkte und Diensten im VMware-Ökosystem wird möglicherweise nicht erwartet, dass sich die Anforderungen an die Kennwortkomplexität ändern, und die Installation könnte fehlschlagen.

PowerCLI-Befehlsbeurteilung

```
Get-SsoPasswordPolicy
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-SsoPasswordPolicy | Set-SsoPasswordPolicy -MinLength 15 -MaxLength 64 -MinNumericCount
1 -MinSpecialCharCount 1 -MinAlphabeticCount 2 -MinUppercaseCount 1 -MinLowercaseCount 1
-MaxIdenticalAdjacentCharacters 3
```

Festlegen des Standorts in vSphere Client

Verwaltung > Single Sign-On > Konfiguration > Lokale Konten > Kennwortrichtlinie

Konfigurieren der maximalen Anzahl an Tagen zwischen Kennwortänderungen

vCenter Server muss mit einem angemessenen maximalen Kennwortalter konfiguriert werden.

Moderne Best Practices für Kennwörter (siehe u. a. NIST 800-63B, Abschnitt 5.1.1.2) zeigen, dass bei angemessener Kennwortentropie die Sicherheit nicht dadurch verbessert wird, dass Benutzer willkürlich zur Änderung ihrer Kennwörter in bestimmten Intervallen aufgefordert werden. Viele automatisierte Sicherheitstools und Frameworks für die Einhaltung behördlicher Auflagen berücksichtigen diese Orientierungshilfe nicht und setzen diese Empfehlung möglicherweise außer Kraft.

Werte

Installationsstandardwert: 90

Empfohlener Baseline-Wert: 99999

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-SsoPasswordPolicy | Select PasswordLifetimeDays
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-SsoPasswordPolicy | Set-SsoPasswordPolicy -PasswordLifetimeDays 9999
```

Festlegen des Standorts in vSphere Client

Verwaltung > Single Sign-On > Konfiguration > Lokale Konten > Kennwortrichtlinie

Einschränken der Kennwortwiederverwendung

Konfigurieren Sie die Einstellung für den Kennwortverlauf, um die Wiederverwendung von Kennwörtern auf vCenter Server einzuschränken.

Richtlinien zur Kennwortkomplexität führen manchmal dazu, dass Benutzer ältere Kennwörter wiederverwenden. Das Konfigurieren der Einstellung für den Kennwortverlauf auf vCenter Server kann dazu beitragen, diese Situation zu verhindern.

Werte

Standardwert der Installation: 5

Empfohlener Baseline-Wert: 5

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-SsoPasswordPolicy | Select ProhibitedPreviousPasswordsCount
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-SsoPasswordPolicy | Set-SsoPasswordPolicy -ProhibitedPreviousPasswordsCount 5
```

Festlegen des Standorts in vSphere Client

Verwaltung > Single Sign-On > Konfiguration > Lokale Konten > Kennwortrichtlinie

Konfigurieren des Texts des Anmelde-Banners für den Zugriff über SSH

Konfigurieren Sie den vCenter Server-Text des Anmelde-Banners für den Zugriff über SSH.

vCenter Server ermöglicht eine Anmeldenachricht, die Eindringlinge abschreckt und autorisierten Benutzern Verpflichtungen vermittelt. Diese Konfiguration legt den Text fest, der angezeigt wird, wenn ein Client eine Verbindung über SSH herstellt. Der Standardtext gibt Angreifern Informationen über die Systemkonfiguration preis und sollte geändert werden.

Werte

Installationsstandardwert: VMware vCenter Server- *Version*

Typ: vCenter Server mit einem eingebetteten Platform Services Controller

Vorgeschlagener Baseline-Wert: Wenden Sie sich hinsichtlich des für Ihre Umgebung geltenden Texts an die Rechtsberater Ihrer Organisation.

Beispieltext: Nur autorisierte Benutzer. Die vollzogene oder versuchte unbefugte Nutzung dieses Systems ist verboten und kann straf-, zivil-, sicherheits- oder verwaltungsrechtliche Konsequenzen und/oder Sanktionen nach sich ziehen. Durch die Nutzung dieses Informationssystems erklären Sie sich mit der Überwachung und Aufzeichnung ohne vorherige Ankündigung oder Genehmigung einverstanden. Bei der Nutzung dieses Systems haben Benutzer keinen Anspruch auf Privatsphäre. Sämtliche auf diesem System gespeicherten oder über dieses System übertragenen oder durch Überwachung und/oder Aufzeichnung erlangten Informationen können für Strafverfolgungsbehörden offengelegt und/oder gemäß Bundes- und Landesgesetzen sowie den Richtlinien der Organisation verwendet werden. Verlassen Sie jetzt das System, wenn Sie kein autorisierter Benutzer dieses Systems sind.

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-AdvancedSetting -Entity $VC -Name etc.issue
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-AdvancedSetting -Entity $VC -Name etc.issue | Set-AdvancedSetting -Value "Authorized
users only. Actual or attempted unauthorized use of this system is prohibited and may
result in criminal, civil, security, or administrative proceedings and/or penalties.
Use of this information system indicates consent to monitoring and recording, without
notice or permission. Users have no expectation of privacy in any use of this system.
Any information stored on, or transiting this system, or obtained by monitoring and/or
recording, may be disclosed to law enforcement and/or used in accordance with Federal law,
State statute, and organization policy. If you are not an authorized user of this system,
exit the system at this time."
```

Festlegen des Standorts in vSphere Client

Verwaltung > Single Sign-On > Konfiguration > Anmeldenachricht

Festlegen des Aufgaben- und Aufbewahrungsintervalls

Für vCenter Server muss die Aufgaben- und Ereignisaufbewahrung auf ein geeignetes Intervall festgelegt sein.

vCenter Server behält Aufgaben- und Ereignisdaten bei, bis sie auslaufen, wodurch Speicherplatz gespart wird. Das Alter ist konfigurierbar. Dies wirkt sich nur auf die lokale Speicherung von Ereignisdaten auf der vCenter Server-Appliance aus.

Werte

Standardwert der Installation: 30

Empfohlener Baseline-Wert: 30

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Nicht verfügbar (keine öffentliche API verfügbar)

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar (keine öffentliche API verfügbar)

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Aktivieren der Remoteprotokollierung

Aktivieren Sie die Remoteprotokollierung von vCenter Server-Ereignissen.

Die Remoteprotokollierung auf einem zentralen Host erhöht die Sicherheit von vCenter Server, indem Protokolle sicher gespeichert werden. Die Remoteprotokollierung vereinfacht die Hostüberwachung und unterstützt aggregierte Analysen zur Erkennung koordinierter Angriffe. Die zentralisierte Protokollierung verhindert Manipulationen und dient als zuverlässiger langfristiger Überwachungsdatensatz. Mit der Einstellung `vpxd.event.syslog.enabled` wird die Remoteprotokollierung aktiviert.

Werte

Standardwert der Installation: True.

Empfohlener Baseline-Wert: True

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-AdvancedSetting -Entity $VC -Name vpxd.event.syslog.enabled
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-AdvancedSetting -Entity $VC -Name vpxd.event.syslog.enabled | Set-AdvancedSetting
-Value true
```

Festlegen des Standorts in vSphere Client

vCenter Server auswählen > Konfigurieren > Erweiterte Einstellungen

FIPS aktivieren

vCenter Server muss die FIPS-validierte Kryptografie aktivieren.

Die FIPS-Kryptografie nimmt eine Reihe von Änderungen am System vor, um schwächere Verschlüsselungen zu entfernen. Die Aktivierung von FIPS führt dazu, dass vCenter Server neu gestartet wird.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: True

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Die FIPS-Kryptografie nimmt eine Reihe von Änderungen am System vor, um schwächere Verschlüsselungen zu entfernen. Die Aktivierung von FIPS führt dazu, dass vCenter Server neu gestartet wird.

PowerCLI-Befehlsbeurteilung

```
Invoke-GetSystemGlobalFips
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$spec = Initialize-SystemSecurityGlobalFipsUpdateSpec -Enabled $true
Invoke-SetSystemGlobalFips -SystemSecurityGlobalFipsUpdateSpec $spec
```

Festlegen des Standorts in vSphere Client

Weitere Informationen hierzu finden Sie unter Aktivieren und Deaktivieren von FIPS auf der vCenter Server Appliance.

Konfigurieren von Überwachungsdatensätzen

vCenter Server muss Überwachungsdatensätze erstellen, die Informationen enthalten, um festzustellen, welche Art von Ereignissen aufgetreten ist.

Es ist wichtig, sicherzustellen, dass genügend Informationen in Überwachungsprotokollen für Diagnose- und Diagnosezwecke vorhanden sind. Mit der Einstellung `config.log.level` werden Überwachungsdatensätze konfiguriert.

Werte

Standardwert der Installation: Info

Empfohlener Baseline-Wert: Info

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-AdvancedSetting -Entity $VC -Name config.log.level
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-AdvancedSetting -Entity $VC -Name config.log.level | Set-AdvancedSetting -Value info
```

Festlegen des Standorts in vSphere Client

vCenter Server-Host > Konfigurieren > Erweiterte Einstellungen

Deaktivieren des MAC-Lernvorgangs

Alle Distributed Switch-Portgruppen müssen den MAC-Lernvorgang deaktivieren, sofern die Verwendung nicht absichtlich erfolgt.

Der MAC-Lernvorgang ermöglicht es einem Distributed Switch, Netzwerkkonnektivität für Systeme bereitzustellen, bei denen mehr als eine MAC-Adresse auf einer vNIC verwendet wird. Dies kann in speziellen Fällen nützlich sein, etwa bei verschachtelter Virtualisierung (z. B. bei der Ausführung von ESXi in ESXi). MAC Learning unterstützt auch unbekanntes Unicast Flooding. Wenn ein Paket, das von einem Port empfangen wird, eine unbekannte MAC-Zieladresse aufweist, wird das Paket normalerweise verworfen. Bei aktiviertem Flooding des Datenverkehrs vom Typ „Unbekannter Unicast“ leitet der Port diesen Datenverkehr an jeden Port auf dem

Switch weiter, für den MAC Learning und unbekanntes Unicast-Flooding aktiviert wurden. Diese Eigenschaft ist standardmäßig aktiviert, wenn der MAC-Lernvorgang aktiviert ist. Deaktivieren Sie den MAC-Lernvorgang, es sei denn, er wird absichtlich für eine bekannte Arbeitslast verwendet, die dies erfordert.

Werte

Installationsstandardwert: Deaktiviert

Vorgeschlagener Baseline-Wert: Deaktiviert

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Einige Arbeitslasten verwenden diese Netzwerktaktiken rechtmäßig und sind von den Standardwerten und dem gewünschten Zustand negativ betroffen.

PowerCLI-Befehlsbeurteilung

```
(Get-VDPortgroup -Name
$VDPG).ExtensionData.Config.DefaultPortConfig.MacManagementPolicy.MacLearningPolicy |
Select-Object -ExpandProperty Enabled
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$VDPGview = Get-VDPortgroup -Name $VDPG | Get-View
$ConfigSpec = New-Object VMware.Vim.DVPortgroupConfigSpec
$ConfigSpec.DefaultPortConfig = New-Object VMware.Vim.VMwareDVSPortSetting
$ConfigSpec.DefaultPortConfig.MacManagementPolicy = New-Object
VMware.Vim.DVSMacManagementPolicy
$ConfigSpec.DefaultPortConfig.MacManagementPolicy.MacLearningPolicy = New-Object
VMware.Vim.DVSMacLearningPolicy
$ConfigSpec.DefaultPortConfig.MacManagementPolicy.MacLearningPolicy.Enabled = $false
$ConfigSpec.ConfigVersion = $VDPGview.Config.ConfigVersion
$VDPGview.ReconfigureDVPortgroup_Task($ConfigSpec)
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar. Der MAC-Lernvorgang kann auf einer verteilten virtuellen Portgruppe mithilfe der vSphere API aktiviert werden. Weitere Informationen finden Sie in der *vSphere Web Services-API-Referenz*.

Konfigurieren der Details des Anmeldenachrichten-Banners

Konfigurieren Sie die Details des vCenter Server-Anmelde-Banners für vSphere Client.

vCenter Server bietet die Möglichkeit, eine Anmeldenachricht anzuzeigen. Die Anmeldenachricht wird beispielsweise dazu verwendet, Eindringlinge über die Rechtswidrigkeit ihrer Aktivitäten zu informieren und autorisierten Benutzern mitzuteilen, welche Erwartungen und Verpflichtungen sie bei der Verwendung des Systems erfüllen und akzeptieren müssen. Diese Konfiguration legt den detaillierten Text aus der Nachricht der vSphere Client-Anmeldeseite fest.

Werte

Standardwert der Installation: Nicht konfiguriert

Vorgeschlagener Baseline-Wert: Wenden Sie sich hinsichtlich des für Ihre Umgebung geltenden Texts an die Rechtsberater Ihrer Organisation.

Beispieltext: Nur autorisierte Benutzer. Die vollzogene oder versuchte unbefugte Nutzung dieses Systems ist verboten und kann straf-, zivil-, sicherheits- oder verwaltungsrechtliche Konsequenzen und/oder Sanktionen nach sich ziehen. Durch die Nutzung dieses Informationssystems erklären Sie sich mit der Überwachung und Aufzeichnung ohne vorherige Ankündigung oder Genehmigung einverstanden. Bei der Nutzung dieses Systems haben Benutzer keinen Anspruch auf Privatsphäre. Sämtliche auf diesem System gespeicherten oder über dieses System übertragenen oder durch Überwachung und/oder Aufzeichnung erlangten Informationen können für Strafverfolgungsbehörden offengelegt und/oder gemäß Bundes- und Landesgesetzen sowie den Richtlinien der Organisation verwendet werden. Verlassen Sie jetzt das System, wenn Sie kein autorisierter Benutzer dieses Systems sind.

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Nicht verfügbar (keine öffentliche API verfügbar)

Sie können die Anmeldenachricht konfigurieren, indem Sie den folgenden Befehl in einer Appliance-Shell ausführen:

```
/opt/vmware/bin/sso-config.sh -set_login_banner -title login_banner_title logonBannerFile
```

Beachten Sie, die Shell erneut zu deaktivieren, wenn Sie fertig sind.

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar (keine öffentliche API verfügbar)

Sie können die Anmeldenachricht konfigurieren, indem Sie den folgenden Befehl in einer Appliance-Shell ausführen:

```
/opt/vmware/bin/sso-config.sh -set_login_banner -title login_banner_title logonBannerFile
```

Beachten Sie, die Shell erneut zu deaktivieren, wenn Sie fertig sind.

Festlegen des Standorts in vSphere Client

Verwaltung > Single Sign-On > Konfiguration > Anmeldenachricht > Bearbeiten

Aktivieren des Anmelde-Banners

Aktivieren Sie das vCenter Server-Anmelde-Banner für vSphere Client.

vCenter Server bietet die Möglichkeit, eine Anmeldenachricht anzuzeigen. Die Anmeldenachricht wird beispielsweise dazu verwendet, Eindringlinge über die Rechtswidrigkeit ihrer Aktivitäten zu informieren und autorisierten Benutzern mitzuteilen, welche Erwartungen und Verpflichtungen sie bei der Verwendung des Systems erfüllen und akzeptieren müssen. Diese Konfiguration aktiviert die Anzeige der Nachricht auf der Anmeldeseite des vSphere Client.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: True

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Nicht verfügbar (keine öffentliche API verfügbar)

Sie können die Anmeldenachricht konfigurieren, indem Sie den folgenden Befehl in einer Appliance-Shell ausführen:

```
/opt/vmware/bin/sso-config.sh -set_logon_banner -title logon_banner_title logonBannerFile
```

Beachten Sie, die Shell erneut zu deaktivieren, wenn Sie fertig sind.

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar (keine öffentliche API verfügbar)

Sie können die Anmeldenachricht konfigurieren, indem Sie den folgenden Befehl in einer Appliance-Shell ausführen:

```
/opt/vmware/bin/sso-config.sh -set_logon_banner -title logon_banner_title logonBannerFile
```

Beachten Sie, die Shell erneut zu deaktivieren, wenn Sie fertig sind.

Festlegen des Standorts in vSphere Client

Verwaltung > Single Sign-On > Konfiguration > Anmeldenachricht > Bearbeiten

Konfigurieren des Texts des Anmelde-Banners

Konfigurieren Sie den vCenter Server-Text des Anmelde-Banners für vSphere Client.

vCenter Server bietet die Möglichkeit, eine Anmeldenachricht anzuzeigen. Die Anmeldenachricht wird beispielsweise dazu verwendet, Eindringlinge über die Rechtswidrigkeit ihrer Aktivitäten zu informieren und autorisierten Benutzern mitzuteilen, welche Erwartungen und Verpflichtungen sie bei der Verwendung des Systems erfüllen und akzeptieren müssen. Mit dieser Konfiguration wird der Text festgelegt, der auf der Anmeldeseite von vSphere Client angezeigt wird.

Werte

Standardwert der Installation: Nicht konfiguriert

Vorgeschlagener Baseline-Wert: Wenden Sie sich hinsichtlich des spezifischen Texts an die Rechtsberater Ihrer Organisation.

Beispieltext: Durch die Verwendung dieses Systems werden die Organisationsrichtlinien, die dieses System regeln, zur Kenntnis genommen und ihnen zugestimmt.

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Nicht verfügbar (keine öffentliche API verfügbar)

Sie können die Anmeldenachricht konfigurieren, indem Sie den folgenden Befehl in einer Appliance-Shell ausführen:

```
/opt/vmware/bin/sso-config.sh -set_logon_banner -title logon_banner_title logonBannerFile
```

Beachten Sie, die Shell erneut zu deaktivieren, wenn Sie fertig sind.

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar (keine öffentliche API verfügbar)

Sie können die Anmeldenachricht konfigurieren, indem Sie den folgenden Befehl in einer Appliance-Shell ausführen:

```
/opt/vmware/bin/sso-config.sh -set_logon_banner -title logon_banner_title logonBannerFile
```

Beachten Sie, die Shell erneut zu deaktivieren, wenn Sie fertig sind.

Festlegen des Standorts in vSphere Client

Verwaltung > Single Sign-On > Konfiguration > Anmeldenachricht > Bearbeiten

Separate Authentifizierung und Autorisierung für Administratoren

vCenter Server muss die Authentifizierung und Autorisierung für Administratoren trennen.

Die Kombination aus Authentifizierung und Autorisierung, wie dies bei Diensten wie Active Directory der Fall ist, birgt im Falle von Kompromittierungen das Risiko von Infrastrukturverstößen. Stellen Sie daher für vCenter Server sicher, dass Sie Authentifizierung und Autorisierung für Administratoren trennen. Erwägen Sie nach Möglichkeit die Verwendung von lokalen SSO-Gruppen für die Autorisierung, um Risiken besser zu verwalten.

Werte

Standardwert der Installation: Nicht konfiguriert

Vorgeschlagener Baseline-Wert: Nicht konfiguriert

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Für die Bereitstellung des vCenter Server-Zugriffs war eine Interaktion mit vCenter Server-SSO erforderlich. Automatisierung ist mit PowerCLI möglich.

PowerCLI-Befehlsbeurteilung

Nicht verfügbar (keine öffentliche API verfügbar)

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar (keine öffentliche API verfügbar)

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Festlegen der Richtlinie für gefälschte Übertragungen auf „Ablehnen“

Legen Sie alle Distributed Switches und deren Portgruppen so fest, dass gefälschte Übertragungen abgelehnt werden.

Eine virtuelle Maschine kann die Identität von Netzwerkadaptern annehmen, indem sie MAC-Adressen ändert, was Sicherheitsbedrohungen darstellt. Indem die Option „Gefälschte Übertragungen“ auf allen Distributed Switches und Portgruppen auf „Ablehnen“ festgelegt wird, überprüft ESXi MAC-Adressen und verhindert einen solchen Identitätswechsel.

Werte

Standardwert der Installation: Ablehnen

Empfohlener Baseline-Wert: Ablehnen

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Einige Arbeitslasten verwenden diese Netzwerktaktiken rechtmäßig und sind standardmäßig negativ betroffen.

PowerCLI-Befehlsbeurteilung

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy | Set-VDSecurityPolicy -ForgedTransmits
$false
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy | Set-VDSecurityPolicy -ForgedTransmits
$false
```

Festlegen des Standorts in vSphere Client

Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Festlegen der Richtlinie „MAC-Adressänderungen“ auf „Ablehnen“

Legen Sie die Richtlinie „MAC-Adressänderungen“ auf dem vSphere Standard-Switch und den dazu gehörigen Portgruppen auf „Ablehnen“ fest.

Das Zulassen, dass virtuelle Maschinen MAC-Adressen ändern, stellt Sicherheitsrisiken dar und ermöglicht eine mögliche Imitation von Netzwerkadaptern. Die Ablehnung von MAC-Änderungen auf allen Distributed Switches und Portgruppen verhindert dies, kann sich jedoch auf bestimmte Anwendungen wie Microsoft Clustering oder die von der MAC-Adresse abhängige Lizenzierung auswirken. Nehmen Sie bei Bedarf Ausnahmen von dieser Sicherheitsleitlinie vor.

Werte

Standardwert der Installation: Ablehnen

Empfohlener Baseline-Wert: Ablehnen

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Einige Arbeitslasten verwenden diese Netzwerktaktiken rechtmäßig und werden durch die Einstellung „Ablehnen“ negativ beeinflusst.

PowerCLI-Befehlsbeurteilung

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy
```

PowerCLI-Befehlsbeurteilung

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy | Set-VDSecurityPolicy -MacChanges $false
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy | Set-VDSecurityPolicy -MacChanges
$false
```

Festlegen des Standorts in vSphere Client

Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Festlegen der Richtlinie „Promiskuitiver Modus“ auf „Ablehnen“

Legen Sie die Richtlinie „Promiskuitiver Modus“ auf dem vSphere Standard-Switch und dessen Portgruppen auf „Ablehnen“ fest.

Durch die Aktivierung des promiskuitiven Modus für eine Portgruppe können alle verbundenen virtuellen Maschinen alle Netzwerkpakete lesen, was ein potenzielles Sicherheitsrisiko darstellt. Obwohl das Zulassen des promiskuitiven Modus manchmal für das Debugging oder die Überwachung erforderlich ist, wird die Standardeinstellung „Ablehnen“ empfohlen. Nehmen Sie nach Bedarf Ausnahmen für bestimmte Portgruppen vor.

Werte

Standardwert der Installation: Ablehnen

Empfohlener Baseline-Wert: Ablehnen

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Einige Arbeitslasten verwenden diese Netzwerktaktiken rechtmäßig und werden durch die Einstellung „Ablehnen“ negativ beeinflusst.

PowerCLI-Befehlsbeurteilung

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy | Set-VDSecurityPolicy -AllowPromiscuous
$false
```

```
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy | Set-VDSecurityPolicy
-AllowPromiscuous $false
```

Festlegen des Standorts in vSphere Client

Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Zurücksetzen von Portkonfigurationen beim Trennen von virtuellen Maschinen

vCenter Server muss die Portkonfiguration zurücksetzen, wenn virtuelle Maschinen getrennt werden.

Wenn eine virtuelle Maschine vom virtuellen Switch-Port getrennt wird, ist es wünschenswert, sollte die Portkonfiguration zurückgesetzt werden, damit eine andere virtuelle Maschine, die angehängt wird, über einen Port in einem bekannten Zustand verfügt.

Werte

Standardwert der Installation: Aktiviert

Empfohlener Baseline-Wert: Aktiviert

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
(Get-VDPortgroup -Name $VDPG).ExtensionData.Config.Policy | Select-Object -ExpandProperty
PortConfigResetAtDisconnect
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$VDPGview = Get-VDPortgroup -Name $VDPG | Get-View
$ConfigSpec = New-Object VMware.Vim.DVPortgroupConfigSpec
$ConfigSpec.DefaultPortConfig = New-Object VMware.Vim.VMwareDVSPortSetting
$ConfigSpec.Policy = New-Object VMware.Vim.VMwareDVSPortgroupPolicy
$ConfigSpec.Policy.PortConfigResetAtDisconnect = $true
$ConfigSpec.ConfigVersion = $VDPGview.Config.ConfigVersion
$VDPGview.ReconfigureDVPortgroup_Task($ConfigSpec)
```

Festlegen des Standorts in vSphere Client

Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Deaktivieren von Cisco Discovery Protocol oder Link Layer Discovery Protocol

Deaktivieren Sie die Teilnahme am Cisco Discovery Protocol (CDP) oder LLDP (Link Layer Discovery Protocol) auf Distributed Switches, sofern nicht absichtlich verwendet.

Der vSphere Distributed Virtual Switch kann CDP oder LLDP einbinden und potenziell vertrauliche unverschlüsselte Informationen wie IP-Adressen und Systemnamen im Netzwerk teilen. So können CDP und LLDP Angreifern dabei helfen, Ihre Umgebung zu verstehen oder zu imitieren. CDP und LLDP sind jedoch auch äußerst hilfreich für legitime Anwendungsfälle. Deaktivieren Sie CDP und LLDP, es sei denn, dies ist für die Fehlerbehebung oder Konfigurationsvalidierung erforderlich.

Werte

Installationsstandardwert: Überwachen

Vorgeschlagener Baseline-Wert: Keine

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
(Get-VDSwitch -Name $VDS).ExtensionData.config.LinkDiscoveryProtocolConfig | Select-Object
-ExpandProperty Operation
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$VDview = Get-VDSwitch -Name $VDS | Get-View
$ConfigSpec = New-Object VMware.Vim.VMwareDVSConfigSpec
$ConfigSpec.LinkDiscoveryProtocolConfig = New-Object VMware.Vim.LinkDiscoveryProtocolConfig
$ConfigSpec.LinkDiscoveryProtocolConfig.Protocol = 'cdp'
$ConfigSpec.LinkDiscoveryProtocolConfig.Operation = 'none'
$ConfigSpec.ConfigVersion = $VDview.Config.ConfigVersion
$VDview.ReconfigureDvs_Task($ConfigSpec)
```

Festlegen des Standorts in vSphere Client

Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Sicherstellen des NetFlow-Datenverkehrempfangs durch autorisierte Collectors

vCenter Server muss sicherstellen, dass NetFlow-Datenverkehr an autorisierte Collectors gesendet wird.

Die vSphere Distributed Switch kann unverschlüsselte NetFlow-Daten exportieren und Details zu virtuellen Netzwerken und Datenverkehrsmustern anzeigen. Stellen Sie sicher, dass die NetFlow-Nutzung autorisiert und ordnungsgemäß konfiguriert ist, um Datenlecks zu verhindern.

Werte

Installationsstandardwert: Überwachen

Vorgeschlagener Baseline-Wert: Keine

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
(Get-VDSwitch -Name $VDS).ExtensionData.config.IpfixConfig.CollectorIpAddress | Select-
Object -ExpandProperty CollectorIpAddress
(Get-VDPortgroup -Name $VDPG).ExtensionData.Config.DefaultPortConfig.IpfixEnabled | Select-
Object -ExpandProperty Value
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$VDPGview = Get-VDPortgroup -Name $VDPG | Get-View
$ConfigSpec = New-Object VMware.Vim.DVPortgroupConfigSpec
$ConfigSpec.DefaultPortConfig = New-Object VMware.Vim.VMwareDVSPortSetting
$ConfigSpec.DefaultPortConfig.IpfixEnabled = New-Object VMware.Vim.BoolPolicy
$ConfigSpec.DefaultPortConfig.IpfixEnabled.Inherited = $false
$ConfigSpec.DefaultPortConfig.IpfixEnabled.Value = $false
$ConfigSpec.ConfigVersion = $VDPGview.Config.ConfigVersion
$VDPGview.ReconfigureDVPortgroup_Task($ConfigSpec)
```

Festlegen des Standorts in vSphere Client

Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Konfigurieren der Portsicherheit für virtuelle Maschinen

Der vCenter Server darf die Portgruppeneinstellungen auf Portebene auf Distributed Switches nicht außer zum Blockieren von Ports außer Kraft setzen.

Für die Einrichtung eindeutiger virtueller Maschinen sind möglicherweise Außerkraftsetzungen der Konfiguration auf Portebene erforderlich. Achten Sie jedoch darauf, diese zu überwachen, um eine nicht autorisierte Verwendung zu verhindern. Nicht überwachte Außerkraftsetzungen können einen breiteren Zugriff ermöglichen, wenn eine weniger sichere Distributed Switch-Konfiguration ausgenutzt wird.

Werte

Standardwert der Installation:

Außerkraftsetzung von „Ports blockieren“: TRUE

Alle anderen Außerkraftsetzungen: FALSE

Empfohlener Baseline-Wert:

Außerkraftsetzung von „Ports blockieren“: TRUE

Alle anderen Außerkraftsetzungen: FALSE

Empfohlene Aktion

Überwachen Sie die Standardeinstellung für die Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
(Get-VDPortgroup -Name $VDPG).ExtensionData.Config.Policy
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$VDPGview = Get-VDPortgroup -Name $VDPG | Get-View
$ConfigSpec = New-Object VMware.Vim.DVPortgroupConfigSpec
$ConfigSpec.DefaultPortConfig = New-Object VMware.Vim.VMwareDVSPortSetting
$ConfigSpec.Policy = New-Object VMware.Vim.VMwareDVSPortgroupPolicy
$ConfigSpec.Policy.UplinkTeamingOverrideAllowed = $false
$ConfigSpec.Policy.BlockOverrideAllowed = $true
$ConfigSpec.Policy.LivePortMovingAllowed = $false
$ConfigSpec.Policy.VlanOverrideAllowed = $false
$ConfigSpec.Policy.SecurityPolicyOverrideAllowed = $false
$ConfigSpec.Policy.VendorConfigOverrideAllowed = $false
$ConfigSpec.Policy.ShapingOverrideAllowed = $false
$ConfigSpec.Policy.IpfixOverrideAllowed = $false
$ConfigSpec.Policy.TrafficFilterOverrideAllowed = $false
$ConfigSpec.ConfigVersion = $VDPGview.Config.ConfigVersion
$VDPGview.ReconfigureDVPortgroup_Task($ConfigSpec)
```

Festlegen des Standorts in vSphere Client

Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Entfernen des Port-Mirroring

vCenter Server muss nicht autorisierte Port-Mirroring-Sitzungen auf Distributed Switches entfernen.

Der vSphere Distributed Switch kann den Datenverkehr zwischen Ports spiegeln, wodurch die Datenverkehrsbeobachtung aktiviert wird. Zur Aufrechterhaltung der Sicherheit müssen alle nicht autorisierten Port-Mirroring-Sitzungen auf Distributed Switches entfernt werden.

Werte

Standardwert der Installation: Nicht konfiguriert

Vorgeschlagener Baseline-Wert: Nicht konfiguriert

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
(Get-VDSwitch -Name $VDS).ExtensionData.config.VspanSession
```

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar

Festlegen des Standorts in vSphere Client

Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Einschränken von Virtual Guest Tagging

vCenter Server muss die Verwendung von Virtual Guest Tagging (VGT) auf Distributed Switches einschränken.

Wenn Sie eine Portgruppe auf VLAN 4095 festlegen, wird Virtual Guest Tagging (VGT) ermöglicht, sodass die virtuelle Maschine VLAN-Tags verarbeiten muss. Aktivieren Sie VGT nur für die virtuellen Maschinen, die zur Verwaltung von VLAN-Tags autorisiert und ausgestattet sind. Eine unangemessene Verwendung kann zu Denial-of-Service-Szenarien oder nicht autorisierten VLAN-Datenverkehrsinteraktionen führen.

Werte

Standardwert der Installation: Nicht konfiguriert

Vorgeschlagener Baseline-Wert: Nicht konfiguriert

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VDPortgroup -Name $VDPG | Where {$_.ExtensionData.Config.Uplink -ne "True"} | Select
Name,VlanConfiguration
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VDPortgroup $VDPG | Set-VDVlanConfiguration -VlanId "New_VLAN#"
```

Festlegen des Standorts in vSphere Client

Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Prüfung auf VMware-Wartung in der vCenter Server-Version

Stellen Sie sicher, dass die vCenter Server-Version nicht den VMware-Status „Ende des allgemeinen Supports“ erreicht hat.

Werte

Standardwert der Installation: Nicht verfügbar

Empfohlener Baseline-Wert: Nicht verfügbar

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar

Festlegen des Speicherorts in der vCenter Server-Verwaltungsschnittstelle

Aktualisieren

Einschränken des Zugriffs auf SSH

Der vCenter Server-SSH-Dienst muss deaktiviert werden.

vCenter Server Appliance wird als Appliance bereitgestellt und ist für die Verwaltung über die vCenter Server-Verwaltungsschnittstelle, vSphere Client und die APIs vorgesehen. SSH ist ein Fehlerbehebungs- und Support-Tool, das nur bei Bedarf aktiviert werden sollte. vCenter Server High Availability verwendet SSH, um die Replizierung und das Failover zwischen den Knoten zu koordinieren. Die Verwendung dieser Funktion erfordert, dass SSH aktiviert bleibt.

Werte

Installationsstandardwert: Deaktiviert

Vorgeschlagener Baseline-Wert: Deaktiviert

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Hinweis Sie müssen zuerst mithilfe des `Connect-CISServer`-Cmdlets eine Verbindung mit dem vCenter Server-Host herstellen.

```
(Get-CisService -Name "com.vmware.appliance.access.ssh").get()
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
(Get-CisService -Name "com.vmware.appliance.access.ssh").set($false)
```

Festlegen des Speicherorts in der vCenter Server-Verwaltungsschnittstelle

Zugriff

Überprüfen des Ablaufs des Root-Benutzerkennworts

Der Kennwortablauf des vCenter Server-Root-Kontos muss entsprechend konfiguriert werden.

Moderne Best Practices für Kennwörter (u. a. NIST 800-63B, Abschnitt 5.1.1.2) zeigen, dass bei angemessener Kennwortentropie die Sicherheit nicht dadurch verbessert wird, dass Benutzer willkürlich zur Änderung ihrer Kennwörter in bestimmten Intervallen aufgefordert werden. Viele automatisierte Sicherheitstools und Frameworks für die Einhaltung behördlicher Auflagen berücksichtigen diese Orientierungshilfe nicht und setzen diese Empfehlung möglicherweise außer Kraft.

Werte

Standardwert der Installation: Ja

Empfohlener Baseline-Wert: Nein

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Wenn das Kennwort vor seinem Ablauf nicht zurückgesetzt werden kann, sind Wiederherstellungsverfahren erforderlich.

PowerCLI-Befehlsbeurteilung

Hinweis Sie müssen zuerst mithilfe des `Connect-CISServer`-Cmdlets eine Verbindung mit dem vCenter Server-Host herstellen.

```
(Get-CisService -Name "com.vmware.appliance.local_accounts.policy").get()
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
(Get-CisService -Name "com.vmware.appliance.local_accounts.policy").set(@{max_days=9999;
min_days=1; warn_days=7})
```

Festlegen des Speicherorts in der vCenter Server-Verwaltungsschnittstelle

Administration

Konfigurieren der dateibasierten Sicherung und Wiederherstellung

Konfigurieren Sie die dateibasierte Sicherung und Wiederherstellung, sodass Sie Ihre vCenter Server Appliance und deren Konfiguration mithilfe des Installationsprogramms für vCenter Server wiederherstellen können. Die Sicherung und Wiederherstellung ist ein wichtiger Bestandteil beim Schützen Ihrer Umgebung.

Werte

Standardwert der Installation: Nicht konfiguriert

Vorgeschlagener Baseline-Wert: Konfiguriert

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar

Festlegen des Speicherorts in der vCenter Server-Verwaltungsschnittstelle

Sicherung

Konfigurieren der Firewall, sodass nur Datenverkehr von autorisierten Netzwerken zugelassen wird

vCenter Server Appliance muss die Firewall so konfigurieren, dass nur Datenverkehr von autorisierten Netzwerken zugelassen wird.

Stellen Sie sicher, dass der gesamte eingehende und ausgehende Netzwerkdatenverkehr blockiert wird, sofern nicht explizit zugelassen, wodurch die Angriffsfläche reduziert und nicht autorisierter Zugriff auf das System verhindert wird. Ausgehender (Egress-)Datenverkehr wird weder blockiert noch sind verwandte oder hergestellte Verbindungen vorhanden, sodass vCenter Server Appliance weiterhin mit Systemen kommunizieren kann, auf denen die Verbindung initiiert wird. Verwenden Sie Perimeter-Firewalls, um diese Verbindungstypen zu drosseln.

Werte

Installationsstandardwert: Verbindungen von jeder IP-Adresse zulässig.

Vorgeschlagener Baseline-Wert: Verbindungen sind nur von autorisierten Infrastruktur- und Verwaltungsarbeitsstationen zulässig.

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Konnektivitätsverlust. Stellen Sie sicher, dass Sie eine Zulassungsregel für sich selbst konfigurieren, bevor Sie eine Regel vom Typ „Alle verweigern“ konfigurieren.

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar

Festlegen des Speicherorts in der vCenter Server-Verwaltungsschnittstelle

Firewall

Konfigurieren des Remoteprotokollservers

Konfigurieren Sie einen Remoteprotokollserver für vCenter Server.

Die Remoteprotokollierung auf einem zentralen Host erhöht die Sicherheit von vCenter Server, indem Protokolle sicher gespeichert werden. Die Remoteprotokollierung vereinfacht die Hostüberwachung und unterstützt aggregierte Analysen zur Erkennung koordinierter Angriffe. Die zentralisierte Protokollierung verhindert Manipulationen und dient als zuverlässiger langfristiger Überwachungsdatensatz.

Werte

Standardwert der Installation: Nicht konfiguriert

Vorgeschlagener Baseline-Wert: Sitespezifischer Protokollserver

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Hinweis Sie müssen zuerst mithilfe des `Connect-CISServer`-Cmdlets eine Verbindung mit dem vCenter Server-Host herstellen.

```
(Get-CisService -Name "com.vmware.appliance.logging.forwarding").get()
```

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Konfigurieren der Uhrzeitsynchronisierung

vCenter Server muss über zuverlässige Zeitsynchronisierungsquellen verfügen.

Kryptografie, Überwachungsprotokollierung, Clustervorgänge sowie Reaktion auf Vorfälle und Forensik sind stark von der synchronisierten Uhrzeit abhängig. Für NTP (Network Time Protocol) müssen mindestens vier Quellen verfügbar sein. Wenn Sie sich zwischen zwei Quellen oder einer Quelle entscheiden müssen, sollten Sie eine Quelle vorziehen.

Werte

Standardwert der Installation: Nicht definiert

Vorgeschlagener Baseline-Wert: sitespezifisch oder:

0.vmware.pool.ntp.org,

1.vmware.pool.ntp.org,

2.vmware.pool.ntp.org,

3.vmware.pool.ntp.org

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Hinweis Sie müssen zuerst mithilfe des `Connect-CISServer`-Cmdlets eine Verbindung mit dem vCenter Server-Host herstellen.

```
(Get-CisService -Name ""com.vmware.appliance.timesync"").get()
(Get-CisService -Name ""com.vmware.appliance.ntp"").get()
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
(Get-CisService -Name ""com.vmware.appliance.timesync"").set(""NTP"")
(Get-CisService -Name
""com.vmware.appliance.ntp"").set(""0.vmware.pool.ntp.org,1.vmware.pool.ntp.org,2.vmware.po
ol.ntp.org,3.vmware.pool.ntp.org"")
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Installieren von Software-Updates

Stellen Sie sicher, dass in vCenter Server alle Software-Updates installiert sind.

Indem vCenter Server-Patches auf dem neuesten Stand gehalten werden, können Schwachstellen verringert werden. Angreifer können bekannte Schwachstellen ausnutzen, wenn sie versuchen, nicht autorisierten Zugriff zu erlangen oder Rechte zu erhöhen.

Aktualisieren Sie beim Anwenden von Updates zuerst vCenter Server, wenn ein Update verfügbar ist, und fahren Sie dann mit der Aktualisierung von ESXi fort. Diese Reihenfolge stellt sicher, dass die Verwaltungsebene aktualisiert wird, bevor die ESXi-Hosts aktualisiert werden.

Werte

Standardwert der Installation: Nicht verfügbar

Empfohlener Baseline-Wert: Nicht verfügbar

Empfohlene Aktion

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

Nicht verfügbar

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar

Festlegen des Standorts in vSphere Client

Informationen finden Sie in der Dokumentation *Verwalten des Lebenszyklus von Host und Cluster*.

Rotieren des vpxuser-Kennworts

vCenter Server muss das vpxuser-Kennwort so konfigurieren, dass es in einem geeigneten Intervall rotiert wird.

Mit der Einstellung `VirtualCenter.VimPasswordExpirationInDays` wird der Rotationszeitraum konfiguriert. Stellen Sie sicher, dass vCenter Server das Kennwort, das automatisch auf den ESXi-Hosts festgelegt wird, ordnungsgemäß rotiert.

Werte

Standardwert der Installation: 30

Empfohlener Baseline-Wert: 30

Empfohlene Aktion

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-AdvancedSetting -Entity $VC -Name VirtualCenter.VimPasswordExpirationInDays
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-AdvancedSetting -Entity $VC -Name VirtualCenter.VimPasswordExpirationInDays | Set-
AdvancedSetting -Value 30
```

Festlegen des Standorts in vSphere Client

vCenter Server auswählen > Konfigurieren > Erweiterte Einstellungen

Referenz zu Sicherheitskontrollen für virtuelle Maschinen

Diese Sicherheitskontrollen stellen einen Baseline-Satz von Best Practices für die Sicherheit virtueller Maschinen bereit. Sie sind dahingehend gegliedert, dass die Vor- und Nachteile der Implementierung der Kontrolle verdeutlicht werden. Erweiterte Systemeinstellungen können Sie entweder über die bereitgestellte PowerCLI ändern oder unter vSphere Client (**Host > Konfigurieren > System > Erweiterte Systemeinstellungen**).

Verwendete Variable

Die in diesem Abschnitt vorgestellten PowerCLI-Befehle verwenden folgende Variable:

- $VM = "*virtual_machine_name*"

mks.enable3d

Deaktiviert 3D-Grafikfunktionen auf virtuellen Maschinen, die nicht benötigt werden, um potenzielle Angriffsvektoren zu reduzieren und so die allgemeine Systemsicherheit zu verbessern.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: False

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting mks.enable3d
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting mks.enable3d | Set-AdvancedSetting -Value FALSE
```

ethernet*.filter*.name

Beschränkt den Zugriff auf virtuelle Maschinen über die Netzwerk-API „dvFilter“.

Die Schnittstelle „dvFilter“ wird von Tools wie NSX zum Filtern und Überprüfen des Netzwerkdatenverkehrs verwendet. Sie kann auch von anderen Tools verwendet werden. Stellen Sie sicher, dass diese Tools autorisiert sind.

Werte

Installationsstandardwert: nicht vorhanden

Vorgeschlagener Baseline-Wert: nicht vorhanden

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Legitime Netzwerktools, einschließlich NSX, erfordern möglicherweise diese Funktionalität.

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting "ethernet*.filter*.name*"
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting "ethernet*.filter*.name*" | Remove-AdvancedSetting
```

Verhindern, dass virtuelle Maschinen von nicht autorisierten Quellen gestartet werden

Virtuelle Maschinen müssen das Starten von nicht autorisierten Quellen verhindern.

Ein nicht autorisierter Zugriff auf eine virtuelle Maschine kann auftreten, wenn das primäre Startvolume nicht verfügbar ist und die EFI-Firmware alternative Startquellen sucht, etwa den Netzwerkstart. Dies kann durch Netzwerksteuerungen sowie durch die erweiterten Parameter `bios.bootDeviceClasses`, `bios.bootOrder` und `bios.hddOrder` verringert werden.

`bios.bootDeviceClasses` hat das Format „allow:XXXX“ oder „deny:XXXX“, wobei XXXX eine kommagetrennte Liste von Startklassen ist. Zu den Startklassen zählen „net“ (Netzwerk-PXE-Start), „usb“ (von angehängten USB-Geräten), „pcmcia“ (PCMCIA-Erweiterungskarten, derzeit nicht verwendet), „cd“ (von angehängten virtuellen CD-/DVD-Geräten), „hd“ (von angehängten virtuellen Festplatten), „fd“ (von virtuellen Diskettenlaufwerken), „reserved“ (von unbekannten Geräten), efishell (in die EFI-Shell) und „all“ oder „any“ (mit „all“ identisch).

Die Verwendung von „allow“ oder „deny“ gibt auch implizit das Gegenteil an. Beispiel:

- „deny:all“ verbietet alle Startklassen.
- „deny:net“ lässt den Netzwerkstart nicht zu, lässt aber alle anderen zu.
- „allow:hd“ lässt nur den Festplattenstart zu und verweigert alle anderen.
- „allow:hd,cd“ lässt den Festplattenstart und dann den Start des CD-Geräts zu und verweigert alle anderen.

Es kann sein, dass für neue virtuelle Maschinen ein CD-/DVD-Start erforderlich ist. Zudem kann es sein, dass einige dynamische Umgebungen, etwa Labs, den Netzwerkstart verwenden. Legen Sie diese Umgebungen entsprechend fest, und dokumentieren Sie Ihre Begründung.

Werte

Installationsstandardwert: allow:all

Vorgeschlagener Baseline-Wert: allow:hd (sobald das Gastbetriebssystem installiert ist)

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Die virtuelle Maschine kann nicht mehr von nicht spezifizierten Quellen gestartet werden, was sich negativ auf Situationen auswirken kann, in denen PXE-Start- oder Wiederherstellungsmedien erforderlich sind. Der Parameter kann jedoch problemlos über PowerCLI skaliert werden. Ein alternativer Ansatz besteht darin, verweigerte Methoden wie „deny:net“ anzugeben.

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting bios.bootDeviceClasses
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting bios.bootDeviceClasses | Set-AdvancedSetting -Value
"allow:hd"
```

RemoteDisplay.maxConnections

Beschränkt die Anzahl der Konsolenverbindungen mit einer virtuellen Maschine.

Die Begrenzung der gemeinsamen Nutzung der Konsole für die virtuelle Maschine auf einen Benutzer verhindert mehrere Beobachter und erhöht so die Sicherheit. Dies kann jedoch versehentlich dazu führen, dass Dienste abgelehnt werden.

Werte

Installationsstandardwert: -1

Empfohlener Baseline-Wert: 1

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Es kann zu einer Denial-of-Service-Bedingung kommen, bei der die Konsole nicht verwendet werden kann, weil der eine Benutzer verbunden ist oder eine getrennte Konsolensitzung

weiterhin besteht. Für andere Produkte, etwa VMware Cloud Director, kann es sein, dass diese Option auf einen höheren Wert festgelegt werden muss.

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting RemoteDisplay.maxConnections
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting RemoteDisplay.maxConnections | Set-AdvancedSetting
-Value 1
```

Begrenzen der Passthrough-Funktionalität des PCI-Geräts

Virtuelle Maschinen müssen die Passthrough-Funktionalität des PCI-Geräts begrenzen.

DirectPath E/A-Funktionen ermöglichen virtuellen Maschinen den direkten Zugriff auf Systemhardware, was sich auf Tools zur Risikominderung wie vMotion, DRS und Hochverfügbarkeit auswirkt. DirectPath E/A-Funktionen bieten Angreifern möglicherweise auch privilegierten Hardwarezugriff. Stellen Sie sicher, dass nur erforderliche virtuelle Maschinen über dieses Recht verfügen, was durch Gastbetriebssystem-Sicherheitskontrollen kompensiert wird.

Werte

Installationsstandardwert: nicht vorhanden

Vorgeschlagener Baseline-Wert: nicht vorhanden

Aktion erforderlich

Überwachungsprotokoll

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Passthrough-Geräte, etwa GPUs, wären negativ betroffen, wenn sie getrennt werden. Überwachen und dokumentieren Sie die geschäftlichen Anforderungen für diese virtuellen Maschinen.

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-PassthroughDevice
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-PassthroughDevice | Remove-PassthroughDevice
```

Entfernen unnötiger virtueller Hardwaregeräte für virtuelle Maschinen

Virtuelle Maschinen müssen unnötige virtuelle Hardware entfernen.

Vermeiden Sie unnötige virtuelle Hardware von virtuellen Maschinen, um potenzielle Angriffsflächen zu reduzieren. Selten verwendete Ports, temporäre CD-/DVD-Laufwerke und Hardware, die durch Migrationen eingeführt werden, könnten anfällig sein. Wenn Sie diese entfernen, verringert sich das Risiko, dass Software eingeführt wird oder Daten aus einer geschützten Umgebung herausgeschleust werden.

Werte

Installationsstandardwert: Konfiguriert

Vorgeschlagener Baseline-Wert: nicht vorhanden

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Das Entfernen des CD-ROM-Geräts kann sich auf die Installation und Wartung von VMware Tools auswirken. Das Entfernen von XHCI-Controllern kann sich für einige Gastbetriebssysteme auswirken auf die Konnektivität von Tastatur und Maus der Konsole.

PowerCLI-Befehlsbeurteilung

```
$VMview = Get-VM -Name $VM | Get-View
$UnnecessaryHardware
= "VirtualUSBController|VirtualUSBXHCIController|VirtualParallelPort|VirtualFloppy|
VirtualSerialPort|VirtualHdAudioCard|VirtualAHCIController|VirtualEnsoniq1371|VirtualCdrom"

$VMview.Config.Hardware.Device | Where-Object {$_.GetType().Name -match
$UnnecessaryHardware} | Foreach-Object {
    $devname = $_.GetType().Name
    Write-Host "$VM`: [WARNING] VM has a $devname device. Please evaluate and consider
removing." -ForegroundColor Yellow
}
```

Beispiel für PowerCLI-Befehlsstandardisierung

Nicht verfügbar

Festlegen des Standorts in vSphere Client

Virtuelle Maschine > Einstellungen bearbeiten > Virtuelle Hardware

tools.guestlib.enableHostInfo

Verhindert, dass virtuelle Maschinen Hostinformationen über den Hypervisor abrufen.

Indem verhindert wird, dass virtuelle Maschinen Hostinformationen über den Hypervisor abrufen, verringert sich das Risiko erweiterter Angriffe, da Angreifern wichtige Details zum physischen Host verweigert werden.

Werte

Standardwert der Installation: False

Vorgeschlagener Baseline-Wert: „Falsch“ oder „Nicht definiert“

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guestlib.enableHostInfo
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guestlib.enableHostInfo | Remove-
AdvancedSetting
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar. Dies ist eine VMX-Dateieinstellung.

Festlegen der Verschlüsselung für Fault Tolerance

Virtuelle Maschinen müssen für Fault Tolerance eine Verschlüsselung anfordern.

Die Anforderung einer Verschlüsselung für Fault Tolerance in virtuellen Maschinen gewährleistet eine sichere Datenübertragung. Während die standardmäßige „opportunistische“ Verschlüsselung wahrscheinlich aufgrund der allgegenwärtigen AES-NI-Unterstützung in vSphere-kompatibler Hardware zu einer Verschlüsselung führt, garantiert das Erzwingen der „erforderlichen“ Verschlüsselung keine unverschlüsselten Vorgänge.

Werte

Installationsstandardwert: ftEncryptionOpportunistic

Vorgeschlagener Baseline-Wert: ftEncryptionRequired

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
(Get-VM -Name $VM).ExtensionData.Config.FtEncryptionMode
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$VMview = Get-VM -Name $VM | Get-View
$ConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
$ConfigSpec.FtEncryptionMode = New-object
VMware.Vim.VirtualMachineConfigSpecEncryptedFtModes
$ConfigSpec.FtEncryptionMode = "ftEncryptionRequired"
$VMview.ReconfigVM_Task($ConfigSpec)
```

Festlegen des Standorts in vSphere Client

Virtuelle Maschine > Einstellungen bearbeiten > VM-Optionen > Verschlüsselung

isolation.tools.copy.disable

Deaktiviert Konsolenkopiervorgänge auf virtuellen Maschinen.

Durch das Deaktivieren von Konsolenkopiervorgängen auf virtuellen Maschinen wird das Kopieren von Daten zwischen der virtuellen Maschine und dem lokalen Client verhindert, unabhängig davon, ob der Benutzer über die Web-Konsole, VMRC oder eine andere Methode auf zugreift.

Werte

Standardwert der Installation: True.

Vorgeschlagener Baseline-Wert: „True“ oder „Nicht definiert“

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.copy.disable
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.copy.disable | Remove-
AdvancedSetting
```

isolation.tools.paste.disable

Deaktiviert Konsolen-Einfügevorgänge auf virtuellen Maschinen.

Durch Deaktivieren von Konsolen-Einfügevorgängen auf virtuellen Maschinen wird die Datenübertragung vom lokalen Client zur virtuellen Maschine blockiert, unabhängig davon, ob der Benutzer die Web-Konsole, VMRC oder eine andere Konsole verwendet.

Werte

Standardwert der Installation: True.

Vorgeschlagener Baseline-Wert: „True“ oder „Nicht definiert“

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.paste.disable
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.paste.disable | Remove-
AdvancedSetting
```

isolation.tools.diskShrink.disable

Deaktiviert das Verkleinern virtueller Festplatten auf virtuellen Maschinen.

Durch das Deaktivieren der Verkleinerung von virtuellen Festplatten auf virtuellen Maschinen werden Probleme in Bezug auf die Nichtverfügbarkeit von Festplatten vermieden. Benutzer ohne administrative Rechte können diesen Vorgang in der Gastumgebung in der Regel nur eingeschränkt durchführen.

Werte

Standardwert der Installation: True.

Vorgeschlagener Baseline-Wert: „True“ oder „Nicht definiert“

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.diskShrink.disable
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.diskShrink.disable | Remove-
AdvancedSetting
```

isolation.tools.diskWiper.disable

Deaktiviert Vorgänge zum Löschen virtueller Festplatten auf virtuellen Maschinen.

Durch das Deaktivieren des Löschens von virtuellen Festplatten auf virtuellen Maschinen werden Probleme in Bezug auf die Nichtverfügbarkeit von Festplatten vermieden. Benutzer ohne administrative Rechte können diesen Vorgang in der Gastumgebung in der Regel nur eingeschränkt durchführen.

Werte

Standardwert der Installation: True.

Vorgeschlagener Baseline-Wert: „True“ oder „Nicht definiert“

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.diskWiper.disable
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.diskWiper.disable | Remove-
AdvancedSetting
```

isolation.device.connectable.disable

Verhindert, dass virtuelle Maschinen unbefugt entfernt, verbunden und Geräte geändert werden.

Durch das Verhindern nicht autorisierter Geräteänderungen auf virtuellen Maschinen wird verhindert, dass nicht administrative Benutzer oder Prozesse Geräteeinstellungen verbinden, trennen oder anpassen können. Diese Maßnahme dämmt unbefugte Zugriffe und Betriebsunterbrechungen ein, reduziert Denial-of-Service-Risiken sowie einige Möglichkeiten zum Herausschleusen von Daten.

Werte

Standardwert der Installation: True.

Vorgeschlagener Baseline-Wert: „True“ oder „Nicht definiert“

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.device.connectable.disable
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.device.connectable.disable | Remove-
AdvancedSetting
```

isolation.tools.dnd.disable

Deaktiviert Drag-and-Drop-Vorgänge auf Konsolen für die virtuelle Maschine.

Durch das Deaktivieren von Drag-and-Drop-Vorgängen in der Konsole einer virtuellen Maschine wird verhindert, dass Benutzer Daten zwischen der virtuellen Maschine und dem lokalen Client übertragen, unabhängig vom Konsolentyp, was wiederum die Datensicherheit erhöht.

Werte

Standardwert der Installation: True.

Vorgeschlagener Baseline-Wert: „True“ oder „Nicht definiert“

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.dnd.disable
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.dnd.disable | Remove-AdvancedSetting
```

tools.setInfo.sizeLimit

Begrenzt die von der virtuellen Maschine auf die VMX-Datei übergebenen Informationsmeldungen.

Durch die Begrenzung der Informationsmeldungen der virtuellen Maschine auf die VMX-Datei wird verhindert, dass die Standardgröße von 1 MB überschritten wird. Diese Option verhindert potenzielle Denial-of-Service-Situationen, die auftreten können, wenn der Datenspeicher voll ist.

Werte

Installationsstandardwert: 1048576

Vorgeschlagener Baseline-Wert: 1048576 oder „Nicht definiert“

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting tools.setInfo.sizeLimit
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting tools.setInfo.sizeLimit | Remove-AdvancedSetting
```

Aktivieren der Protokollierung

Virtuelle Maschinen müssen die Diagnoseprotokollierung aktivieren.

Die Diagnoseprotokollierung für virtuelle Maschinen hilft bei der Diagnose und Fehlerbehebung.

Werte

Standardwert der Installation: True.

Empfohlener Baseline-Wert: True

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Where {$_.ExtensionData.Config.Flags.EnableLogging -ne "True"}
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$VMview = Get-VM -Name $VM | Get-View
$ConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
$ConfigSpec.Flags = New-Object VMware.Vim.VirtualMachineFlagInfo
$ConfigSpec.Flags.EnableLogging = $true
$VMview.ReconfigVM_Task($ConfigSpec)
```

log.keepOld

Begrenzt die Anzahl der aufbewahrten Diagnoseprotokolle der virtuellen Maschine.

Indem Sie die Anzahl der aufbewahrten Diagnoseprotokolle einschränken, vermeiden Sie, dass Datenspeicher gefüllt wird, ohne dass Sie dabei die Diagnosefunktionalität beeinträchtigen.

Werte

Installationsstandardwert: 10

Vorgeschlagener Baseline-Wert 10 oder „Nicht definiert“

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting log.keepOld
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting log.keepOld | Remove-AdvancedSetting
```

log.rotateSize

Begrenzt die Größe der Diagnoseprotokolle der virtuellen Maschine.

Durch die Begrenzung der Größe von Diagnoseprotokollen auf virtuellen Maschinen wird ein übermäßiger Speicherplatzverbrauch verhindert, insbesondere bei virtuellen Maschinen mit langer Ausführungsdauer. Der empfohlene Mindestgrenzwert beträgt 2 MB.

Werte

Installationsstandardwert: 2048000

Vorgeschlagener Baseline-Wert: 2048000 oder „Nicht definiert“

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting log.rotateSize
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting log.rotateSize | Remove-AdvancedSetting
```

tools.guestlib.enableHostInfo

Deaktiviert die Funktion zum Senden von Hostinformationen an Gäste.

Durch die Konfiguration einer virtuellen Maschine zum Abrufen detaillierter Informationen über den physischen Host könnte ein Angreifer diese Informationen möglicherweise verwenden, um weitere Angriffe auf dem Host durchzuführen. Da der Standardzustand der gewünschte Zustand ist, können Sie die Überwachung vornehmen, indem Sie überprüfen, ob diese Einstellung nicht oder auf „False“ festgelegt ist.

Werte

Standardwert der Installation: False

Vorgeschlagener Baseline-Wert: „Falsch“ oder „Nicht definiert“

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Wenn es innerhalb des Gastbetriebssystems nicht möglich ist, Leistungsinformationen über den Host abzurufen, kann die Fehlerbehebung erschwert werden.

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guestlib.enableHostInfo
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guestlib.enableHostInfo | Remove-
AdvancedSetting
```

tools.guest.desktop.autolock

Sperrt die Gastsitzung der virtuellen Maschine, wenn die Remote-Konsole getrennt wird.

Durch das Sperren virtueller Maschinen beim Schließen der letzten Konsolenverbindung kann ein potenzieller nicht autorisierter Zugriff durch Angreifer verhindert werden, die angemeldete Konsolensitzungen ausnutzen.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: True

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guest.desktop.autolock
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guest.desktop.autolock | Remove-
AdvancedSetting
```

Aktivieren der Verschlüsselung für vMotion

Virtuelle Maschinen müssen für vMotion eine Verschlüsselung anfordern.

Die Anforderung einer Verschlüsselung für vMotion auf virtuellen Maschinen gewährleistet eine sichere Datenübertragung. Die standardmäßige „opportunistische“ Verschlüsselung führt wahrscheinlich zu einer Verschlüsselung aufgrund der weit verbreiteten AES-NI-Unterstützung in vSphere-kompatibler Hardware. Durch das Erzwingen der „erforderlichen“ Verschlüsselung werden jedoch unverschlüsselte Vorgänge verhindert.

Werte

Installationsstandardwert: Opportunistisch

Vorgeschlagener Baseline-Wert: Erforderlich

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
(Get-VM -Name $VM).ExtensionData.Config.MigrateEncryption
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$VMview = Get-VM -Name $VM | Get-View
$ConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
$ConfigSpec.MigrateEncryption = New-Object
VMware.Vim.VirtualMachineConfigSpecEncryptedVMotionModes
$ConfigSpec.MigrateEncryption = "required"
$VMview.ReconfigVM_Task($ConfigSpec)
```

Sicherheitskontrollen des Gastbetriebssystems

Diese Sicherheitskontrollen bieten einen Baseline-Satz an Best Practices für Gastbetriebssysteme. Sie sind dahingehend gegliedert, dass die Vor- und Nachteile der Implementierung der Kontrolle verdeutlicht werden. Um Änderungen an diesen Steuerelementen vorzunehmen, verwenden Sie entweder die bereitgestellte PowerCLI oder den vSphere Client.

Verwendete Variable

Die in diesem Abschnitt vorgestellten PowerCLI-Befehle verwenden folgende Variable:

- $VM = "*virtual_machine_name*"

Pfad der VMware Tools

Der Standard-Installationspfad für VMware Tools lautet `C:\Program Files\VMware\VMware Tools`.

Secure Boot für das Gastbetriebssystem konfigurieren

Das Gastbetriebssystem muss Secure Boot aktivieren.

Secure Boot, das von allen modernen Gastbetriebssystemen unterstützt wird, nutzt Verschlüsselung mit öffentlichem Schlüssel, um Firmware, Bootloader, Treiber und Betriebssystemkernel zu validieren. Indem Secure Boot das Starten von Systemen mit unsicherer Bootkettengültigkeit verhindert, schränkt es Malware wirksam ein.

Werte

Standardwert der Installation: Standortspezifisch

Empfohlener Baseline-Wert: True

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Für die Aktivierung von Secure Boot nach der Installation eines Gastbetriebssystems sind möglicherweise weitere Schritte erforderlich. Eine Anleitung finden Sie in der Dokumentation Ihres Gastbetriebssystems.

PowerCLI-Befehlsbeurteilung

```
(Get-VM -Name $VM).ExtensionData.Config.BootOptions.EfiSecureBootEnabled
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
$VMobj = (Get-VM -Name $VM)
$ConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
$bootOptions = New-Object VMware.Vim.VirtualMachineBootOptions
$bootOptions.EfiSecureBootEnabled = $true
$ConfigSpec.BootOptions = $bootOptions
$task = $VMobj.ExtensionData.ReconfigVM_Task($ConfigSpec)
```

Festlegen des Standorts in vSphere Client

Virtuelle Maschine > Einstellungen bearbeiten > VM-Optionen

Einschränkung der Verwendung von MSI-Transformationen

Das Gastbetriebssystem muss die Verwendung von MSI-Transformationen bei der Neukonfiguration von VMware Tools einschränken.

MSI-Transformationen ermöglichen das Ändern der Installationsdatenbank auf Microsoft Windows-Gastbetriebssystemen. Dies kann hilfreich sein, bietet aber auch die Möglichkeit, aus vSphere das Sicherheitsprofil des Gastbetriebssystems zu ändern.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: False

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Administratoren müssen bei Bedarf andere Methoden nutzen, um VMware Tools zu aktualisieren und neu zu konfigurieren.

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get autoupgrade allow-msi-transforms
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set autoupgrade allow-msi-transforms false
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Deaktivieren von Appinfo

Das Gastbetriebssystem muss das Erfassen von Appinfo-Informationen deaktivieren, wenn dieses nicht erforderlich ist.

Appinfo ist eine Methode zur Anwendungserkennung über VMware Tools. Wenn Sie dieses Tool nicht verwenden, deaktivieren Sie das Modul, um die Angriffsfläche zu verringern.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: True

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Produkte und Dienste innerhalb des VMware-Ökosystems erfordern diese Funktionalität möglicherweise.

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get appinfo disabled
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set appinfo disabled true
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Deaktivieren von ContainerInfo

Das Gastbetriebssystem muss ContainerInfo deaktivieren, wenn dies nicht erforderlich ist.

Das VMware Tools ContainerInfo-Plug-In für Linux erfasst die Liste der in einem Linux-Gastbetriebssystem ausgeführten Container.

Werte

Standardwert der Installation: 21600

Empfohlener Baseline-Wert: 0

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Produkte und Dienste innerhalb des VMware-Ökosystems erfordern diese Funktionalität möglicherweise.

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get containerinfo poll-interval
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set containerinfo poll-interval 0
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Gastvorgänge deaktivieren

Deaktivieren Sie Gastvorgänge, sofern diese nicht erforderlich ist.

Bei Gastvorgängen handelt es sich um eine Reihe von Funktionen, die den meisten Host-zu-Gast-Interaktionen zugrunde liegen. Die Deaktivierung verringert die Angriffsfläche, wirkt sich aber auch erheblich auf die Funktionalität aus. Stellen Sie sicher, dass diese Funktionen in Ihrer Umgebung nicht benötigt werden. Deaktivieren Sie keine Gastvorgänge auf Vorlagen-VMs.

Eine Liste der Funktionen finden Sie in der folgenden Dokumentation:

https://vdc-download.vmware.com/vmwb-repository/dcr-public/fe08899f-1eec-4d8d-b3bc-a6664c168c2c/7fdf97a1-4c0d-4be0-9d43-2ceebbc174d9/doc/vim.vm.guest.GuestOperationsManager.html

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: True

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Produkte und Dienste innerhalb des VMware-Ökosystems erfordern diese Funktionalität möglicherweise.

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get guestoperations disabled
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set guestoperations disabled true
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Erneute Anpassung des Gastbetriebssystems verhindern

Sie müssen eine erneute Anpassung des Gastbetriebssystems auf bereitgestellten und angepassten virtuellen Maschinen verhindern.

Der Bereitstellungsprozess virtueller Maschinen bietet vSphere-Administratoren zahlreiche Möglichkeiten, virtuelle Maschinen mittels Skripts und dem Ausführen von Befehlen anzupassen. Diese Anpassungsansätze können einem Angreifer auch eine Möglichkeit bieten, durch das Klonen und die Neuanpassung Zugriff auf Daten innerhalb einer virtuellen Maschine zu erhalten. Verhindern Sie, dass eine virtuelle Maschine nach der Bereitstellung erneut angepasst werden kann. Diese Änderung können Sie jederzeit rückgängig machen.

Werte

Standardwert der Installation: True.

Empfohlener Baseline-Wert: False

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Virtuelle Maschinen können nach dem Einrichten beim Klonen angepasst werden. Nehmen Sie diese Änderung nicht an Vorlage-VMs vor.

Diese Änderung kann sich negativ auf Notfallwiederherstellungsprozesse auswirken, welche IP-Adressen über VMware Site Recovery Manager oder VMware Cloud Disaster Recovery ändern. Weitere Informationen finden Sie in der folgenden Dokumentation.

https://docs.vmware.com/de/VMware-Cloud-Disaster-Recovery/services/vmware-cloud-disaster-recovery/GUID-94202BE7-FEAF-4E35-8B55-15F6B3798309.html

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get deployPkg enable-customization
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set deployPkg enable-customization false
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Deaktivieren von GuestStore-Upgradevorgängen

Der Gastbetriebssystem muss GuestStore-Upgradevorgänge deaktivieren, sofern sie nicht benötigt werden.

Die GuestStore-Funktion bietet einen einfachen und flexiblen Mechanismus, um VMware-spezifische oder benutzerdefinierte Inhalte aus einem GuestStore-Repository gleichzeitig an mehrere Gäste zu verteilen. Sofern Sie diese Funktion nicht verwenden, deaktivieren Sie das Plug-In, um die Angriffsfläche zu verkleinern.

Werte

Standardwert der Installation: Manuell

Empfohlener Baseline-Wert: Aus

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Produkte und Dienste innerhalb des VMware-Ökosystems erfordern diese Funktionalität möglicherweise.

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get gueststoreupgrade policy
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set gueststoreupgrade policy off
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Deaktivieren der Diensterkennung

Das Gastbetriebssystem muss die Diensterkennung deaktivieren, sobald diese nicht benötigt wird.

Das VMware Tools-Plug-In für die Diensterkennung stellt eine Verbindung zu Aria Operations her und liefert dem Produkt zusätzliche Daten zu Gastbetriebssystemen und Arbeitslasten. Sofern Sie diese Funktion nicht verwenden, deaktivieren Sie das Plug-In, um die Angriffsfläche zu verkleinern.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: True

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Produkte und Dienste innerhalb des VMware-Ökosystems erfordern diese Funktionalität möglicherweise.

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get servicediscovery disabled
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set servicediscovery disabled true
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Aktivieren der Protokollierung für VMware Tools

Das Gastbetriebssystem muss die Protokollierung für VMware Tools aktivieren.

Stellen Sie sicher, dass VMware Tools Informationen korrekt protokolliert. Beispiele finden Sie unter https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf.

Werte

Standardwert der Installation: True.

Empfohlener Baseline-Wert: True

Aktion erforderlich

Überprüfen Sie die Installationsvorgabe.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get logging log
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set logging log true
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Senden von VMware Tools-Protokollen an den Systemprotokolldienst

Das Gastbetriebssystem muss VMware Tools-Protokolle an den Systemprotokolldienst senden.

Standardmäßig sendet VMware Tools Protokolle an eine Datei auf der Festplatte. Konfigurieren Sie Protokolle so, dass sie für die Verwaltung und zentrale Archivierung auf Linux-Gästen an Syslog und auf Microsoft Windows-Geräten an den Windows-Ereignisdienst gesendet werden.

Werte

Standardwert der Installation: Datei

Empfohlener Baseline-Wert: Syslog

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Aktualisieren Sie Prozesse, die darauf angewiesen sind, dass sich diese Dateien am Standardspeicherort befinden.

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get logging vmsvc.handler
VMwareToolboxCmd.exe config get logging toolboxcmd.handler
VMwareToolboxCmd.exe config get logging vgauthsvc.handler
VMwareToolboxCmd.exe config get logging vmtoolsd.handler
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set logging vmsvc.handler syslog
VMwareToolboxCmd.exe config set logging toolboxcmd.handler syslog
VMwareToolboxCmd.exe config set logging vgauthsvc.handler syslog
VMwareToolboxCmd.exe config set logging vmtoolsd.handler syslog
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Sicherstellen, dass die Version von VMware Tools auf dem neuesten Stand ist

Das Gastbetriebssystem muss sicherstellen, dass VMware Tools auf dem neuesten Stand ist.

VMware Tools sind ein wichtiger Teil des VMware-Ökosystems. Mit VMware Tools können Sie die Verwaltung von Gastbetriebssystemen durchführen, z. B.:

- Ordnungsgemäßes Herunterfahren
- Lebenszyklusverwaltung
- Abrufen von Treibern für paravirtualisierte Geräte
- Anpassen und Bereitstellen von VM-Vorlagen

Wie alle Softwareprodukte muss auch VMware Tools bei Bedarf verwaltet und aktualisiert werden. Stellen Sie sicher, dass Sie eine unterstützte Version für Ihr Gastbetriebssystem ausführen – unabhängig davon, ob sie als Teil der Linux-Distribution bereitgestellt oder durch Sie für Microsoft Windows installiert wurde.

Werte

Standardwert der Installation: Nicht verfügbar

Empfohlener Baseline-Wert: Nicht verfügbar

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine

PowerCLI-Befehlsbeurteilung

```
Get-VM -Name $VM | Select-Object -Property
Name,@{Name='ToolsVersion';Expression={$_.Guest.ToolsVersion}}
```

Beispiel für PowerCLI-Befehlsstandardisierung

Standortspezifisch. VMware Tools kann auf mehreren Wegen aktualisiert werden. Treiber für VMXNET3 und PVSCSI sind auch über Windows Update verfügbar. Stellen Sie daher sicher, dass Sie diese in Tools wie WSUS importieren.

Festlegen des Standorts in vSphere Client

Virtuelle Maschine > VM-Details > VMware Tools

Deaktivieren von GlobalConf

Das Gastbetriebssystem muss GlobalConf deaktivieren, sofern es nicht erforderlich ist.

Die Funktion „GlobalConf“ von VMware Tools bietet die Möglichkeit, Konfigurationen der `tools.conf`-Datei auf virtuelle Maschinen zu übertragen.

Werte

Standardwert der Installation: False

Empfohlener Baseline-Wert: False

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Bei Bedarf müssen Administratoren andere Methoden anwenden, um VMware Tools zu aktualisieren und neu zu konfigurieren.

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get globalconf enabled
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set globalconf enabled false
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Begrenzen der automatischen Verlängerung von VMware Tools-Funktionen

Das Gastbetriebssystem muss das automatische Entfernen von VMware Tools-Funktionen begrenzen.

Automatische Upgradeprozesse von VMware Tools können Funktionen zur VMware Tools-Installation hinzufügen oder daraus entfernen. Dies kann hilfreich sein, eröffnet aber auch die Möglichkeit, das Sicherheitsprofil des Gastbetriebssystems aus vSphere zu ändern.

Werte

Standardwert der Installation: True.

Empfohlener Baseline-Wert: False

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Bei Bedarf müssen Administratoren andere Methoden anwenden, um VMware Tools zu aktualisieren und neu zu konfigurieren.

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get autoupgrade allow-remove-feature
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set autoupgrade allow-remove-feature false
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Konfigurieren von VMware Tools für automatische Upgrades

Das Gastbetriebssystem muss VMware Tools-Upgrades automatisch für die Anforderungen der Umgebung konfigurieren.

VMware Tools-Updates können von vSphere initiiert werden, was für die Aufrechterhaltung aktueller VMware Tools-Versionen hilfreich sein kann. Deaktivieren Sie diese Funktion, wenn Sie VMware Tools auf andere Weise verwalten und aktualisieren. Lassen Sie automatische Updates grundsätzlich aktiviert.

Werte

Standardwert der Installation: True.

Empfohlener Baseline-Wert: True

Aktion erforderlich

Überprüfen Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Bei Bedarf müssen Administratoren andere Methoden anwenden, um VMware Tools zu aktualisieren und neu zu konfigurieren.

PowerCLI-Befehlsbeurteilung

```
VMwareToolboxCmd.exe config get autoupgrade allow-upgrade
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
VMwareToolboxCmd.exe config set autoupgrade allow-upgrade true
```

Festlegen des Standorts in vSphere Client

Nicht verfügbar

Überprüfen der Hardwareversion der virtuellen Maschine

Das Gastbetriebssystem muss sicherstellen, dass die Hardware der virtuellen Maschine Version 19 oder höher ist (sofern unterstützt).

Die virtuelle Maschine (Hardwareversion 19) ist kompatibel mit ESXi 7.0 Update 2 und höher. Neuere Versionen der Hardware virtueller Maschinen ermöglichen neue Funktionen und eine bessere Leistung. Erwägen Sie ein Upgrade auf VM-Hardware 20, sofern Sie ein vollständiges Update auf vSphere 8.0 oder höher durchgeführt haben. Gehen Sie beim Upgrade wie immer umsichtig vor und testen Sie den Upgrade-Prozess gründlich, bevor Sie ihn systemweit durchführen.

Berücksichtigen Sie alle Standorte, an denen eine virtuelle Maschine ausgeführt werden könnte oder an denen Sie die virtuelle Maschine möglicherweise wiederherstellen müssen. Beispielsweise müssen Benutzer des VMware Cloud Disaster Recovery-Dienstes die vSphere-Ebenen potenzieller Wiederherstellungs-SDDCs berücksichtigen. Obwohl VMware Cloud auf vSphere ausgeführt wird, sind möglicherweise nicht dieselben unterstützten virtuellen Hardwareversionen verfügbar.

Änderungen an der Konfiguration der von VMware bereitgestellten virtuellen Appliances werden nicht unterstützt und können zu Dienstunterbrechungen führen.

Hinweis Wenn Sie die Hardwareversion der virtuellen Maschine aktualisieren, werden auch Treiberaktualisierungen und weitere Updates durchgeführt. Die Auswirkungen sind in der Regel minimal.

Werte

Standardwert der Installation: Standortspezifisch

Empfohlener Baseline-Wert: vmx-19 oder höher

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Beim Ändern der Hardwareversionen virtueller Maschinen werden auch die Geräteversionen im Gast geändert, was sich negativ auswirken kann. Testen Sie Upgrades virtueller Hardwareversionen immer vorab und denken Sie daran, dass Snapshots auch die Version der virtuellen Maschine erfassen, weshalb Sie im Bedarfsfall Versionen wiederherstellen können.

Änderungen an der Konfiguration der von VMware bereitgestellten virtuellen Appliances werden nicht unterstützt und können zu Dienstunterbrechungen führen.

PowerCLI-Befehlsbeurteilung

```
(Get-VM -Name $VM | Get-View) | Select-Object -Property Name,@{Name='HW
Version';Expression={$_.Config.Version}}
```

Beispiel für PowerCLI-Befehlsstandardisierung

```
Set-VM -VM $VM -HardwareVersion vmx-19
```

Festlegen des Standorts in vSphere Client

Beim Erstellen einer virtuellen Maschine im Assistenten „Neue virtuelle Maschine“ legen Sie mit der Auswahl **Kompatibilität auswählen** die Hardwareversion der virtuellen Maschine fest.

Referenz der vSAN-Sicherheitskontrollen

Diese Sicherheitskontrollen stellen einen Baseline-Satz von Best Practices für vSAN bereit. Sie sind dahingehend gegliedert, dass die Vor- und Nachteile der Implementierung der Kontrolle verdeutlicht werden. Informationen zum Vornehmen von Änderungen an diesen Steuerungen finden Sie in der Dokumentation zu *Verwalten von VMware vSAN*.

Schützen von Daten im Ruhezustand

vSAN müssen Daten im Ruhezustand schützen.

Die vSAN-Verschlüsselung für Daten im Ruhezustand hilft dabei, die Vertraulichkeit sensibler Daten zu wahren, während sie sich auf Speichergeräten befinden, und verringert das Risiko eines unbefugten Zugriffs oder einer Offenlegung im Falle von physischem Diebstahl oder Verlust.

Sie können diesen Konfigurationsparameter ändern, während der Cluster betriebsbereit ist. Durch die Aktivierung des Schutzes für Daten im Ruhezustand werden Festplattengruppen (für vSAN OSA) neu formatiert und gespeicherte Objekte (für vSAN ESA) neu geschrieben. Dieser Hintergrundvorgang kann einige Zeit in Anspruch nehmen. Arbeitslasten müssen nicht

ausgeschaltet werden. In vSAN ESA 8.0 Update 2 wurde die Funktion eingeführt, den Schutz für Daten im Ruhezustand auf einem vorhandenen vSAN ESA-Datenspeicher zu aktivieren. In vSAN ESA 8.0 Update 3 ist es nun wieder möglich, die Funktion zu deaktivieren. Führen Sie die neueste Version von vSAN aus, wenn Sie ESA verwenden.

Werte

Installationsstandardwert: Deaktiviert

Vorgeschlagener Baseline-Wert: Aktiviert

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Die gesamte Verschlüsselung erfolgt auf Kosten von CPU-Zyklen und potenzieller Speicherlatenz. Wie stark sich dies auf Arbeitslasten auswirkt, hängt von einer Vielzahl von Faktoren ab, etwa der Konfiguration der zugrunde liegenden Hardware und dem Typ sowie der Häufigkeit der Speicher-E/A-Vorgänge durch die Arbeitslast.

Schützen von Daten beim Durchlaufen des Netzwerks

vSAN müssen Daten im Ruhezustand, einschließlich der speicherbezogenen Netzwerkkommunikation, schützen.

Die vSAN-Verschlüsselung in Übertragung begriffener Daten trägt dazu bei, dass sensible Daten beim Durchlaufen des Netzwerks vertraulich bleiben, wodurch das Risiko von unbefugtem Zugriff oder Abfangen reduziert wird.

Sie können diesen Konfigurationsparameter ändern, während der Cluster betriebsbereit ist.

Werte

Installationsstandardwert: Deaktiviert

Vorgeschlagener Baseline-Wert: Aktiviert

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Die gesamte Verschlüsselung erfolgt auf Kosten von CPU-Zyklen und potenzieller Speicherlatenz. Wie stark sich dies auf Arbeitslasten auswirkt, hängt von einer Vielzahl von Faktoren ab, etwa der Konfiguration der zugrunde liegenden Hardware und dem Typ sowie der Häufigkeit der Speicher-E/A-Vorgänge durch die Arbeitslast.

Einschränken des Zugriffs auf NFS-Dateifreigaben

NFS-Dateifreigaben in vSAN-Dateidiensten müssen so konfiguriert sein, dass der Zugriff eingeschränkt wird.

Wählen Sie beim Konfigurieren einer NFS-Dateifreigabe die Option zum Anpassen des Netzwerkzugriffs aus, und konfigurieren Sie einen restriktiven Satz von Berechtigungen.

Werte

Installationsstandardwert: Kein Zugriff

Vorgeschlagener Baseline-Wert: Netzwerkzugriff anpassen

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Verlust der Konnektivität mit Clients.

Verschlüsseln der KMU-Authentifizierung

KMU-Dateifreigaben in vSAN-Dateidiensten dürfen nur die verschlüsselte KMU-Authentifizierungskommunikation akzeptieren.

Aktivieren Sie beim Konfigurieren einer KMU-Dateifreigabe die Option für die Protokollverschlüsselung.

Werte

Installationsstandardwert: Deaktiviert

Empfohlener Baseline-Wert: Aktiviert

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Keine.

Aktivieren der bidirektionalen/gegenseitigen CHAP-Authentifizierung

Das vSAN iSCSI-Ziel muss die bidirektionale/gegenseitige CHAP-Authentifizierung aktivieren.

Gegenseitiges CHAP bietet eine zusätzliche Schutzebene, da sowohl der Initiator (Client) als auch das Ziel (Server) gegenseitig ihre Identität bestätigen müssen. Dies verhindert, dass zwischen den beiden Instanzen übertragene Daten durch nicht autorisierte Entitäten abgefangen oder geändert werden.

Werte

Installationsstandardwert: Deaktiviert

Empfohlener Baseline-Wert: Aktiviert

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Die Konfiguration von Clients kann schwieriger sein.

Reservieren von Speicherplatz zum Abschließen interner Wartungsvorgänge

vSAN muss Platz reservieren, um die internen Wartungsvorgänge abzuschließen.

Über die vSAN-Kapazitätseinstellung für die Vorgangsreserve wird sichergestellt, dass vSAN immer über ausreichend freien Speicherplatz verfügt, um die Verfügbarkeit und Zuverlässigkeit des vSAN-Datenspeichers aufrechtzuerhalten und potenzielle Datenverluste oder Dienstunterbrechungen aufgrund unzureichender Kapazität während Vorgängen wie Richtlinienänderungen zu verhindern.

Sie können diesen Konfigurationsparameter ändern, während der Cluster betriebsbereit ist.

Werte

Installationsstandardwert: Deaktiviert

Empfohlener Baseline-Wert: Aktiviert

Aktion erforderlich

Ändern Sie den Standardwert der Installation.

Mögliche funktionale Auswirkungen einer Änderung des Standardwerts

Durch die Aktivierung dieser Option wird die nutzbare Kapazität des vSAN-Datenspeichers reduziert.

Informationen zum National Institute of Standards and Technology

Das National Institute of Standards and Technology (Nationales Institut für Standards und Technologie, NIST) ist eine nicht regulatorische Regierungsbehörde, die Technologien, Metriken, Standards und Richtlinien entwickelt. Die Übereinstimmung mit NIST-Standards und -Richtlinien hat in vielen Branchen heute oberste Priorität.

Das National Institute of Standards and Technology (Nationale Institut für Standards und Technologie, NIST) wurde 1901 begründet und ist nun Teil des US-Handelsministeriums. Das NIST ist eines der ältesten naturwissenschaftlichen Laboratorien der Vereinigten Staaten. Heute werden NIST-Messungen für die Unterstützung von Technologien ganz unterschiedlicher Größenordnungen eingesetzt: von nanoskaligen Geräten bis hin zu erdbebensicheren Wolkenkratzern und globalen Kommunikationsnetzen.

Der Federal Information Security Management Act (FISMA) ist ein 2002 verabschiedetes Bundesgesetz der Vereinigten Staaten, das es den Bundesbehörden zur Auflage machte, ein Programm für Informationssicherheit und -schutz zu entwickeln, zu dokumentieren und umzusetzen. Das NIST spielt eine wichtige Rolle bei der FISMA-Implementierung, indem wichtige Sicherheitsstandards und -richtlinien (z. B. FIPS 199, FIPS-200 und SP-800-Serie) entwickelt werden.

Regierung und private Organisationen verwenden NIST 800-53, um Informationssysteme zu sichern. Cybersicherheits- und Datenschutzkontrollen sind unerlässlich, um Unternehmensabläufe (einschließlich Auftrag, Funktionen, Image und Reputation), Unternehmenswerte und Einzelpersonen vor einer Vielzahl von Bedrohungen zu schützen. Zu diesen Bedrohungen gehören feindliche Cyberangriffe, Naturkatastrophen, strukturelle Ausfälle und menschliche Fehler. VMware hat einen externen Prüfungspartner beauftragt, um VMware-Produkte und -Lösungen anhand des in NIST 800-53 aufgeführten Katalogs an Kontrollen zu bewerten. Weitere Informationen finden Sie auf der NIST-Webseite unter https://www.nist.gov/cyberframework.

Informationen zu DISA STIGs

Die Defense Information Systems Agency (DISA) erstellt und veröffentlicht Security Technical Implementation Guides (STIGs). DISA STIGs enthalten technische Anleitungen für das Absichern von Systemen und die Reduzierung von Bedrohungen.

Die Defense Information Systems Agency (DISA) ist die Kampfunterstützungsagentur des US-Verteidigungsministeriums (DoD), die für die Aufrechterhaltung des Sicherheitsstatus des DOD Information Network (DODIN) verantwortlich ist. DISA setzt unter anderem folgende Methode ein, um diese Aufgabe auszuführen: Entwicklung, Verbreitung und Beauftragung der Implementierung von Security Technical Implementation Guides (STIGs). Kurz gesagt: STIGs sind portierbare, standardbasierte Handbücher für Hardening-Systeme. STIGs sind für US-DoD-IT-Systeme obligatorisch und bieten somit eine geprüfte, sichere Grundlage für Nicht-DoD-Einheiten, anhand derer sie ihren Sicherheitsstatus messen können.

Auf der Grundlage von DISA-Protokollen und Feedback übermitteln Anbieter wie VMware Vorschläge für Security Hardening-Anleitungen zur Evaluierung an DISA. Sobald dieser Vorgang abgeschlossen ist, wird das offizielle STIG auf der Website der DISA-Organisation unter https://public.cyber.mil/stigs/ veröffentlicht. VMware enthält sicherheitsbasierte Baselines und Hardening-Anleitungen für vSphere im *vSphere Security Configuration Guide*. Weitere Informationen finden Sie unter https://core.vmware.com/security.

Über NERC CIP

Die North American Electric Reliability Corporation (NERC) ist eine gemeinnützige internationale Regulierungsbehörde mit der Aufgabe, die Zuverlässigkeit und Sicherheit des nordamerikanischen Massenstromsystems zu gewährleisten, einschließlich der USA, Kanadas und eines Teils von Baja California in Mexiko.

NERC entwickelt, setzt und überwacht Zuverlässigkeitsstandards und schult und zertifiziert Mitarbeiter aus der Industrie. Die CIP-Standards (Critical Infrastructure Protection), eine Schlüsselkomponente der Vorschriften von NERC, wurden entwickelt, um wichtige Cyber-Assets des elektrischen Massensystems zu sichern. Diese Standards schreiben spezifische Sicherheitsmanagementkontrollen, Systemsicherheitsmanagement, Informationsschutz und Schwachstellenbewertungen für Dienstprogramme und andere Einheiten innerhalb des Massenbetriebssystems vor.

Weitere Informationen finden Sie auf der NERC-CIP-Webseite unter https://core.vmware.com/nerc-cip.

Informationen zu VMware Security Development Lifecycle

Das VMware Security Development Lifecycle (SDL)-Programm identifiziert und mindert Sicherheitsrisiken während der Entwicklungsphase von VMware-Softwareprodukten. VMware betreibt auch das VMware Security Response Center (VSRC), um die Analyse und Behebung von Software-Sicherheitsproblemen in VMware-Produkten durchzuführen.

Unter SDL versteht man die Softwareentwicklungsmethodik, die die Gruppe „VMware Security Engineering, Communication, and Response“ (vSECR) sowie VMware-Produktentwicklungsgruppen einsetzen, um Sicherheitsprobleme zu identifizieren und zu minimieren. Weitere Informationen zum VMware Security Development Lifecycle erhalten Sie auf der Webseite unter https://www.vmware.com/security/sdl.html.

Das VSRC arbeitet mit Kunden und der Sicherheitsforschungs-Community zusammen, um folgende Ziele zu erreichen: Behandlung von Sicherheitsproblemen und rechtzeitige Bereitstellung umsetzbarer Sicherheitsinformationen für Kunden. Weitere Informationen zum VMware Security Response Center erhalten Sie auf der Webseite unter https://www.vmware.com/security/vsrc.html.

Überwachungsprotokollierung in vSphere

Die Überwachungsprotokollierung von Netzwerkdatenverkehr, Compliance-Warnungen, Firewall-Aktivitäten, Betriebssystemänderungen und Provisioning-Aktivitäten gilt als Best Practice für die Aufrechterhaltung der Sicherheit in jeder IT-Umgebung. Darüber hinaus ist die Protokollierung eine spezifische Anforderung im Rahmen vieler Bestimmungen und Standards.

Einer der ersten Schritte, um sicherzustellen, dass Sie sich der Änderungen an Ihrer Infrastruktur bewusst sind, ist die Überwachung Ihrer Umgebung. Standardmäßig umfasst vSphere Tools, mit denen Sie Änderungen anzeigen und verfolgen können. Beispielsweise können Sie über die Registerkarte „Aufgaben und Ereignisse“ im vSphere Client auf einem beliebigen Objekt in Ihrer vSphere-Hierarchie sehen, welche Änderungen vorgenommen wurden. Sie können PowerCLI auch verwenden, um Ereignisse und Aufgaben abzurufen. VMware Aria Operations for Logs bietet zudem Überwachungsprotokollierung zur Unterstützung der Erfassung und Aufbewahrung wichtiger Systemereignisse. Schließlich gibt es viele Tools von Drittanbietern, die vCenter Server-Überwachung anbieten.

Protokolldateien können auch dabei helfen festzustellen, wer oder was auf einen Host, eine virtuelle Maschine usw. zugreift. Weitere Informationen finden Sie unter Speicherorte der ESXi-Protokolldateien.

Single Sign-On-Audit-Ereignisse

Single Sign-On (SSO)-Überwachungsereignisse sind Aufzeichnungen von Benutzer- oder Systemaktionen für den Zugriff auf die SSO-Dienste.

In vCenter Server 6.7 Update 2 und höher wurde die VMware vCenter Single Sign-On-Überwachung verbessert, indem Ereignisse für die folgenden Vorgänge hinzugefügt wurden:

- Benutzerverwaltung
- Anmelden
- Gruppenerstellung
- Identitätsquelle
- Richtlinienaktualisierungen

Die unterstützten Identitätsquellen sind vsphere.local, integrierte Windows-Authentifizierung (IWA) und Active Directory über LDAP.

Wenn ein Benutzer sich bei vCenter Server über Single Sign-On anmeldet oder Änderungen vornimmt, die SSO betreffen, werden die folgenden Überwachungsereignisse in die SSO-Überwachungsprotokolldatei geschrieben:

- **Anmeldungs- und Abmeldungsversuche:** Ereignisse für alle erfolgreichen und fehlgeschlagenen Anmeldungs- und Abmeldungsvorgänge.
- **Berechtigungsänderung:** Ereignis für eine Änderung an einer Benutzerrolle oder Berechtigungen.
- **Kontoänderung:** Ereignis für die Änderung an den Benutzerkontoinformationen, z. B. Benutzername, Kennwort oder zusätzliche Kontoinformationen.
- **Sicherheitsänderung:** Ereignis für eine Änderung an einer Konfiguration, einem Parameter oder einer Richtlinie im Zusammenhang mit der Sicherheit.
- **Konto aktiviert oder deaktiviert:** Ereignis, wenn ein Konto aktiviert oder deaktiviert wird.
- **Identitätsquelle:** Ereignis für das Hinzufügen, Löschen oder Bearbeiten einer Identitätsquelle.

Im vSphere Client werden Ereignisdaten auf der Registerkarte **Überwachen** angezeigt. Informationen finden Sie in der Dokumentation *vSphere-Überwachung und -Leistung*.

SSO-Überwachungsereignisdaten enthalten die folgenden Details:

- Zeitpunkt, zu dem das Ereignis stattfand.
- Benutzer, der die Aktion durchgeführt hat.
- Beschreibung des Ereignisses.
- Schweregrad des Ereignisses.

- IP-Adresse des Clients, der für die Verbindung zum vCenter Server verwendet wurde, falls verfügbar.

Übersicht über das SSO-Überwachungsereignisprotokoll

Der vSphere Single Sign-On-Vorgang schreibt Überwachungsereignisse in die Datei `audit_events.log` im Verzeichnis `/var/log/audit/sso-events/`,

Vorsicht Bearbeiten Sie die Datei `audit_events.log` nie manuell, da damit die Überwachungsprotokollierung fehlschlagen könnte.

Beachten Sie Folgendes bei der Arbeit mit der Datei `audit_events.log`:

- Die Protokolldatei wird archiviert, sobald sie 50 MB erreicht.
- Es werden maximal 10 Archivdateien aufbewahrt. Wenn die maximale Anzahl erreicht ist, wird die älteste Datei entfernt, wenn ein neues Archiv erstellt wird.
- Die Archivdateien werden mit dem Namen `audit_events-<index>.log.gz` benannt, wobei „index“ eine Zahl zwischen 1 und 10 ist. Das erste erstellte Archiv ist „index 1“, und die Zahl wird mit jedem nachfolgenden Archiv erhöht.
- Die ältesten Ereignisse befinden sich im Archiv „index 1“. Die Datei mit der höchsten Indexnummer ist das neueste Archiv.

Grundlegendes zur Sicherheit und Übereinstimmung – nächste Schritte

Das Durchführen einer Sicherheitsbeurteilung ist der erste Schritt zum Verständnis von Schwachstellen in Ihrer Infrastruktur. Eine Sicherheitsbeurteilung ist Teil einer Sicherheitsüberwachung, bei dem sowohl Systeme als auch Praktiken geprüft werden, einschließlich der Sicherheitsübereinstimmung.

Eine Sicherheitsbeurteilung besteht im Allgemeinen aus einer Überprüfung der physischen Infrastruktur Ihres Unternehmens (Firewalls, Netzwerke, Hardware usw.), um Sicherheitsrisiken und Schwachstellen zu identifizieren. Eine Sicherheitsbeurteilung ist nicht das Gleiche wie eine Sicherheitsüberwachung. Eine Sicherheitsüberwachung umfasst nicht nur eine Überprüfung der physischen Infrastruktur, sondern auch die Prüfung anderer Bereiche wie Richtlinien und Standardverfahren, einschließlich der Sicherheitsübereinstimmung. Nach der Überwachung können Sie über die Schritte entscheiden, mit denen Sie die Probleme innerhalb des Systems beheben.

Stellen Sie sich bei der Vorbereitung einer Sicherheitsüberwachung die folgenden allgemeinen Fragen:

1. Ist für unsere Organisation die Einhaltung bestimmter Übereinstimmungsvorschriften vorgeschrieben? Wenn ja, welche?
2. Wie lang ist unser Überwachungsintervall?

3 Wie lang ist unser internes Selbsteinschätzungsintervall?

4 Haben wir Zugang zu früheren Überwachungsergebnissen, und haben wir diese geprüft?

5 Unterstützt uns eine externe Prüffirma bei der Vorbereitung der Überwachung? Falls ja, inwieweit ist diese Firma mit Virtualisierung vertraut?

6 Führen wir Schwachstellenscans für die Systeme und Anwendungen durch? Wann und wie oft?

7 Worin bestehen unsere internen Cybersicherheitsrichtlinien?

8 Ist Ihre Überwachungsprotokollierung entsprechend Ihren Bedürfnissen konfiguriert? Weitere Informationen hierzu finden Sie unter Überwachungsprotokollierung in vSphere.

Wenn keine spezifischen Hilfestellungen oder Leitlinien dazu vorliegen, wo Sie anfangen sollten, können Sie Ihre vSphere-Umgebung wie folgt direkt sichern:

- Halten Sie Ihre Umgebung mit den neuesten Software- und Firmware-Patches aktualisiert
- Pflegen Sie eine angemessene Kennwortverwaltung und Hygiene für alle Konten
- Gehen Sie die vom Anbieter genehmigten Sicherheitsempfehlungen durch
- Sehen Sie die VMware Security Configuration Guides ein (siehe Referenz zu vSphere-Sicherheitskontrollen)
- Nutzen Sie die überall bereitgestellten und bewährten Leitlinien von Richtlinienrahmen wie NIST, ISO usw.
- Folgen Sie den Leitlinien aus regulatorischen Übereinstimmungsrahmenwerken wie PCI, DISA und FedRAMP

vCenter Server und FIPS

In vSphere 7.0 Update 2 und höher können Sie FIPS-validierte Kryptografie für die vCenter Server Appliance aktivieren.

FIPS 140-2 ist ein US- und kanadischer Behördenstandard, der Sicherheitsanforderungen für kryptografische Module spezifiziert. vSphere verwendet FIPS-validierte kryptografische Module, die mit denen durch den FIPS 140-2-Standard angegebenen übereinstimmen. Mit einer vSphere FIPS-Unterstützung sollen Konformitäts- und Sicherheitsaktivitäten in verschiedenen regulierten Umgebungen erleichtert werden.

In vSphere 6.7 und höher verwenden ESXi und der vCenter Server FIPS-validierte Kryptografie, um Verwaltungsschnittstellen und die VMware Certificate Authority (VMCA) zu schützen.

vSphere 7.0 Update 2 und höhere Versionen enthalten zusätzliche validierte FIPS-Kryptographie für die vCenter Server Appliance.

Hinweis vSphere bevorzugt die Kompatibilität gegenüber FIPS, daher müssen einige Komponenten berücksichtigt werden. Weitere Informationen hierzu finden Sie unter Überlegungen bei der Verwendung von FIPS.

In ESXi verwendete FIPS-Module

Ein kryptografisches Modul ist ein Satz von Hardware, Software oder Firmware, die Sicherheitsfunktionen implementiert. ESXi verwendet mehrere FIPS 140-2-validierte kryptografische Module.

Die folgende Tabelle zeigt den Satz von FIPS 140-2-validierten kryptografischen Modulen, die von ESXi verwendet werden.

Tabelle 17-3. FIPS-Module

Kryptografisches Modul	Version	Algorithmen (CAVP)	Nummer des Zertifikats
Kryptografisches VMkernel-Modul	2,0	AES-CBC, AES-CBC-CS3, AES-CTR, AES-ECB, AES-GCM, AES-XTS Testing Revision 2.0, Counter DRBG, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512, SHA-1, SHA2-256, SHA2-512 (A2792)	Zertifikat läuft
OpenSSL-FIPS-Objektmodul	3.0	AES, CKG, CVL, DRBG, DSA, ECDSA, HMAC, KAS-RSA-SSC, KBKDF, KDA, KMAC, KTS, KTS-RSA, PBKDF, RSA, SHA-3, SHS, Triple-DES (A1938)	Zertifikat 4282
VMware OpenSSL FIPS Object Module	2.0.20-vmw	AES, CKG, /drbg, DSA, ECDSA, HMAC, KAS-SSC, RSA, SHS, Triple-DES (C470)	Zertifikat 3857
Kryptografisches ESXboot-Modul von VMware	1.0	HMAC-SHA2-224, RSA SigVer (FIPS186-4), SHA2-224, SHA2-256, SHA2-384, SHA2-512	Zertifikat 4442
boring Crypto Module von VMware	6.0	AES, CVL, DRBG, ECDSA, HMAC, KAS, KAS-SSC, KTS, RSA, SHS, Triple-DES (A4970)	Zertifikat #4694

Aktivieren und Deaktivieren von FIPS auf der vCenter Server Appliance

Sie können validierte FIPS-Kryptographie mithilfe von HTTP-Anforderungen auf der vCenter Server Appliance aktivieren oder deaktivieren. Validierte FIPS-Kryptographie ist standardmäßig deaktiviert.

Zur Ausführung von HTTP-Anforderungen stehen mehrere Möglichkeiten zur Verfügung. Diese Aufgabe zeigt die Verwendung des Developer Center im vSphere Client zum Aktivieren und Deaktivieren der validierten FIPS-Kryptographie auf der vCenter Server Appliance. Im *VMware vCenter Server Management-Programmierhandbuch* finden Sie weitere Informationen zur Verwendung von APIs zum Arbeiten mit der vCenter Server Appliance.

Verfahren

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

2 Wählen Sie im Menü die Option **Developer Center** aus.

3 Klicken Sie auf **API-Explorer**.

4 Wählen Sie im Dropdown-Menü **API auswählen** die Option **Appliance** aus.

5 Führen Sie einen Bildlauf nach unten durch die Kategorien durch und erweitern Sie **system/security/global_fips**.

6 Erweitern Sie **GET** und klicken Sie auf **Ausführen** unter **Ausprobieren**.

   Sie können die aktuelle Einstellung unter **Antwort** anzeigen.

7 Ändern Sie die Einstellung.

   a Zum Aktivieren von FIPS erweitern Sie **PUT**, geben Folgendes in `request_body` ein und klicken auf **Ausführen**.

   ```
   {
   "enabled":true
   }
   ```

   b Zum Deaktivieren von FIPS erweitern Sie **PUT**, geben Folgendes in `request_body` ein und klicken auf **Ausführen**.

   ```
   {
   "enabled":false
   }
   ```

Ergebnisse

Die vCenter Server Appliance wird neu gestartet, nachdem Sie die validierte FIPS-Kryptografie aktiviert oder deaktiviert haben.

Überlegungen bei der Verwendung von FIPS

Beim Aktivieren von FIPS auf der vCenter Server Appliance weisen bestimmte Komponenten derzeit funktionale Einschränkungen auf.

Nach der Aktivierung von FIPS auf dem vCenter Server sollten keine Unterschiede feststellbar sein. Es gibt jedoch einige Überlegungen, die zu berücksichtigen sind.

Tabelle 17-4. Überlegungen zu FIPS

Produkt oder Komponente	Überlegungen	Problemumgehung:
vSphere Single Sign-On	Wenn Sie FIPS aktivieren, unterstützt vCenter Server nur kryptografische Module für die Authentifizierung im Verbund. Folglich funktionieren RSA SecureID und bestimmte CAC-Karten nicht mehr.	Verwenden Sie Verbundauthentifizierung. Details finden Sie in der Dokumentation zur *vSphere-Authentifizierung*.
Nicht-VMware-Plug-Ins und Plug-Ins der vSphere Client-Partner-Benutzeroberfläche	Diese Plug-Ins funktionieren möglicherweise nicht mit aktiviertem FIPS.	Führen Sie ein Upgrade der Plug-Ins durch, um konforme Verschlüsselungsbibliotheken zu verwenden. Weitere Informationen finden Sie im Thema „Vorbereiten lokaler Plug-Ins für FIPS-Konformität“ in der Dokumentation zu *vSphere Client SDK*.
Zertifikate	Zertifikate mit Schlüsselgrößen größer als 3072 Bit wurden nicht getestet.	Generieren Sie Zertifikate mit Schlüsseln in den Größen 2048 oder 3072 Bit.