

# Seguridad de vSphere

Actualización 2

Modificado el 27 de abril de 2022

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

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

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware Spain, S.L.**  
Calle Rafael Boti 26  
2.ª planta  
Madrid 28023  
Tel.: +34 914125000  
[www.vmware.com/es](http://www.vmware.com/es)

Copyright © 2009-2022 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

# Contenido

Acerca de la seguridad de vSphere 13

Información actualizada 15

## 1 Seguridad en el entorno de vSphere 17

Proteger hipervisor de ESXi 17

Proteger los sistemas vCenter Server y los servicios asociados 19

Proteger máquinas virtuales 20

Proteger la capa de redes virtuales 21

Contraseñas en el entorno de vSphere 23

Recursos y prácticas recomendadas de seguridad 24

## 2 Autenticar vSphere con vCenter Single Sign-On 27

Descripción general de vCenter Single Sign-On 28

Cómo vCenter Single Sign-On protege el entorno 28

Componentes de vCenter Single Sign-On 31

Cómo influye vCenter Single Sign-On en la instalación 32

Cómo influye vCenter Single Sign-On en las actualizaciones 32

Usar vCenter Single Sign-On con vSphere 35

Grupos del dominio vsphere.local 37

Comportamiento de bloqueo y requisitos de contraseña de vCenter Server 39

Configurar orígenes de identidad de vCenter Single Sign-On 40

Orígenes de identidad para vCenter Server con vCenter Single Sign-On 41

Establecer el dominio predeterminado de vCenter Single Sign-On 43

Agregar un origen de identidad de vCenter Single Sign-On 43

Configurar orígenes de identidad de Active Directory 45

Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory 47

Editar un origen de identidad de vCenter Single Sign-On 48

Quitar un origen de identidad de vCenter Single Sign-On 49

Usar vCenter Single Sign-On con autenticación de sesión de Windows 49

Autenticación de dos factores con vCenter Server 50

Configuración de la autenticación de tarjeta inteligente para vCenter Single Sign-On 51

Usar la línea de comandos para configurar la autenticación de tarjeta inteligente 52

Usar la interfaz web de Platform Services Controller para administrar la autenticación de tarjeta inteligente 55

Configurar directivas de revocación para autenticación de tarjeta inteligente 59

Configurar la autenticación de RSA SecurID 61

Administrar el banner de inicio de sesión	63
Utilizar vCenter Single Sign-On como el proveedor de identidad para otro proveedor de servicios	64
Agregar un proveedor de servicios SAML	65
Servicio de token de seguridad (STS)	66
Generar un nuevo certificado de firma de STS en el dispositivo	67
Generar un nuevo certificado de firma de STS en una instalación de Windows de vCenter	68
Actualizar el certificado del servicio de token de seguridad	70
Determinar la fecha de caducidad de un certificado SSL de LDAPS	71
Administrar directivas de vCenter Single Sign-On	72
Editar la directiva de contraseñas de vCenter Single Sign-On	72
Editar la directiva de bloqueo de vCenter Single Sign-On	73
Editar la directiva de tokens de vCenter Single Sign-On	74
Administrar usuarios y grupos de vCenter Single Sign-On	75
Agregar usuarios de vCenter Single Sign-On	76
Deshabilitar y habilitar usuarios de vCenter Single Sign-On	77
Eliminar un usuario de vCenter Single Sign-On	78
Editar un usuario de vCenter Single Sign-On	78
Agregar un grupo de vCenter Single Sign-On	79
Agregar miembros a un grupo de vCenter Single Sign-On	80
Quitar miembros de un grupo de vCenter Single Sign-On	80
Eliminar usuarios de solución vCenter Single Sign-On	81
Cambiar la contraseña de vCenter Single Sign-On	82
Prácticas recomendadas de seguridad de vCenter Single Sign-On	83
Solucionar problemas en vCenter Single Sign-On	83
Determinar la causa de un error de Lookup Service	83
No se puede iniciar sesión con la autenticación del dominio de Active Directory	85
Se produce un error en el inicio de sesión en vCenter Server porque la cuenta de usuario está bloqueada	86
La replicación de VMware Directory Service puede tardar mucho	87

### 3 Certificados de seguridad de vSphere 88

Requisitos de certificados para distintas rutas de acceso de la solución	89
Descripción general de la administración de certificados	94
Descripción general del reemplazo de certificados	97
Casos en que vSphere 6.0 utiliza certificados	99
Servicios básicos de identidad de VMware y VMCA	102
Descripción general de VMware Endpoint Certificate Store	103
Administrar la revocación de certificados	105
Reemplazar certificados en implementaciones de gran tamaño	105
Administrar certificados con la interfaz web de Platform Services Controller	108

Explorar almacenes de certificados desde la interfaz web de Platform Services Controller	109
Reemplazar certificados por certificados firmados por VMCA desde la interfaz web de Platform Services Controller	110
Convertir una VMCA en una entidad de certificación intermedia desde la interfaz web de Platform Services Controller	111
Configurar el sistema para utilizar certificados personalizados desde Platform Services Controller	113
Generar solicitudes de firma de certificado con vSphere Certificate Manager (certificados personalizados)	114
Agregar un certificado raíz de confianza al almacén de certificados	115
Agregar certificados personalizados desde Platform Services Controller	116
Administrar certificados con la utilidad vSphere Certificate Manager	117
Revertir la última operación realizada volviendo a publicar certificados antiguos	119
Restablecer todos los certificados	119
Regenerar un certificado raíz de VMCA nuevo y reemplazo de todos los certificados	119
Convertir a VMCA en una entidad de certificación intermedia (Certificate Manager)	120
Generar una CSR con vSphere Certificate Manager y preparar certificados raíz (CA intermedia)	120
Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazo de todos los certificados	122
Reemplazar un certificado SSL de máquina por un certificado de VMCA (entidad de certificación intermedia)	124
Reemplazar certificados de usuario de solución por certificados de VMCA (entidad de certificación intermedia)	125
Reemplazar todos los certificados por certificados personalizados (Certificate Manager)	126
Generar solicitudes de firma de certificado con vSphere Certificate Manager (certificados personalizados)	126
Reemplazar un certificado SSL de máquina por un certificado personalizado	127
Reemplazar los certificados de usuarios de soluciones con certificados personalizados	128
Reemplazar certificados de forma manual	130
Descripción general de cómo iniciar y detener servicios	130
Reemplazar certificados firmados por VMCA existentes por certificados firmados por VMCA nuevos	131
Generar un nuevo certificado raíz firmado por VMCA	131
Reemplazar certificados SSL de máquina por certificados firmados por VMCA	134
Reemplazar los certificados de usuario de solución por certificados nuevos firmados por VMCA	137
Reemplazar el certificado de VMware Directory Service en entornos de modo mixto	144
Utilizar VMCA como entidad de certificación intermedia	145
Reemplazar el certificado raíz (entidad de certificación intermedia)	146
Reemplazar certificados SSL de máquina (entidad de certificación intermedia)	148
Reemplazar certificados de usuarios de solución (entidad de certificación intermedia)	152
Reemplazar certificado para VMware Directory Service	158

Reemplazar el certificado de VMware Directory Service en entornos de modo mixto	159
Usar certificados de terceros con vSphere	160
Solicitar certificados e importar un certificado raíz personalizado	161
Reemplazar certificados SSL de máquina por certificados personalizados	163
Reemplazar los certificados de usuarios de soluciones con certificados personalizados	165
Reemplazar certificado para VMware Directory Service	167
Reemplazar el certificado de VMware Directory Service en entornos de modo mixto	168
Administrar certificados y servicios con comandos de CLI	169
Privilegios necesarios para operaciones de administración de certificados	170
Cambiar la configuración de certtool	171
Referencia de comandos de inicialización de certtool	172
Referencia de comandos de administración certtool	175
Referencia de comandos vecs-cli	178
Referencia de comando dir-cli	182
Ver certificados de vCenter con vSphere Web Client	188
Establecer el umbral para las advertencias de caducidad de certificados de vCenter	188

## 4 Tareas de administración de permisos y usuarios de vSphere 190

Descripción de la autorización en vSphere	191
Descripción general del modelo de permisos de vCenter Server	192
Herencia jerárquica de permisos	194
Configuración de varios permisos	196
Ejemplo 1: herencia de varios permisos	197
Ejemplo 2: permisos secundarios que anulan permisos primarios	197
Ejemplo 3: función de usuario que anula la función de grupo	198
Administrar permisos para componentes de vCenter	199
Agregar un permiso a un objeto de inventario	200
Cambiar permisos	201
Quitar permisos	201
Cambiar la configuración de validación de permisos	201
Permisos globales	202
Agregar permisos globales	203
Permisos en objetos de etiqueta	204
Usar funciones para asignar privilegios	205
Funciones del sistema vCenter Server	207
Crear una función personalizada	208
Clonar una función	208
Editar una función	209
Prácticas recomendadas para funciones y permisos	209
Privilegios necesarios para la realización de tareas comunes	210

## 5 Proteger hosts ESXi 214

- Usar de scripts para administrar las opciones de configuración de hosts 215
- Configurar hosts ESXi con Host Profiles 216
- Recomendaciones generales sobre seguridad de ESXi 217
  - Bloqueo de cuenta y contraseñas ESXi 218
  - Recomendaciones de seguridad para redes de ESXi 221
  - Deshabilitar el explorador de objetos administrados (MOB) 221
  - Deshabilitar claves autorizadas (SSH) 222
- Administrar certificados para hosts ESXi 222
  - Certificados y actualizaciones de hosts 225
  - Configuración predeterminada de certificados de ESXi 225
  - Ver la información de caducidad de certificados de varios hosts ESXi 227
  - Ver los detalles de certificado para un host único de ESXi 228
  - Renovar o actualizar de certificados de ESXi 228
  - Cambiar configuración predeterminada de certificados 229
  - Descripción general de los cambios de modo de certificación 230
  - Cambiar el modo de certificado 232
  - Reemplazo de certificados y claves SSL de ESXi 233
    - Requisitos de las solicitudes de firma de certificados de ESXi 234
    - Reemplazar el certificado y de la clave predeterminados de ESXi Shell 234
    - Reemplazar la clave y el certificado predeterminados con el comando vifs 235
    - Reemplazar un certificado predeterminado mediante el método PUT de HTTPS 236
    - Actualizar el almacén TRUSTED\_ROOTS de vCenter Server (certificados personalizados) 237
  - Usar certificados personalizados con Auto Deploy 237
  - Restaurar archivos de certificados y claves de ESXi 239
- Personalizar hosts con el perfil de seguridad 240
  - Configurar firewalls de ESXi 240
    - Administrar la configuración del firewall de ESXi 241
    - Agregar direcciones IP permitidas para un host ESXi 242
    - Puertos de firewall entrantes y salientes para hosts de ESXi 243
    - Comportamiento de firewall del cliente NFS 246
    - Comandos de firewall ESXCLI de ESXi 247
  - Personalizar los servicios de ESXi desde el perfil de seguridad 248
  - Habilitar o deshabilitar un servicio en el perfil de seguridad 249
  - Modo de bloqueo 250
    - Comportamiento del modo de bloqueo 252
    - Habilitar el modo de bloqueo con vSphere Web Client 254
    - Deshabilitar el modo de bloqueo mediante vSphere Web Client 254
    - Habilitar o deshabilitar el modo normal de bloqueo desde la interfaz de usuario de la consola directa 255

Especificar cuentas con privilegios de acceso en el modo de bloqueo	256
Comprobar los niveles de aceptación de hosts y VIB	258
Asignar permisos para ESXi	259
Privilegios de usuario raíz	261
Privilegios del usuario vpxuser	261
Privilegios de usuario dcui	261
Usar Active Directory para administrar usuarios de ESXi	262
Instalar o actualizar vSphere Authentication Proxy	262
Configurar un host para utilizar Active Directory	263
Agregar un host a un dominio de servicio de directorio	265
Ver la configuración del servicio de directorio	265
Usar vSphere Authentication Proxy	266
Instalar o actualizar vSphere Authentication Proxy	266
Configurar un host para que utilice vSphere Authentication Proxy para autenticar	268
Configurar vSphere Authentication Proxy	269
Exportar certificados de vSphere Authentication Proxy	269
Importar un certificado de servidor proxy en ESXi	270
Usar vSphere Authentication Proxy para agregar un host a un dominio	271
Reemplazar el certificado del proxy de autenticación en el host ESXi	271
Prácticas recomendadas de seguridad de ESXi	272
Dispositivos PCI/PCIe y ESXi	273
Configurar la autenticación de tarjeta inteligente de ESXi	274
Habilitar la autenticación de tarjeta inteligente	274
Deshabilitar la autenticación de tarjeta inteligente	275
Autenticar credenciales de usuario durante problemas de conectividad	276
Usar la autenticación de tarjeta inteligente en el modo de bloqueo	276
Claves SSH de ESXi	276
Seguridad de SSH	277
Cargar una clave SSH mediante un comando vifs	277
Cargar una clave SSH mediante el método PUT de HTTPS	278
Usar ESXi Shell	279
Usar vSphere Web Client para habilitar el acceso a ESXi Shell	280
Crear un tiempo de espera para la disponibilidad de ESXi Shell en vSphere Web Client	281
Crear un tiempo de espera para sesiones de ESXi Shell inactivas en vSphere Web Client	281
Usar la interfaz de usuario de la consola directa (DCUI) para habilitar el acceso a ESXi Shell	282
Crear un valor de tiempo de espera de disponibilidad de ESXi Shell en la interfaz de usuario de la consola directa	282
Crear un tiempo de espera para sesiones de ESXi Shell inactivas	283
Iniciar sesión en ESXi Shell para solucionar problemas	284
Modificar la configuración del proxy web de ESXi	284



Consideraciones de seguridad de vSphere Auto Deploy 285

Administrar archivos de registro de ESXi 285

Configurar Syslog en hosts ESXi 286

Ubicaciones de archivos de registro de ESXi 287

Proteger tráfico de registro de Fault Tolerance 288

## 6 Proteger sistemas vCenter Server 289

Prácticas recomendadas de seguridad de vCenter Server 289

Prácticas recomendadas sobre el control de acceso a vCenter Server 289

Configurar la directiva de contraseñas de vCenter Server 291

Proteger el host de Windows para vCenter Server 292

Quitar certificados caducados o revocados, y registros de instalaciones con errores 292

Limitar la conectividad de red de vCenter Server 293

Restringir el uso de clientes Linux 293

Examinar los complementos instalados 294

Prácticas recomendadas de seguridad de vCenter Server Appliance 294

Comprobar huellas digitales para hosts ESXi heredados 295

Comprobar que la validación de certificados SSL mediante una copia de archivos de red está habilitada 296

Puertos TCP y UDP de vCenter Server 296

Controlar el acceso a la herramienta de supervisión de hardware basada en CIM 298

## 7 Proteger máquinas virtuales 300

Limitación de los mensajes informativos de máquinas virtuales a archivos VMX 300

Evitar la reducción de discos virtuales 301

Prácticas recomendadas de seguridad para las máquinas virtuales 302

Protección general de la máquina virtual 302

Usar plantillas para implementar máquinas virtuales 303

Minimizar el uso de la consola de máquina virtual 304

Evitar que las máquinas virtuales asuman el control de los recursos 304

Deshabilitar funciones innecesarias en máquinas virtuales 305

Quitar dispositivos de hardware innecesarios 305

Deshabilitar las características de visualización que no se utilizan 306

Deshabilitar características no expuestas 307

Deshabilitar transferencias de archivos por HGFS 308

Deshabilitar las operaciones para copiar y pegar entre el sistema operativo invitado y la consola remota 308

Limitar la exposición de los datos confidenciales copiados al portapapeles 309

Restringir la ejecución de comandos dentro de una máquina virtual a los usuarios 309

Evitar que un usuario o proceso de máquina virtual desconecten dispositivos 310

Modificar el límite de memoria variable del sistema operativo invitado 311

- Evitar que los procesos del sistema operativo invitado envíen mensajes de configuración al host 312
- Evitar utilizar discos independientes no persistentes 312

## 8 Proteger las redes de vSphere 314

- Introducción a la seguridad de red de vSphere 314
- Proteger la red con firewalls 316
  - Firewalls para configuraciones con vCenter Server 316
  - Conexión con vCenter Server mediante un firewall 317
  - Firewalls para configuraciones sin vCenter Server 318
  - Conectar hosts ESXi mediante firewalls 318
  - Conectar con la consola de la máquina virtual mediante un firewall 318
- Proteger el conmutador físico 319
- Proteger puertos de conmutadores estándar con directivas de seguridad 320
- Proteger conmutadores estándar de vSphere 321
  - Cambios de dirección MAC 322
  - Transmisiones falsificadas 322
  - Operación en modo promiscuo 323
- Proteger conmutadores distribuidos y grupos de puertos distribuidos de vSphere 323
- Proteger las máquinas virtuales con VLAN 324
  - Consideraciones de seguridad para VLAN 326
  - Proteger las VLAN 326
- Crear una DMZ de una red en un único host ESXi 327
- Crear varias redes en un único host ESXi 328
- Seguridad del protocolo de Internet 330
  - Lista de asociaciones de seguridad disponibles 331
  - Agregar una asociación de seguridad IPsec 331
  - Quitar una asociación de seguridad IPsec 332
  - Lista de directivas de seguridad IPsec disponibles 332
  - Crear una directiva de seguridad IPsec 333
  - Quitar una directiva de seguridad IPsec 334
- Garantizar la correcta configuración de SNMP 334
- Usar conmutadores virtuales con vSphere Network Appliance API solo cuando es necesario 335
- Prácticas recomendadas de seguridad de redes de vSphere 335
  - Recomendaciones generales sobre seguridad de redes 336
  - Etiquetar componentes de redes 337
  - Documentación y verificación del entorno VLAN de vSphere 338
  - Adoptar prácticas de aislamiento de red de sonido 339

## 9 Prácticas recomendadas relacionadas con varios componentes de vSphere 341

- Sincronizar los relojes en la red de vSphere 341
  - Sincronización de los relojes de ESXi con un servidor horario de red 342

Configurar la sincronización de hora en vCenter Server Appliance	342
Usar la sincronización de hora de VMware Tools	342
Agregar o reemplazar servidores NTP en la configuración de vCenter Server Appliance	343
Sincronizar la hora de vCenter Server Appliance con un servidor NTP	344
Prácticas recomendadas de seguridad de almacenamiento	345
Proteger almacenamiento iSCSI	345
Proteger dispositivos de iSCSI	345
Proteger una SAN iSCSI	346
Crear máscaras y dividir en zonas para recursos de SAN	347
Usar credenciales Kerberos para NFS 4.1	347
Comprobar que está deshabilitado el envío de datos de rendimiento del host a los invitados	348
Configurar tiempos de espera de ESXi Shell y vSphere Web Client	349
<b>10 Administrar la configuración del protocolo TLS con la utilidad de reconfiguración de TLS</b>	<b>350</b>
Puertos que permiten deshabilitar versiones de TLS	350
Deshabilitar las versiones de TLS en vSphere	352
Instalar la utilidad de configuración de TLS	353
Realizar una copia de seguridad manual opcional	354
Deshabilitar las versiones de TLS en los sistemas vCenter Server	356
Deshabilitar las versiones de TLS en los hosts ESXi	357
Deshabilitar las versiones de TLS en los sistemas Platform Services Controller	358
Revertir los cambios de configuración de TLS	360
Deshabilitar las versiones de TLS en vSphere Update Manager	362
Deshabilitar las versiones anteriores de TLS para Update Manager, puerto 9087	362
Deshabilitar las versiones anteriores de TLS para Update Manager, puerto 8084	363
Volver a habilitar las versiones de TLS deshabilitadas para el puerto 9087 de Update Manager	364
Volver a habilitar las versiones de TLS deshabilitadas para el puerto 8084 de Update Manager	365
<b>11 Privilegios definidos</b>	<b>367</b>
Privilegios de alarmas	368
Privilegios de Auto Deploy y perfiles de imagen	369
Privilegios de los certificados	371
Privilegios de la biblioteca de contenido	371
Privilegios de centro de datos	373
Privilegios de almacenes de datos	374
Privilegios de clústeres de almacenes de datos	375
Privilegios de Distributed Switch	375
Privilegios de ESX Agent Manager	376
Privilegios de extensiones	376

Privilegios de carpeta	377
Privilegios globales	377
Privilegios de CIM para hosts	379
Privilegios de configuración de hosts	379
Inventario del host	380
Privilegios de operaciones locales en hosts	381
Privilegios de vSphere Replication de host	382
Privilegios de perfiles de host	382
Privilegios de proveedor de Inventory Service	383
Privilegios de etiquetado de Inventory Service	383
Privilegios de red	384
Privilegios de rendimiento	384
Privilegios de permisos	385
Privilegios de almacenamiento basado en perfiles	385
Privilegios de recursos	386
Privilegios para tareas programadas	387
Privilegios de sesiones	387
Privilegios de vistas de almacenamiento	388
Privilegios de tareas	388
Privilegios del servicio de transferencia	389
Privilegios de directivas de VRM	389
Privilegios de configuración de máquinas virtuales	389
Privilegios de operaciones de invitado de máquina virtual	391
Privilegios para la interacción con máquinas virtuales	392
Privilegios de inventario de máquinas virtuales	403
Privilegios de aprovisionamiento de las máquinas virtuales	404
Privilegios de configuración de servicios de la máquina virtual	406
Privilegios de administración de snapshots de las máquinas virtuales	406
Privilegios de vSphere Replication de máquinas virtuales	407
Privilegios de grupo dvPort	407
Privilegios de vApp	408
Privilegios de vServices	410

# Acerca de la seguridad de vSphere

*Seguridad de vSphere* proporciona información sobre cómo proteger el entorno de vSphere® para VMware® vCenter® Server y VMware ESXi.

A modo de ayuda para proteger el entorno de vSphere, en esta documentación se describen las características de seguridad disponibles y las medidas que se pueden adoptar para proteger el entorno contra ataques.

A modo de ayuda para proteger el entorno de vSphere, en esta documentación se describen las características de seguridad disponibles y las medidas que se pueden adoptar para proteger el entorno contra ataques.

**Tabla 1-1. Información destacada de *Seguridad de vSphere***

Temas	Contenido destacado
Autenticación con vCenter Single Sign-On	<ul style="list-style-type: none"><li>■ Funcionalidad y servicios de vCenter Single Sign-On.</li><li>■ Agregar y administrar orígenes de identidad.</li><li>■ Directivas de vCenter Single Sign-On.</li><li>■ Usuarios y grupos.</li></ul>
Administración de usuarios y permisos	<ul style="list-style-type: none"><li>■ Modelo de permisos (funciones, grupos y objetos).</li><li>■ Crear funciones personalizadas.</li><li>■ Crear permisos.</li><li>■ Administrar permisos globales.</li></ul>
Administración de certificados	<ul style="list-style-type: none"><li>■ Administración de certificados de ESXi</li><li>■ Administración de certificados para vCenter Server y servicios relacionados.<ul style="list-style-type: none"><li>■ Administración de certificados mediante la interfaz de usuario.</li><li>■ Reemplazo de certificados mediante la utilidad Certificate Manager.</li><li>■ Usar la CLI para la administración manual de certificados (incluye ejemplos).</li></ul></li></ul>
Características de seguridad del host	<ul style="list-style-type: none"><li>■ Modo de bloqueo y otras funciones del perfil de seguridad</li><li>■ Autenticación de la tarjeta inteligente del host</li><li>■ vSphere Authentication Proxy</li></ul>

Tabla 1-1. Información destacada de *Seguridad de vSphere* (continuación)

Temas	Contenido destacado
Prácticas recomendadas y fortalecimiento de la seguridad	<p>Prácticas recomendadas y consejos de expertos en seguridad de VMware.</p> <ul style="list-style-type: none"> <li>■ Seguridad de vCenter Server.</li> <li>■ Seguridad de los hosts.</li> <li>■ Seguridad de las máquinas virtuales.</li> <li>■ Seguridad de las redes.</li> </ul>
Privilegios de vSphere	Lista completa de todos los privilegios de vSphere admitidos en esta versión.

## Documentación relacionada

Además de este documento, VMware publica una *Guía de fortalecimiento* para cada versión de vSphere, a la cual puede accederse desde <http://www.vmware.com/security/hardening-guides.html>. La *Guía de fortalecimiento* es una hoja de cálculo con entradas para distintos problemas de seguridad posibles. Incluye elementos para tres perfiles de riesgo distintos. Este *Seguridad de vSphere* documento no incluye información para el Perfil de riesgo 1 (que constituye el entorno de seguridad más alta, como asuntos secretos del gobierno).

## Audiencia prevista

Esta información está dirigida a administradores de sistemas Windows y Linux expertos que están familiarizados con la tecnología de máquina virtual y las operaciones de centro de datos.

# Información actualizada

Esta documentación sobre *Seguridad de vSphere* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de la documentación sobre *Seguridad de vSphere*.

Revisión	Descripción
27 de abril de 2022	■ Actualización menor a <a href="#">Privilegios de vistas de almacenamiento</a> .
05 de noviembre 2021	■ Actualización menor a <a href="#">Prácticas recomendadas de seguridad de ESXi</a> . ■ Se corrigió <a href="#">Deshabilitar las versiones de TLS en los hosts ESXi</a> para indicar que inicia sesión en la instancia de vCenter Server.
14 de agosto de 2020	En VMware, valoramos la inclusión. Para fomentar este principio entre nuestros clientes, nuestros partners y nuestra comunidad interna, estamos reemplazando parte de la terminología en nuestro contenido. Hemos actualizado esta guía para eliminar el lenguaje no inclusivo. ■ Actualización menor a <a href="#">Proteger máquinas virtuales</a> .
4 de octubre de 2017	■ En <a href="#">Descripción general de los cambios de modo de certificación</a> , se establece que, para hacer el cambio de modo, es aceptable poner los hosts en modo de mantenimiento y desconectarlos. No es necesario eliminar los hosts.
ES-001949-07	■ Se agregó un tema nuevo, <a href="#">Requisitos de certificados para distintas rutas de acceso de la solución</a> , que brinda detalles de requisitos de certificados. Se eliminó el tema anterior, que tenía menos detalles. ■ Se agregó el capítulo nuevo <a href="#">Capítulo 10 Administrar la configuración del protocolo TLS con la utilidad de reconfiguración de TLS</a> .
ES-001949-06	■ Se actualizó <a href="#">Usar la línea de comandos para configurar la autenticación de tarjeta inteligente</a> para indicar claramente que no se permiten espacios en las listas separadas por comas de certificados. ■ Se incorporó la ubicación del script en <a href="#">Usar la línea de comandos para configurar la autenticación de tarjeta inteligente</a> . ■ Se aclaró que es necesaria la cadena de certificados completa en <a href="#">Reemplazar los certificados de usuarios de soluciones con certificados personalizados</a> . ■ Se solucionó un problema en la introducción a <a href="#">Configuración de varios permisos</a> .
ES-001949-05	■ Se añadió información sobre la validación y el período de validación en <a href="#">Cambiar la configuración de validación de permisos</a> .
ES-001949-04	■ Se solucionó un error con el nombre de un parámetro en <a href="#">Comprobar que la validación de certificados SSL mediante una copia de archivos de red está habilitada</a> . ■ Se añadió información sobre la ubicación del comando <code>service-control</code> en Windows en <a href="#">Administrar certificados y servicios con comandos de CLI</a> .

Revisión	Descripción
ES-001949-03	<ul style="list-style-type: none"> <li>■ Se añadió información sobre los permisos de etiquetas en <a href="#">Permisos en objetos de etiqueta</a>.</li> <li>■ Se explicó mejor el orden de los certificados en <a href="#">Generar una CSR con vSphere Certificate Manager y preparar certificados raíz (CA intermedia)</a>.</li> </ul>
ES-001949-02	<ul style="list-style-type: none"> <li>■ Se agregó una nota sobre el inicio de sesión con vSphere Client en <a href="#">Capítulo 2 Autenticar vSphere con vCenter Single Sign-On</a>.</li> <li>■ Explicación en <a href="#">Configurar orígenes de identidad de Active Directory</a>. El sistema debe estar unido a un nombre de Active Directory y el nombre de dominio debe poder resolverse mediante DNS.</li> </ul>
ES-001949-01	<ul style="list-style-type: none"> <li>■ Se corrigió el orden de los certificados en <a href="#">Generar una CSR con vSphere Certificate Manager y preparar certificados raíz (CA intermedia)</a>.</li> <li>■ Se actualizó <a href="#">Bloqueo de cuenta y contraseñas ESXi</a>. Las frases de contraseña no están habilitadas de manera predeterminada.</li> <li>■ Se corrigieron los pasos para acceder al shell del dispositivo en <a href="#">Usar la línea de comandos para configurar la autenticación de tarjeta inteligente</a>.</li> <li>■ Solución para <a href="#">Cambiar la contraseña de vCenter Single Sign-On</a>. Si la contraseña caduca, debe ponerse en contacto con el administrador.</li> <li>■ Se actualizó el script de PowerCLI en <a href="#">Usar de scripts para administrar las opciones de configuración de hosts</a>.</li> <li>■ Se actualizó la información sobre la cantidad de instancias de vCenter Server en <a href="#">Cómo influye vCenter Single Sign-On en la instalación</a>.</li> <li>■ Varias actualizaciones en <a href="#">Usar la línea de comandos para configurar la autenticación de tarjeta inteligente</a>, <a href="#">Usar la interfaz web de Platform Services Controller para administrar la autenticación de tarjeta inteligente</a> y <a href="#">Configurar la autenticación de RSA SecurID</a>.</li> <li>■ Correcciones en <a href="#">Puertos TCP y UDP de vCenter Server</a>. Por ejemplo, el puerto 903 y el puerto 5900-5964 se utilizan en el host y no en el sistema de vCenter Server. Otros puertos, como 9090, solo se utilizan de forma interna.</li> <li>■ Se quitó la información sobre claves DSA de <a href="#">Cargar una clave SSH mediante un comando vifs</a>.</li> <li>■ Se actualizó <a href="#">Servicio de token de seguridad (STS)</a> para que incluya el procedimiento para generar un nuevo certificado de firma de STS.</li> </ul>
ES-001949-00	Versión inicial.



# Seguridad en el entorno de vSphere

# 1

Los componentes de un entorno de vSphere vienen protegidos desde el inicio mediante una variedad de características, como certificados, autorización, un firewall en cada instancia de ESXi, acceso limitado, etc. La configuración predeterminada se puede modificar de varias maneras. Por ejemplo, se pueden establecer permisos en los objetos de vCenter, abrir puertos de firewall o cambiar los certificados predeterminados. Esto permite contar con la máxima flexibilidad en la protección de sistemas vCenter Server, hosts ESXi y máquinas virtuales.

La descripción general detallada de las diferentes áreas de vSphere que requieren atención permite planificar la estrategia de seguridad. También se pueden aprovechar los recursos de seguridad adicionales de vSphere disponibles en el sitio web de VMware.

Este capítulo incluye los siguientes temas:

- [Proteger hipervisor de ESXi](#)
- [Proteger los sistemas vCenter Server y los servicios asociados](#)
- [Proteger máquinas virtuales](#)
- [Proteger la capa de redes virtuales](#)
- [Contraseñas en el entorno de vSphere](#)
- [Recursos y prácticas recomendadas de seguridad](#)

## Proteger hipervisor de ESXi

El hipervisor de ESXi ya viene protegido. Puede aumentar la protección de los hosts ESXi con el modo de bloqueo y otras características integradas. Si configura un host de referencia y hace cambios en todos los hosts basados en los perfiles de ese host, o si realiza una administración generada por script, proporciona una mayor protección para el entorno, ya que garantiza que los cambios se apliquen en todos los hosts.

Use las siguientes características, que se describen en detalle en esta guía, para mejorar la protección de los hosts ESXi que se administran con vCenter Server. También consulte el informe técnico *Seguridad de VMware vSphere Hypervisor*.

### Limitar el acceso a ESXi

De forma predeterminada, los servicios de ESXi Shell y SSH no se ejecutan, y solo el usuario raíz puede iniciar sesión en la interfaz de usuario de la consola directa (DCUI). Si decide habilitar el acceso a ESXi o SSH, puede establecer los tiempos de espera para reducir el riesgo de que se produzca un acceso no autorizado.

Los usuarios que pueden acceder al host ESXi deben tener permisos para administrar el host. Puede establecer permisos en el objeto de host de vCenter Server que administra el host.

### Utilización de usuarios designados y privilegio mínimo

De forma predeterminada, el usuario raíz puede realizar varias tareas. En lugar de permitir a los administradores iniciar sesión en el host ESXi con la cuenta de usuario raíz, se pueden aplicar diferentes privilegios de configuración de host en distintos usuarios designados desde la interfaz de administración de permisos de vCenter Server. Es posible crear funciones personalizadas, asignar privilegios a una función y asociar la función con un usuario designado y un objeto de host ESXi desde vSphere Web Client.

En los casos en los que haya un solo host, los usuarios se administran de forma directa. Consulte la documentación de *Administración de vSphere con vSphere Client*.

### Reducción de la cantidad de puertos de firewall de ESXi abiertos

De forma predeterminada, los puertos de firewall del host ESXi se abren solo cuando se inicia el servicio correspondiente. Se pueden utilizar los comandos de vSphere Web Client, ESXCLI o PowerCLI para comprobar y administrar el estado de los puertos de firewall.

Consulte [Configurar firewalls de ESXi](#).

### Automatización de la administración de hosts ESXi

Ya que generalmente es importante que diferentes hosts del mismo centro de datos estén sincronizados, utilice la instalación generada por script o vSphere Auto Deploy para aprovisionar los hosts. Los hosts se pueden administrar con los scripts. Una alternativa a la administración generada por script son los perfiles de host. Se debe configurar un host de referencia, exportar el perfil de host y aplicar el perfil de host al host. El perfil de host se puede aplicar directamente o como parte del aprovisionamiento con Auto Deploy.

Consulte [Usar de scripts para administrar las opciones de configuración de hosts](#) y lea *Instalación y configuración de vSphere* para obtener información sobre vSphere Auto Deploy.

### Aprovechamiento del modo de bloqueo

En el modo de bloqueo, solo se puede acceder a los hosts ESXi a través de vCenter Server de forma predeterminada. A partir de vSphere 6.0, se puede seleccionar el modo de bloqueo estricto o el modo de bloqueo normal, y definir los usuarios con excepción para permitir el acceso directo a las cuentas de servicio, como agentes de copias de seguridad.

Consulte [Modo de bloqueo](#).

### Comprobación de la integridad de los paquetes de VIB

Cada paquete de VIB tiene un nivel de aceptación asociado. Es posible agregar un VIB a un host ESXi solo si el nivel de aceptación es el mismo o mejor que el nivel de aceptación del host. No se puede agregar un VIB CommunitySupported o PartnerSupported a un host a menos que se cambie de forma explícita el nivel de aceptación del host.

Consulte [Comprobar los niveles de aceptación de hosts y VIB](#).

### Administrar certificados de ESXi

En vSphere 6.0 y versiones posteriores, VMware Certificate Authority (VMCA) aprovisiona cada host ESXi con un certificado firmado cuya entidad de certificación raíz de forma predeterminada es VMCA. Si la directiva de la empresa lo requiere, puede reemplazar los certificados existentes por certificados firmados por una CA externa.

Consulte [Administrar certificados para hosts ESXi](#).

### Autenticación de tarjeta inteligente

A partir de vSphere 6.0, ESXi admite la autenticación de tarjeta inteligente como una opción en lugar de la autenticación de nombre de usuario y contraseña.

Consulte [Configurar la autenticación de tarjeta inteligente de ESXi](#).

### Bloqueo de cuenta de ESXi

A partir de vSphere 6.0, se admite el bloqueo de cuentas para el acceso a través de SSH y vSphere Web Services SDK. La interfaz de la consola directa (DCUI) y ESXi Shell no admiten el bloqueo de cuentas. De forma predeterminada, se permite un máximo de diez intentos con errores antes de que la cuenta se bloquee. De forma predeterminada, la cuenta se desbloquea después de dos minutos.

Consulte [Bloqueo de cuenta y contraseñas ESXi](#).

Los parámetros de seguridad de los hosts individuales son similares, pero las tareas de administración pueden ser diferentes. Consulte la documentación de *Administración de vSphere con vSphere Client*.

## Proteger los sistemas vCenter Server y los servicios asociados

El sistema vCenter Server y los servicios asociados están protegidos por autenticación mediante vCenter Single Sign-On y por autorización mediante el modelo de permisos de vCenter Server. Es posible modificar el comportamiento predeterminado y seguir los pasos adicionales para proteger el acceso al entorno.

Cuando proteja el entorno de vSphere, tenga en cuenta que se deben proteger todos los servicios que están asociados con las instancias de vCenter Server. En ciertos entornos, se pueden proteger varias instancias de vCenter Server y una o más instancias de Platform Services Controller.

### Fortalecimiento de todos los equipos host de vCenter

El primer paso para proteger el entorno de vCenter es fortalecer cada equipo en el que se ejecutan vCenter Server o un servicio asociado. El enfoque es similar cuando se trata de una máquina física o una máquina virtual. Siempre instale las revisiones de seguridad más recientes para el sistema operativo y siga las prácticas recomendadas estándar de la industria para proteger el equipo host.

### Información sobre el modelo de certificado de vCenter

De forma predeterminada, VMware Certificate Authority aprovisiona cada host ESXi, cada máquina del entorno y cada usuario de solución con un certificado firmado por VMCA. El entorno se pone en funcionamiento desde el comienzo, pero si la empresa lo requiere, se puede cambiar el comportamiento predeterminado. Consulte [Capítulo 3 Certificados de seguridad de vSphere](#).

Para mejorar la protección, asegúrese de quitar explícitamente los certificados caducados o revocados y las instalaciones con errores.

### Configuración de vCenter Single Sign-On

vCenter Server y los servicios asociados están protegidos con el marco de autenticación de vCenter Single Sign-On. Al instalar el software por primera vez, se especifica una contraseña para el usuario administrator@vsphere.local, y solo ese dominio está disponible como origen de identidad. Es posible agregar otros orígenes de identidad, ya sea de Active Directory o LDAP, y establecer un origen de identidad predeterminado. Posteriormente, los usuarios que se pueden autenticar en un origen de identidad pueden ver objetos y realizar tareas si tienen la autorización para hacerlo. Consulte [Capítulo 2 Autenticar vSphere con vCenter Single Sign-On](#).

### Asignación de funciones a usuarios o grupos

Para mejorar el registro, asocie los permisos que otorga a un objeto con un usuario o grupo designado, y una función predefinida o personalizada. El modelo de permisos de vSphere 6.0 es muy flexible porque ofrece varios modos de autorizar usuarios o grupos. Consulte [Descripción de la autorización en vSphere](#) y [Privilegios necesarios para la realización de tareas comunes](#).

Asegúrese de restringir los privilegios de administrador y el uso de la función de administrador. De ser posible, no utilice el usuario administrador anónimo.

### Configurar NTP

Configure el NTP para cada nodo del entorno. La infraestructura de certificados requiere una marca de tiempo precisa y no funciona correctamente si los nodos no están sincronizados.

Consulte [Sincronizar los relojes en la red de vSphere](#).

## Proteger máquinas virtuales

Para proteger las máquinas virtuales, mantenga revisados los sistemas operativos invitados y proteja el entorno como si fuera una máquina física. Considere deshabilitar las funcionalidades

innecesarias, minimizar el uso de la consola de la máquina virtual y cumplir con las prácticas recomendadas.

### Proteger el sistema operativo invitado

Para proteger el sistema operativo invitado, asegúrese de utilizar las revisiones más recientes y, si corresponde, las aplicaciones antispyware y antimalware. Consulte la documentación del proveedor del sistema operativo invitado. También puede consultar otra información disponible en libros o en Internet para el sistema operativo.

### Deshabilitar funcionalidades innecesarias

Compruebe que las funcionalidades innecesarias estén deshabilitadas para minimizar los puntos de ataque potenciales. Muchas de las características que no se usan con frecuencia se deshabilitan de manera predeterminada. Extraiga el hardware innecesario y deshabilite ciertas características, como Host-Guest Filesystem (HFGS) o la función de copiar y pegar entre una máquina virtual y una consola remota.

Consulte [Deshabilitar funciones innecesarias en máquinas virtuales](#).

### Utilizar plantillas y la administración generada por script

Las plantillas de máquinas virtuales permiten configurar el sistema operativo de manera que se adapte a los requisitos y crear otras máquinas virtuales con la misma configuración.

Si desea cambiar la configuración de la máquina virtual después de la implementación inicial, considere el uso de scripts, por ejemplo, PowerCLI. En esta documentación, se explica cómo realizar tareas mediante la GUI. Considere usar scripts en lugar de la GUI para mantener la coherencia de su entorno. En los entornos de gran tamaño, puede agrupar las máquinas virtuales en carpetas para optimizar el proceso de scripting.

Para obtener información sobre plantillas, consulte [Usar plantillas para implementar máquinas virtuales](#) y *Administración de máquinas virtuales de vSphere*. Para obtener información sobre PowerCLI, consulte la documentación de VMware PowerCLI.

### Minimizar el uso de la consola de la máquina virtual

La consola de máquina virtual cumple la misma función en la máquina virtual que el monitor de un servidor físico. Los usuarios con acceso a una consola de máquina virtual tienen acceso a la administración de la alimentación de la máquina virtual y a los controles de conectividad del dispositivo. Como resultado, el acceso a la consola de máquina virtual podría permitir un ataque malicioso en una máquina virtual.

## Proteger la capa de redes virtuales

La capa de redes virtuales incluye adaptadores de red virtual, conmutadores virtuales, conmutadores virtuales distribuidos, y puertos y grupos de puertos. ESXi se basa en la capa de redes virtuales para establecer las comunicaciones entre las máquinas virtuales y sus usuarios. Asimismo, ESXi utiliza la capa de redes virtuales para comunicarse con las SAN iSCSI, el almacenamiento NAS, etc.

vSphere incluye la matriz completa de características necesarias para una infraestructura segura de redes. Puede proteger cada elemento de la infraestructura por separado, como los conmutadores virtuales, los conmutadores virtuales distribuidos, los adaptadores de red virtuales, etc. Por otra parte, considere las siguientes instrucciones, que se analizan más detalladamente en [Capítulo 8 Proteger las redes de vSphere](#).

### **Aislamiento del tráfico de red**

El aislamiento del tráfico de red es fundamental para proteger el entorno de ESXi. Las distintas redes requieren distintos niveles de aislamiento y acceso. La red de administración aísla los distintos tráficos (tráfico de clientes, de la interfaz de la línea de comandos (CLI) o de la API y del software de terceros) del tráfico normal. Esta red debe estar accesible únicamente para los administradores de sistemas, redes y seguridad.

Consulte [Recomendaciones de seguridad para redes de ESXi](#).

### **Utilización de firewalls para proteger los elementos de la red virtual**

Puede abrir y cerrar los puertos de firewall y proteger cada elemento de la red virtual por separado. Las reglas del firewall asocian los servicios con los firewalls correspondientes y pueden abrir y cerrar el firewall de ESXi de acuerdo con el estado del servicio.

Consulte [Configurar firewalls de ESXi](#).

### **Consideración de las directivas de seguridad de red**

La directiva de seguridad de redes ayuda a proteger el tráfico contra la suplantación de direcciones MAC y la exploración de puertos no deseada. La directiva de seguridad de un conmutador estándar o distribuido se implementa en la Capa 2 (capa de vínculo de datos) de la pila del protocolo de red. Los tres elementos de la directiva de seguridad son el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas.

Consulte la documentación de *Redes de vSphere* para ver las instrucciones.

### **Protección de las redes de las máquinas virtuales**

Los métodos que se utilizan para proteger la red de una máquina virtual dependen del sistema operativo invitado que está instalado, de si las máquinas virtuales funcionan en un entorno confiable y de varios otros factores. Los conmutadores virtuales y conmutadores virtuales distribuidos proporcionan un grado considerable de protección cuando se utilizan junto con otras prácticas de seguridad comunes, como la instalación de firewalls.

Consulte [Capítulo 8 Proteger las redes de vSphere](#).

### **Consideración de VLAN para proteger el entorno**

ESXi admite las VLAN IEEE 802.1q, que se pueden utilizar para proteger aún más la configuración de almacenamiento o de red de la máquina virtual. Las VLAN permiten segmentar una red física de modo que dos máquinas de la misma red física no puedan enviar o recibir paquetes entre ellas a menos que se encuentren en la misma VLAN.

Consulte [Proteger las máquinas virtuales con VLAN](#).

## Protección de las conexiones con el almacenamiento virtualizado

Una máquina virtual almacena archivos del sistema operativo, archivos de programas y otros datos en un disco virtual. Cada disco virtual figura en la máquina virtual como una unidad SCSI que está conectada a una controladora SCSI. La máquina virtual está aislada de los detalles de almacenamiento y no puede acceder a la información del LUN donde reside el disco virtual.

Virtual Machine File System (VMFS) es un sistema de archivos distribuidos y administrador de volumen que presenta volúmenes virtuales en el host ESXi. Usted es responsable de proteger la conexión con el almacenamiento. Por ejemplo, si se está utilizando el almacenamiento iSCSI, se puede configurar el entorno para que utilice CHAP y, si así lo establece la directiva de la empresa, para que utilice CHAP mutuo por medio de vSphere Web Client o de las CLI.

Consulte [Prácticas recomendadas de seguridad de almacenamiento](#).

## Evaluación de la utilización de IPsec

ESXi admite IPsec para IPv6. No se puede utilizar IPsec para IPv4.

Consulte [Seguridad del protocolo de Internet](#).

Asimismo, evalúe si VMware NSX for vSphere es una solución adecuada para proteger la capa de redes del entorno.

## Contraseñas en el entorno de vSphere

La restricción, el bloqueo y la caducidad de las contraseñas en el entorno de vSphere dependen de qué sistema el usuario utiliza como destino, quién es el usuario y cómo se establecen las directivas.

### Contraseñas de ESXi

Las restricciones de contraseñas de ESXi se determinan en el módulo PAM de Linux, pam\_passwdqc. Consulte [Bloqueo de cuenta y contraseñas ESXi](#).

### Contraseñas de vCenter Server y otros servicios de vCenter

vCenter Single Sign-On administra la autenticación de todos los usuarios que inician sesión en vCenter Server y en otros servicios de vCenter. La restricción, el bloqueo y la caducidad de las contraseñas dependen de cuál es el dominio del usuario y quién es el usuario.

#### **administrator@vsphere.local**

La contraseña para el usuario administrator@vsphere.local, o el usuario administrator@mydomain si se seleccionó un dominio distinto durante la instalación, no caduca y no está sujeta a la directiva de bloqueo. En los demás casos, la contraseña debe cumplir con las restricciones establecidas en la directiva de contraseñas de vCenter Single Sign-On. Consulte [Editar la directiva de contraseñas de vCenter Single Sign-On](#).

Si olvida la contraseña de estos usuarios, busque información en la base de conocimientos de VMware sobre la forma de restablecer esta contraseña.

### Otros usuarios de vsphere.local

Las contraseñas de otros usuarios de vsphere.local o de los usuarios del dominio local que se especificó durante la instalación, deben cumplir con las restricciones establecidas en la directiva de bloqueo y en la directiva de contraseñas de vCenter Single Sign-On. Consulte [Editar la directiva de contraseñas de vCenter Single Sign-On](#) y [Editar la directiva de bloqueo de vCenter Single Sign-On](#). Estas contraseñas caducan de manera predeterminada a los 90 días, pero los administradores pueden cambiar la fecha de caducidad como parte de la directiva de contraseñas.

Si un usuario olvida su contraseña de vsphere.local, un usuario administrador puede restablecerla mediante el comando `dir-cli`.

### Otros usuarios

La restricción, el bloqueo y la caducidad de las contraseñas de todos los demás usuarios se determinan según el dominio (el origen de identidad) en el cual el usuario puede autenticarse.

vCenter Single Sign-On admite un origen de identidad predeterminado, y los usuarios pueden iniciar sesión en vSphere Client solo con sus nombres de usuario. El dominio determina los parámetros de las contraseñas. Si los usuarios desean iniciar sesión como usuario en un dominio no predeterminado, pueden incluir el nombre del dominio, es decir, especificar *user@domain* o *domain\user*. Los parámetros de contraseña de los dominios también se aplican en este caso.

## Contraseñas de los usuarios de la interfaz de usuario de la consola directa de vCenter Server Appliance

vCenter Server Appliance es una máquina virtual preconfigurada basada en Linux, que se optimizó para ejecutar vCenter Server y los servicios asociados en Linux.

Durante la implementación de vCenter Server Appliance, se especifica una contraseña para el usuario raíz del sistema operativo Linux del dispositivo y una contraseña para el usuario `administrator@vsphere.local`. Es posible cambiar la contraseña del usuario raíz y realizar otras tareas de administración de usuarios locales de vCenter Server Appliance desde la interfaz de usuario de la consola directa. Consulte *Configuración de vCenter Server Appliance*.

## Recursos y prácticas recomendadas de seguridad

Si sigue las prácticas recomendadas, ESXi y vCenter Server pueden alcanzar el mismo nivel de seguridad, o incluso uno mayor, que un entorno donde no existe la virtualización.

En este manual se incluyen las prácticas recomendadas para los distintos componentes de la infraestructura de vSphere.



Tabla 1-1. Prácticas recomendadas de seguridad

Componente de vSphere	Recurso
Host ESXi	<a href="#">Prácticas recomendadas de seguridad de ESXi</a>
Sistema vCenter Server	<a href="#">Prácticas recomendadas de seguridad de vCenter Server</a>
Máquina virtual	<a href="#">Prácticas recomendadas de seguridad para las máquinas virtuales</a>
Redes de vSphere	<a href="#">Prácticas recomendadas de seguridad de redes de vSphere</a>

Este manual es tan solo una de las fuentes necesarias para garantizar un entorno seguro.

Los recursos de seguridad de VMware, incluidas alertas y descargas, se encuentran disponibles en la Web.

Tabla 1-2. Recursos de seguridad de VMware en la Web

Tema	Recurso
Directiva de seguridad de VMware, alertas de seguridad actualizadas, descargas de seguridad y foros de debate sobre temas de seguridad	<a href="http://www.vmware.com/go/security">http://www.vmware.com/go/security</a>
Directiva de respuestas sobre seguridad corporativa	<a href="http://www.vmware.com/support/policies/security_response.html">http://www.vmware.com/support/policies/security_response.html</a> VMware se compromete a ayudar en el mantenimiento de un entorno seguro. Los problemas de seguridad se solucionan oportunamente. La directiva de respuestas sobre seguridad de VMware define nuestro compromiso con la solución de posibles vulnerabilidades en nuestros productos.
Directiva de compatibilidad con software externo	<a href="http://www.vmware.com/support/policies/">http://www.vmware.com/support/policies/</a> VMware admite diversos sistemas de almacenamiento y agentes de software, como agentes de copia de seguridad, agentes de administración de sistemas, etc. Para consultar las listas de agentes, herramientas y demás opciones de software compatibles con ESXi, busque en <a href="http://www.vmware.com/vmtn/resources/">http://www.vmware.com/vmtn/resources/</a> las guías de compatibilidad de ESXi. La industria ofrece más productos y opciones de configuración de los que VMware puede probar. Si VMware no incluye un producto o una configuración en la guía de compatibilidad, el soporte técnico intentará ayudar a resolver los problemas, pero no podrá garantizar que se pueda usar el producto o la configuración. Siempre evalúe minuciosamente los riesgos para la seguridad que generan los productos o las opciones de configuración no compatibles.
Normas de seguridad y cumplimiento, soluciones de partners y contenido detallado sobre virtualización y cumplimiento	<a href="http://www.vmware.com/go/compliance">http://www.vmware.com/go/compliance</a>
Información sobre validaciones y certificados de seguridad como CCEVS y FIPS para diferentes versiones de los componentes de vSphere	<a href="https://www.vmware.com/support/support-resources/certifications.html">https://www.vmware.com/support/support-resources/certifications.html</a>

Tabla 1-2. Recursos de seguridad de VMware en la Web (continuación)

Tema	Recurso
Guías de fortalecimiento para diferentes versiones de vSphere y otros productos VMware	<a href="https://www.vmware.com/support/support-resources/hardening-guides.html">https://www.vmware.com/support/support-resources/hardening-guides.html</a>
Informe técnico <i>Seguridad de VMware vSphere Hypervisor</i>	<a href="http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf">http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf</a>

# Autenticar vSphere con vCenter Single Sign-On

## 2

vCenter Single Sign-On es un agente de autenticación y una infraestructura de intercambio de tokens de seguridad. Cuando un usuario o un usuario de solución pueden autenticarse en vCenter Single Sign-On, reciben el token SAML. Posteriormente, el usuario puede utilizar el token SAML para autenticarse en los servicios de vCenter. Posteriormente, el usuario puede realizar las acciones para las que tiene privilegios.

Ya que el tráfico está cifrado para todas las comunicaciones y solo los usuarios autenticados puede realizar las acciones para las que tienen privilegios, el entorno permanece seguro.

A partir de vSphere 6.0, vCenter Single Sign-On es parte de Platform Services Controller. Platform Services Controller contiene servicios compartidos que admiten componentes de vCenter Server y vCenter Server. Estos servicios incluyen vCenter Single Sign-On, VMware Certificate Authority, el servicio de licencias y Lookup Service. Consulte *Instalación y configuración de vSphere* para obtener detalles sobre Platform Services Controller.

En el protocolo de enlace inicial, los usuarios se autentican con un nombre de usuario y una contraseña, mientras que los usuarios de solución lo hacen con un certificado. Para obtener información sobre el reemplazo de certificados de usuario de solución, consulte [Capítulo 3 Certificados de seguridad de vSphere](#).

Una vez que un usuario puede autenticarse con vCenter Single Sign-On, se lo puede autorizar para que realice ciertas tareas. En la mayoría de los casos, se asignan privilegios de vCenter Server, pero vSphere incluye otros modelos de permisos. Consulte [Descripción de la autorización en vSphere](#).

---

**Nota** Si desea permitir que un usuario de Active Directory inicie sesión en una instancia de vCenter Server mediante vSphere Client con SSPI, debe unir la instancia de vCenter Server al dominio de Active Directory. Para obtener información sobre cómo unir un vCenter Server Appliance con un Platform Services Controller externo a un dominio de Active Directory, consulte el artículo de la base de conocimientos de VMware en <http://kb.vmware.com/kb/2118543>.

---

Este capítulo incluye los siguientes temas:

- [Descripción general de vCenter Single Sign-On](#)
- [Configurar orígenes de identidad de vCenter Single Sign-On](#)
- [Autenticación de dos factores con vCenter Server](#)

- Utilizar vCenter Single Sign-On como el proveedor de identidad para otro proveedor de servicios
- Servicio de token de seguridad (STS)
- Administrar directivas de vCenter Single Sign-On
- Administrar usuarios y grupos de vCenter Single Sign-On
- Prácticas recomendadas de seguridad de vCenter Single Sign-On
- Solucionar problemas en vCenter Single Sign-On

## Descripción general de vCenter Single Sign-On

Para administrar vCenter Single Sign-On de forma efectiva, debe comprender la arquitectura subyacente y cómo esta afecta la instalación y las actualizaciones.



Dominios y sitios de vCenter Single Sign-On 6.0

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

## Cómo vCenter Single Sign-On protege el entorno

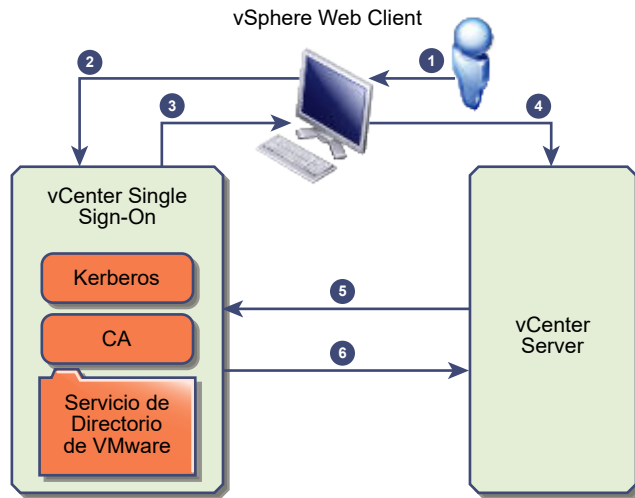
vCenter Single Sign-On permite que los componentes de vSphere se comuniquen entre ellos mediante un mecanismo de token seguro en lugar de solicitar a los usuarios que se autenticuen por separado en cada componente.

vCenter Single Sign-On usa una combinación de servicio de token de seguridad (STS), SSL para tráfico seguro, y autenticación de usuarios humanos mediante Active Directory u OpenLDAP y de usuarios de solución mediante certificados.

## Protocolo de enlace de vCenter Single Sign-On para usuarios humanos

En la siguiente ilustración se muestra el protocolo de enlace para usuarios humanos.

Figura 2-1. Protocolo de enlace de vCenter Single Sign-On para usuarios humanos



- 1 El usuario inicia sesión en vSphere Web Client con un nombre de usuario y una contraseña para acceder al sistema vCenter Server o a otro servicio de vCenter.

El usuario también puede iniciar sesión sin una contraseña y activar la casilla **Usar la autenticación de sesión de Windows**.

- 2 vSphere Web Client pasa la información de inicio de sesión al servicio vCenter Single Sign-On, que comprueba el token SAML de vSphere Web Client. Si vSphere Web Client tiene un token válido, vCenter Single Sign-On comprueba si el usuario se encuentra en el origen de identidad configurado (por ejemplo, Active Directory).
  - Si solo se emplea el nombre de usuario, vCenter Single Sign-On comprueba el dominio predeterminado.
  - Si se incluye un nombre de dominio con el nombre de usuario (*DOMAIN\user1* o *user1@DOMAIN*), vCenter Single Sign-On comprueba ese dominio.
- 3 Si el usuario puede autenticarse en el origen de identidad, vCenter Single Sign-On devuelve un token que representa al usuario en vSphere Web Client.
- 4 vSphere Web Client pasa el token al sistema vCenter Server.
- 5 vCenter Server comprueba con el servidor de vCenter Single Sign-On que el token sea válido y que no haya caducado.
- 6 El servidor de vCenter Single Sign-On devuelve el token al sistema vCenter Server, y así aprovecha el marco de autorización de vCenter Server para otorgar acceso a los usuarios.

Ahora el usuario puede autenticarse, y ver y modificar todos los objetos sobre los que tiene privilegios por su función.

---

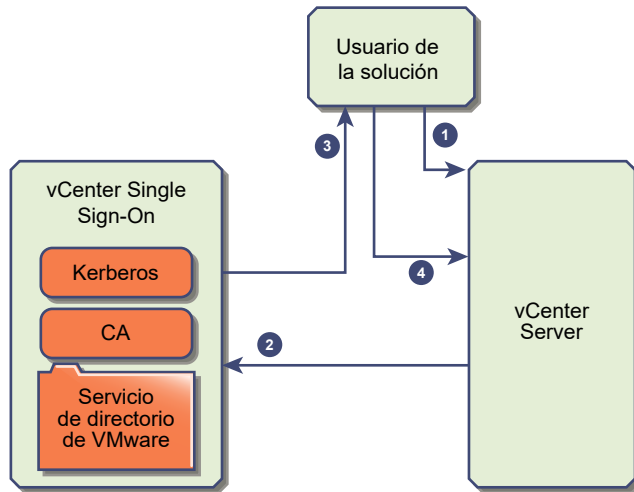
**Nota** Al principio, se asigna la función Sin acceso a cada usuario. Un administrador de vCenter Server debe asignar al menos la función Solo lectura al usuario para que pueda iniciar sesión. Consulte [Agregar un permiso a un objeto de inventario](#).

---

## Protocolo de enlace de vCenter Single Sign-On para usuarios de solución

Los usuarios de solución son conjuntos de servicios que se usan en la infraestructura de vCenter Server, por ejemplo, vCenter Server o las extensiones de vCenter Server. Las extensiones de VMware y las posibles extensiones externas también pueden autenticarse en vCenter Single Sign-On.

Figura 2-2. Protocolo de enlace de vCenter Single Sign-On para usuarios de solución



En el caso de los usuarios de solución, la interacción se produce de la siguiente manera:

- 1 El usuario de solución intenta conectarse a un servicio de vCenter.
- 2 Se redirige al usuario de solución a vCenter Single Sign-On. Si el usuario de solución es nuevo en vCenter Single Sign-On, debe presentar un certificado válido.
- 3 Si el certificado es válido, vCenter Single Sign-On asigna un token SAML (token de portador) al usuario de solución. vCenter Single Sign-On firma el token.
- 4 El usuario de solución se redirige a vCenter Single Sign-On y puede realizar tareas según sus permisos.
- 5 La próxima vez que el usuario de solución deba autenticarse, podrá usar el token SAML para iniciar sesión en vCenter Server.

De forma predeterminada, este protocolo de enlace se aplica automáticamente, ya que VMCA aprovisiona a los usuarios de solución con certificados durante el inicio. Si la directiva de la empresa exige certificados externos firmados por una entidad de certificación, se pueden utilizar esos certificados para reemplazar los certificados de los usuarios de solución. Si esos certificados son válidos, vCenter Single Sign-On asigna un token SAML al usuario de solución. Consulte [Usar certificados de terceros con vSphere](#).

## Componentes de vCenter Single Sign-On

vCenter Single Sign-On incluye el servicio de token de seguridad (STS), un servidor de administración y vCenter Lookup Service, además de VMware Directory Service (vmdir). VMware Directory Service también se usa para la administración de certificados.

Durante la instalación, los componentes se implementan como parte de una implementación integrada o como parte de Platform Services Controller.

### STS (servicio de token de seguridad)

El servicio STS emite tokens de lenguaje de marcado de aserción de seguridad (Security Assertion Markup Language, SAML). Estos tokens de seguridad representan la identidad de un usuario en uno de los tipos de orígenes de identidad compatibles con vCenter Single Sign-On. Los tokens de SAML permiten que los usuarios humanos y los usuarios de soluciones que se autentican correctamente en vCenter Single Sign-On utilicen cualquier servicio de vCenter que sea compatible con vCenter Single Sign-On sin tener que volver a autenticarse en cada servicio.

El servicio vCenter Single Sign-On firma todos los tokens con un certificado de firma y almacena el certificado de firma de tokens en el disco. El certificado del propio servicio también se almacena en el disco.

### Servidor de administración

El servidor de administración permite que los usuarios con privilegios de administrador para vCenter Single Sign-On configuren el servidor vCenter Single Sign-On y administren usuarios y grupos de vSphere Web Client. Inicialmente, solo el usuario `administrator@su_nombre_de_dominio` tenía estos privilegios. En vSphere 5.5 este usuario era `administrator@vsphere.local`. Con vSphere 6.0, puede cambiar el dominio de vSphere cuando instale vCenter Server o implemente vCenter Server Appliance con un nuevo Platform Services Controller. No asigne el nombre de dominio de Microsoft Active Directory u OpenLDAP a su nombre de dominio.

### VMware Directory Service (vmdir)

VMware Directory Service (vmdir) se asocia al dominio que especifique durante la instalación y se incluye en todas las implementaciones integradas y en cada Platform Services Controller. Se trata de un servicio de directorio multiempresa y de replicación de elementos del mismo nivel que pone a disposición un directorio LDAP en el puerto 389. El servicio aún utiliza el puerto 11711 para la compatibilidad con versiones anteriores de vSphere 5.5 y sistemas anteriores.

Si su entorno incluye más de una instancia de Platform Services Controller, se propaga una actualización del contenido de vmdir de una instancia de vmdir a todas las demás.

A partir de vSphere 6.0, VMware Directory Service no solo almacena información de vCenter Single Sign-On, sino también información sobre certificados.

### Servicio de administración de identidades

Controla los orígenes de identidad y las solicitudes de autenticación de STS.

## Cómo influye vCenter Single Sign-On en la instalación

A partir de la versión 5.1, vSphere incluye un servicio vCenter Single Sign-On como parte de la infraestructura de administración de vCenter Server. Este cambio afecta la instalación de vCenter Server.

La autenticación con vCenter Single Sign-On refuerza la seguridad de vSphere porque los componentes de software de vSphere se comunican entre sí a través de un mecanismo de intercambio de token seguro. Además, todos los otros usuarios también se autentican con vCenter Single Sign-On.

A partir de vSphere 6.0, vCenter Single Sign-On se incluye en una implementación integrada o como parte de Platform Services Controller. Platform Services Controller contiene todos los servicios necesarios para la comunicación entre los componentes de vSphere, incluidos vCenter Single Sign-On, VMware Certificate Authority, VMware Lookup Service y el servicio de licencias.

El orden de instalación es importante.

### Primera instalación

Si se trata de una instalación distribuida, debe instalar Platform Services Controller antes de instalar vCenter Server o implementar vCenter Server Appliance. Para una implementación integrada, el orden de instalación correcto se produce en forma automática.

### Instalaciones subsiguientes

Para hasta cuatro instancias de vCenter Server aproximadamente, una instancia de Platform Services Controller puede servir todo el entorno de vSphere. Puede conectar las nuevas instancias de vCenter Server a la misma instancia de Platform Services Controller. Para más de cuatro instancias de vCenter Server aproximadamente, puede instalar una instancia de Platform Services Controller adicional para obtener un mejor rendimiento. El servicio vCenter Single Sign-On de cada Platform Services Controller sincroniza los datos de autenticación con todas las demás instancias. El número exacto depende de cuánto se utilicen las instancias de vCenter Server y de otros factores.

## Cómo influye vCenter Single Sign-On en las actualizaciones

Si actualiza un entorno de instalación simple a una implementación integrada de vCenter Server 6, la actualización se hace sin problemas. Si actualiza una instalación personalizada, el servicio de vCenter Single Sign-On pasa a ser parte de Platform Services Controller después de la actualización. Determinar qué usuarios pueden iniciar sesión en vCenter Server después de una actualización depende de la versión desde la que se realizan la actualización y la configuración de implementación.

Como parte de la actualización, se puede definir un nombre de dominio de vCenter Single Sign-On diferente para utilizar en lugar de vsphere.local.



## Rutas de acceso de actualización

El resultado de la actualización depende de las opciones de instalación que se hayan seleccionado y el modelo de implementación al que se está actualizando.

**Tabla 2-1. Rutas de acceso de actualización**

Origen	Resultado
Instalación simple de vSphere 5.5 y versiones anteriores	vCenter Server con instancia de Platform Services Controller integrada.
Instalación personalizada de vSphere 5.5 y versiones anteriores	<p>Si vCenter Single Sign-On estaba en un nodo diferente que vCenter Server, se crea un entorno con una instancia de Platform Services Controller externa.</p> <p>Si vCenter Single Sign-On estaba en el mismo nodo que vCenter Server, pero los otros servicios están en diferentes nodos, se crea un entorno con una instancia de Platform Services Controller integrada.</p> <p>Si la instalación personalizada incluía varios servidores vCenter Single Sign-On de replicación, se crea un entorno con varias instancias de Platform Services Controller de replicación.</p>

## Usuarios que pueden iniciar sesión después de la actualización de una instalación simple

Si se actualiza un entorno que se aprovisionó con la opción de instalación simple, siempre se obtiene una instalación con una instancia de Platform Services Controller integrada. Determinar qué usuarios tienen autorización para iniciar sesión depende de si el entorno de origen incluye vCenter Single Sign-On.

**Tabla 2-2. Privilegios de inicio de sesión después de la actualización de un entorno de instalación simple**

Versión de origen	Acceso de inicio de sesión para	Notas
vSphere 5.0	Usuarios del sistema operativo local administrator@vsphere.local	Es posible que el sistema solicite el administrador de la carpeta raíz en la jerarquía de inventario de vSphere durante la instalación debido a cambios en los almacenes de usuarios. Si la instalación anterior admitía usuarios de Active Directory, se puede agregar el dominio de Active Directory como un origen de identidad.
vSphere 5.1	Usuarios del sistema operativo local administrator@vsphere.local Admin@SystemDomain	A partir de vSphere 5.5, vCenter Single Sign-On solo admite un origen de identidad predeterminado. Es posible establecer el origen de identidad predeterminado. Los usuarios de un dominio no predeterminado pueden especificar el dominio cuando inician sesión ( <i>DOMAIN\user</i> o <i>user@DOMAIN</i> ).
vSphere 5.5	administrator@vsphere.local o el administrador del dominio que se especificó durante la actualización.  Tal como antes, todos los usuarios de todos los orígenes de identidad pueden iniciar sesión.	

Si se hace una actualización desde vSphere 5.0, que no incluye vCenter Single Sign-On, hacia una versión que incluya vCenter Single Sign-On, los usuarios del sistema operativo local pasan a ser mucho menos importantes que los usuarios de un servicio de directorio como Active Directory. Como resultado, no siempre es posible o incluso recomendado mantener a los usuarios del sistema operativo local como usuarios autenticados.

### Usuarios que pueden iniciar sesión después de la actualización de una instalación personalizada

Si se actualiza un entorno que se aprovisionó con la opción de instalación personalizada, el resultado depende de las primeras elecciones:

- Si vCenter Single Sign-On estaba en el mismo nodo que el sistema vCenter Server, se hará una instalación con una instancia de Platform Services Controller integrada.
- Si vCenter Single Sign-On estaba en un nodo diferente que el sistema vCenter Server, se hará una instalación con una instancia de Platform Services Controller externa.

- Si se realiza una actualización desde vSphere 5.0, se puede seleccionar una instancia de Platform Services Controller externa o integrada como parte del proceso de actualización.

Los privilegios de inicio de sesión posteriores a la actualización dependen de varios factores.

**Tabla 2-3. Privilegios de inicio de sesión después de la actualización de un entorno de instalación personalizada**

Versión de origen	Acceso de inicio de sesión para	Notas
vSphere 5.0	<p>vCenter Single Sign-On reconoce a los usuarios del sistema operativo local de la máquina en la que se instaló Platform Services Controller, pero no de la máquina en la que se instaló vCenter Server.</p> <p><b>Nota</b> No se recomienda el uso de usuarios del sistema operativo local para la administración, especialmente en entornos federados.</p> <p>administrator@vsphere.local puede iniciar sesión en vCenter Single Sign-On y en cada instancia de vCenter Server como usuario administrador.</p>	<p>Si la instalación 5.0 admitía usuarios de Active Directory, estos ya no podrán obtener acceso después de la actualización. Es posible agregar el dominio de Active Directory como origen de identidad.</p>
vSphere 5.1 o vSphere 5.5	<p>vCenter Single Sign-On reconoce a los usuarios del sistema operativo local de la máquina en la que se instaló Platform Services Controller, pero no de la máquina en la que se instaló vCenter Server.</p> <p><b>Nota</b> No se recomienda el uso de usuarios del sistema operativo local para la administración, especialmente en entornos federados.</p> <p>administrator@vsphere.local puede iniciar sesión en vCenter Single Sign-On y en cada instancia de vCenter Server como usuario administrador.</p> <p>En las actualizaciones que se realizan desde vSphere 5.1, Admin@SystemDomain tiene los mismos privilegios que administrator@vsphere.local.</p>	<p>A partir de vSphere 5.5, vCenter Single Sign-On solo admite un origen de identidad predeterminado.</p> <p>Es posible establecer el origen de identidad predeterminado.</p> <p>Los usuarios de un dominio no predeterminado pueden especificar el dominio cuando inician sesión (<i>DOMAIN\user</i> o <i>user@DOMAIN</i>).</p>

## Usar vCenter Single Sign-On con vSphere

Cuando un usuario inicia sesión en un componente de vSphere, o cuando un usuario de solución de vCenter Server accede a otro servicio de vCenter Server, vCenter Single Sign-On lleva a cabo la autenticación. Los usuarios deben autenticarse con vCenter Single Sign-On y tener los privilegios necesarios para interactuar con objetos de vSphere.

vCenter Single Sign-On autentica a los usuarios de solución y a otros usuarios.

- Los usuarios de solución representan un conjunto de servicios en el entorno de vSphere. Durante la instalación, VMCA asigna un certificado a cada usuario de solución de forma predeterminada. El usuario de solución utiliza ese certificado para autenticarse en vCenter Single Sign-On. vCenter Single Sign-On otorga al usuario de solución un token SAML para que pueda interactuar con otros servicios del entorno.

- Cuando otros usuarios inician sesión en el entorno, por ejemplo, desde vSphere Web Client, vCenter Single Sign-On solicita un nombre de usuario y una contraseña. Si vCenter Single Sign-On encuentra un usuario con esas credenciales en el origen de identidad correspondiente, le asigna un token SAML. De esta forma, el usuario puede acceder a otros servicios del entorno sin tener que autenticarse de nuevo.

La configuración de permisos de vCenter Server determina qué objetos puede ver el usuario y qué tareas puede realizar. Los administradores de vCenter Server asignan esos permisos desde la interfaz **Administrar > Permisos** de vSphere Web Client, y no mediante vCenter Single Sign-On. Consulte [Capítulo 4 Tareas de administración de permisos y usuarios de vSphere](#).

## Usuarios de vCenter Single Sign-On y vCenter Server

Con vSphere Web Client, los usuarios se autentican en vCenter Single Sign-On introduciendo sus credenciales en la página de inicio de sesión de vSphere Web Client. Después de conectarse a vCenter Server, los usuarios autenticados pueden ver todas las instancias de vCenter Server u otros objetos de vSphere para los que su función les da privilegios. En esta instancia ya no se requiere autenticación adicional. Consulte [Capítulo 4 Tareas de administración de permisos y usuarios de vSphere](#).

Después de la instalación, el usuario de administrator@vsphere.local tiene acceso de administrador a vCenter Single Sign-On y vCenter Server. Ese usuario puede agregar orígenes de identidad, establecer el origen de identidad predeterminado y administrar usuarios y grupos en el dominio de vCenter Single Sign-On (vsphere.local).

Todos los usuarios que pueden autenticarse en vCenter Single Sign-On pueden restablecer su contraseña, incluso si esta ha caducado, siempre y cuando la sepan. Consulte [Cambiar la contraseña de vCenter Single Sign-On](#). Solo los administradores de vCenter Single Sign-On pueden restablecer la contraseña de los usuarios que ya no tienen su contraseña.

## Usuarios administradores de vCenter Single Sign-On

El acceso a la interfaz de administración de vCenter Single Sign-On se realiza desde vSphere Web Client.

Para configurar vCenter Single Sign-On y administrar usuarios y grupos de vCenter Single Sign-On, el usuario administrator@vsphere.local o un usuario del grupo de administradores de vCenter Single Sign-On deben iniciar sesión en vSphere Web Client. Después de la autenticación, el usuario puede acceder a la interfaz de administración de vCenter Single Sign-On desde vSphere Web Client y administrar orígenes de identidad y dominios predeterminados, especificar directivas de contraseñas y realizar otras tareas administrativas. Consulte [Configurar orígenes de identidad de vCenter Single Sign-On](#).

---

**Nota** No se puede cambiar el nombre del usuario administrator@vsphere.local. Para mejorar la seguridad, se recomienda que cree usuarios designados adicionales en el dominio vsphere.local y les asigne privilegios administrativos. A continuación, puede dejar de utilizar administrator@vsphere.local.

---

## Autenticar diferentes versiones de vSphere

Si un usuario se conecta a un sistema de vCenter Server versión 5.0.x o anterior, vCenter Server autentica al usuario mediante la validación del mismo en un dominio de Active Directory o la lista de usuarios del sistema operativo local. En vCenter Server 5.1 y versiones posteriores, los usuarios se autentican a través de vCenter Single Sign-On.

---

**Nota** No puede utilizar vSphere Web Client para administrar la versión 5.0 o anterior de vCenter Server. Actualice vCenter Server a la versión 5.1 o posterior.

---

## Usuarios de ESXi

ESXi no está integrado con vCenter Single Sign-On. Debe agregar el host ESXi a un dominio de Active Directory explícitamente. Consulte [Configurar un host para utilizar Active Directory](#).

Aún puede crear usuarios locales de ESXi con vSphere Client, vCLI o PowerCLI. vCenter Server no reconoce usuarios locales de ESXi y ESXi no reconoce usuarios de vCenter Server.

---

**Nota** De ser posible, administre los permisos de hosts ESXi mediante vCenter Server.

---

## Cómo iniciar sesión en componentes de vCenter Server

Cuando un usuario inicia sesión en un sistema con vCenter Server desde vSphere Web Client, el comportamiento de inicio de sesión depende de si el usuario se encuentra o no en el dominio predeterminado, es decir, el dominio configurado como el origen de identidad predeterminado.

- Los usuarios que están en el dominio predeterminado pueden iniciar sesión con su nombre de usuario y contraseña.
- Los usuarios que están en un dominio que se ha agregado a vCenter Single Sign-On como un origen de identidad pero que no es el dominio predeterminado, pueden iniciar sesión en vCenter Server pero deben especificar el dominio de una de las siguientes maneras.
  - Incluyendo un prefijo de nombre de dominio; por ejemplo, MIDOMINIO\usuario1
  - Incluyendo el dominio; por ejemplo, usuario1@midominio.com
- Los usuarios que se encuentran en un dominio que no es un origen de identidad de vCenter Single Sign-On no pueden iniciar sesión en vCenter Server. Si el dominio que va a agregar a vCenter Single Sign-On forma parte de una jerarquía de dominios, Active Directory determinará si los usuarios de otros dominios de la jerarquía se autentican o no.

---

**Nota** Si el entorno incluye una jerarquía de Active Directory, consulte el [artículo 2064250 de la base de conocimientos de VMware](#) para obtener detalles sobre las configuraciones compatibles y no compatibles.

---

## Grupos del dominio vsphere.local

El dominio vsphere.local incluye varios grupos predefinidos. Asigne usuarios a uno de esos grupos para poder llevar a cabo las acciones correspondientes.

Para todos los objetos de la jerarquía de vCenter Server, los permisos se asignan mediante el emparejamiento de un usuario y una función con el objeto. Por ejemplo, puede seleccionar un grupo de recursos y otorgar a un grupo de usuarios la función correspondiente para proporcionarle privilegios de lectura en ese grupo de recursos.

Para ciertos servicios que no se administran directamente con vCenter Server, los privilegios se determinan de acuerdo con la pertenencia a uno de los grupos de vCenter Single Sign-On. Por ejemplo, un usuario que es miembro del grupo Administrador puede administrar vCenter Single Sign-On. Un usuario miembro del grupo Administradores de CA puede administrar VMware Certificate Authority, y un usuario que está en el grupo Servicio de licencias.Administradores puede administrar licencias.

Los siguientes grupos están predefinidos en vsphere.local.

**Nota** Muchos de estos grupos son internos de vsphere.local u otorgan a los usuarios privilegios administrativos de alto nivel. Evalúe detenidamente los riesgos antes de agregar usuarios a cualquiera de estos grupos.

**Nota** No elimine ninguno de los grupos predefinidos en el dominio vsphere.local. De lo contrario, se pueden producir errores en la autenticación o el aprovisionamiento de certificados.

**Tabla 2-4. Grupos del dominio vsphere.local**

Privilegio	Descripción
Usuarios	Usuarios del dominio vsphere.local.
Usuarios de solución	Servicios de vCenter del grupo de usuarios de solución. Cada usuario de solución se autentica de forma individual en vCenter Single Sign-On con un certificado. De forma predeterminada, VMCA aprovisiona a los usuarios de solución con certificados. No agregue miembros a este grupo explícitamente.
Administradores de CA	Miembros del grupo Administradores de CA que tienen privilegios de administrador para VMCA. Generalmente, no se recomienda agregar miembros a estos grupos.
Administradores de DC	Los miembros del grupo Administradores de DC pueden llevar a cabo acciones de administrador de la controladora de dominio en VMware Directory Service.  <b>Nota</b> No administre la controladora de dominio directamente. En su lugar, utilice la CLI <code>vmdir</code> o vSphere Web Client para llevar a cabo las tareas correspondientes.
Configuración del sistema.Administradores de shell de Bash	Este grupo solo está disponible para implementaciones de vCenter Server Appliance.  Un usuario de este grupo puede habilitar y deshabilitar el acceso al shell de BASH. De forma predeterminada, un usuario que se conecta a vCenter Server Appliance con SSH tiene acceso solo a los comandos del shell restringido. Los usuarios que están en este grupo pueden acceder al shell de BASH.
Actuar como usuarios	Los miembros del grupo Actuar como usuarios tienen permisos de obtención de tokens Actuar como de vCenter Single Sign-On.
Usuarios de IPDU externos	Este grupo no se utiliza en vSphere. Este grupo se utiliza junto con VMware vCloud Air.

Tabla 2-4. Grupos del dominio vsphere.local (continuación)

Privilegio	Descripción
Configuración del sistema.Administradores	Los miembros del grupo Configuración del sistema.Administradores pueden ver y administrar la configuración del sistema en vSphere Web Client. Estos usuarios pueden ver, iniciar y reiniciar servicios, solucionar problemas de los servicios, y ver y administrar los nodos disponibles.
Cientes de DC	Este grupo se utiliza internamente para permitir al nodo de administración acceder a los datos de VMware Directory Service.  <b>Nota</b> No modifique este grupo. Cualquier cambio puede comprometer la infraestructura de certificados.
Administrador de componentes.Administradores	Los miembros del grupo Administrador de componentes.Administradores pueden ejecutar las API del administrador de componentes que registran servicios o cancelan registros de servicios, es decir, pueden modificar servicios. No es necesario ser miembro de este grupo para tener acceso de lectura en los servicios.
Servicio de licencias.Administradores	Los miembros de Servicio de licencias.Administradores tienen acceso total de escritura a todos los datos relacionados con la concesión de licencias, y pueden agregar, quitar y asignar claves de serie, así como anular estas asignaciones, para todos los activos de productos registrados en el servicio de concesión de licencias.
Administradores	Administradores de VMware Directory Service (vmdir). Los miembros de este grupo pueden realizar tareas de administración de vCenter Single Sign-On. Generalmente, no se recomienda agregar miembros a este grupo.

## Comportamiento de bloqueo y requisitos de contraseña de vCenter Server

Para administrar el entorno, debe conocer la directiva de contraseñas de vCenter Single Sign-On, las contraseñas de vCenter Server y el comportamiento de bloqueo.

### Contraseña para el administrador de vCenter Single Sign-On

La contraseña para administrator@vsphere.local debe cumplir con los siguientes requisitos:

- Tener al menos ocho caracteres
- Tener al menos un carácter en minúscula
- Tener al menos un carácter numérico
- Tener al menos un carácter especial

La contraseña para administrator@vsphere.local no puede superar los 20 caracteres. Solo se permiten caracteres ASCII visibles. Esto significa, por ejemplo, que no se puede utilizar el carácter de espacio.

## Contraseñas de vCenter Server

En vCenter Server, los requisitos de contraseña son dictados por vCenter Single Sign-On o el origen de identidad configurado, el cual puede ser Active Directory, OpenLDAP o el sistema operativo lógico del servidor vCenter Single Sign-On (no se recomienda).

## Comportamiento de bloqueo

Los usuarios quedan bloqueados después de una cantidad preestablecida de intentos consecutivos con errores. De forma predeterminada, los usuarios quedan bloqueados después de cinco intentos consecutivos fallidos en tres minutos, y una cuenta bloqueada se desbloquea automáticamente transcurridos cinco minutos. Puede cambiar estos valores predeterminados a través de la directiva de bloqueo. Consulte [Editar la directiva de bloqueo de vCenter Single Sign-On](#).

A partir de vSphere 6.0, la directiva de bloqueo no afecta al administrador del dominio del sistema (`administrator@vsphere.local` de forma predeterminada).

Los usuarios pueden cambiar su contraseña mediante el comando `dir-cli password change`. Si un usuario olvida su contraseña, el administrador puede restablecerla mediante el comando `dir-cli password reset`.

Consulte [Bloqueo de cuenta y contraseñas ESXi](#), donde se analizan las contraseñas de los usuarios locales de ESXi.

## Configurar orígenes de identidad de vCenter Single Sign-On

Cuando un usuario inicia sesión, vCenter Single Sign-On comprueba en el origen de identidad predeterminado si ese usuario puede autenticarse. Es posible agregar orígenes de identidad, quitar orígenes de identidad y cambiar el valor predeterminado.

vCenter Single Sign-On se configura desde vSphere Web Client. Para configurar vCenter Single Sign-On, se deben tener privilegios de administrador de vCenter Single Sign-On. Tener privilegios de administrador de vCenter Single Sign-On es diferente a tener función de administrador en vCenter Server o ESXi. De forma predeterminada, solo el usuario `administrator@vsphere.local` tiene privilegios de administrador en el servidor de vCenter Single Sign-On de una instalación nueva.

- [Orígenes de identidad para vCenter Server con vCenter Single Sign-On](#)

Puede utilizar orígenes de identidad para adjuntar uno o más dominios a vCenter Single Sign-On. Un dominio es un repositorio para usuarios y grupos que el servidor vCenter Single Sign-On puede utilizar para autenticación de usuarios.

- [Establecer el dominio predeterminado de vCenter Single Sign-On](#)

Cada origen de identidad de vCenter Single Sign-On está asociado a un dominio. vCenter Single Sign-On utiliza el dominio predeterminado para autenticar a un usuario que inicia sesión sin un nombre de dominio. Los usuarios que pertenecen a un dominio que no es el predeterminado deben incluir el nombre de dominio para iniciar sesión.



- **Agregar un origen de identidad de vCenter Single Sign-On**

Los usuarios solo pueden iniciar sesión en vCenter Server si están en un dominio que se agregó como un origen de identidad de vCenter Single Sign-On. Los usuarios administradores de vCenter Single Sign-On pueden agregar orígenes de identidad desde vSphere Web Client.

- **Editar un origen de identidad de vCenter Single Sign-On**

Los usuarios de vSphere se definen en un origen de identidad. Puede editar los detalles de un origen de identidad que está asociado con vCenter Single Sign-On.

- **Quitar un origen de identidad de vCenter Single Sign-On**

Los usuarios de vSphere se definen en un origen de identidad. Puede quitar un origen de identidad de la lista de orígenes de identidad registrados.

- **Usar vCenter Single Sign-On con autenticación de sesión de Windows**

Puede usar vCenter Single Sign-On con la autenticación de sesión de Windows (SSPI). Para que la casilla de la página de inicio de sesión esté disponible, debe tener instalado el complemento de integración de clientes.

## Orígenes de identidad para vCenter Server con vCenter Single Sign-On

Puede utilizar orígenes de identidad para adjuntar uno o más dominios a vCenter Single Sign-On. Un dominio es un repositorio para usuarios y grupos que el servidor vCenter Single Sign-On puede utilizar para autenticación de usuarios.

Un origen de identidad es una colección de datos de usuarios y grupos. Los datos de usuarios y grupos se almacenan en Active Directory, OpenLDAP o localmente en el sistema operativo del equipo en el que está instalado vCenter Single Sign-On.

Tras la instalación, todas las instancias de vCenter Single Sign-On tienen el origen de identidad *your\_domain\_name*; por ejemplo, vsphere.local. Este origen de identidad es interno de vCenter Single Sign-On. Los administradores de vCenter Single Sign-On pueden agregar orígenes de identidad, configurar el origen de identidad predeterminado y crear usuarios y grupos en el origen de identidad vsphere.local.

### Tipos de orígenes de identidad

Las versiones de vCenter Server anteriores a 5.1 eran compatibles con Active Directory y con usuarios del sistema operativo local como repositorios de usuarios. Por ello, los usuarios del sistema operativo local siempre podían autenticarse con el sistema de vCenter Server. Las versiones 5.1 y 5.5 de vCenter Server usan vCenter Single Sign-On para autenticación. Consulte

la documentación de vSphere 5.1 para obtener una lista de orígenes de identidad compatibles con vCenter Single Sign-On 5.1. vCenter Single Sign-On 5.5 admite los siguientes tipos de repositorios de usuarios como orígenes de identidad, pero solo admite un origen de identidad predeterminado.

- Versiones de Active Directory 2003 y posteriores. Se muestran como **Active Directory (autenticación integrada de Windows)** en vSphere Web Client. vCenter Single Sign-On permite especificar un único dominio de Active Directory como origen de identidad. El dominio puede tener dominios secundarios o ser un dominio raíz del bosque. El artículo de la base de conocimientos de VMware [2064250](#) trata sobre las confianzas de Microsoft Active Directory compatibles con vCenter Single Sign-On.
- Active Directory en LDAP. vCenter Single Sign-On admite varios orígenes de identidad de Active Directory en LDAP. Este tipo de origen de identidad se incluye para fines de compatibilidad con el servicio vCenter Single Sign-On incluido con vSphere 5.1. Se muestra como Active Directory **como un servidor LDAP** en vSphere Web Client.
- OpenLDAP versiones 2.4 y posteriores. vCenter Single Sign-On es compatible con varios orígenes de identidad de OpenLDAP. Se muestra como **OpenLDAP** en vSphere Web Client.
- Usuarios del sistema operativo local. Los usuarios del sistema operativo local son locales en el sistema operativo en que se ejecuta el servidor vCenter Single Sign-On. El origen de identidad del sistema operativo local solo existe en implementaciones del servidor vCenter Single Sign-On básicas y no está disponible en implementaciones con varias instancias de vCenter Single Sign-On. Solo se admite un origen de identidad del sistema operativo local. Se muestra como **locales** en vSphere Web Client.

---

**Nota** No utilice los usuarios del sistema operativo local si Platform Services Controller se encuentra en un equipo diferente al del sistema vCenter Server. El empleo de usuarios del sistema operativo local podría tener sentido en una implementación integrada, pero no se recomienda.

---

- Usuarios del sistema vCenter Single Sign-On. Se crea exactamente un origen de identidad del sistema denominado vsphere.local cuando se instala vCenter Single Sign-On. Se muestra como **vsphere.local** en vSphere Web Client.

---

**Nota** En todo momento, solo hay un único dominio predeterminado. Si un usuario de un dominio que no es el predeterminado inicia sesión, debe agregar el nombre de dominio (*DOMAIN\user*) para poder autenticarse correctamente.

---

Los usuarios administradores de vCenter Single Sign-On gestionan los orígenes de identidad de vCenter Single Sign-On.

Puede agregar orígenes de identidad a una instancia de servidor de vCenter Single Sign-On. Los orígenes de identidad remotos se limitan a las implementaciones de servidor de Active Directory y OpenLDAP.

## Establecer el dominio predeterminado de vCenter Single Sign-On

Cada origen de identidad de vCenter Single Sign-On está asociado a un dominio. vCenter Single Sign-On utiliza el dominio predeterminado para autenticar a un usuario que inicia sesión sin un nombre de dominio. Los usuarios que pertenecen a un dominio que no es el predeterminado deben incluir el nombre de dominio para iniciar sesión.

Cuando un usuario inicia sesión en un sistema con vCenter Server desde vSphere Web Client, el comportamiento de inicio de sesión depende de si el usuario se encuentra o no en el dominio predeterminado, es decir, el dominio configurado como el origen de identidad predeterminado.

- Los usuarios que están en el dominio predeterminado pueden iniciar sesión con su nombre de usuario y contraseña.
- Los usuarios que están en un dominio que se ha agregado a vCenter Single Sign-On como un origen de identidad pero que no es el dominio predeterminado, pueden iniciar sesión en vCenter Server pero deben especificar el dominio de una de las siguientes maneras.
  - Incluyendo un prefijo de nombre de dominio; por ejemplo, MIDOMINIO\usuario1
  - Incluyendo el dominio; por ejemplo, usuario1@midominio.com
- Los usuarios que se encuentran en un dominio que no es un origen de identidad de vCenter Single Sign-On no pueden iniciar sesión en vCenter Server. Si el dominio que va a agregar a vCenter Single Sign-On forma parte de una jerarquía de dominios, Active Directory determinará si los usuarios de otros dominios de la jerarquía se autentican o no.

### Procedimiento

- 1 Inicie sesión en vSphere Web Client como administrator@vsphere.local u otro usuario con privilegios de administrador de vCenter Single Sign-On.

Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio vsphere.local.

- 2 Desplácese hasta **Administración > Single Sign-On > Configuración**.
- 3 En la pestaña **Orígenes de identidad**, seleccione un origen de identidad y haga clic en el icono **Establecer como dominio predeterminado**.

En la pantalla del dominio, el dominio predeterminado muestra la opción (predeterminado) en la columna Dominio.

## Agregar un origen de identidad de vCenter Single Sign-On

Los usuarios solo pueden iniciar sesión en vCenter Server si están en un dominio que se agregó como un origen de identidad de vCenter Single Sign-On. Los usuarios administradores de vCenter Single Sign-On pueden agregar orígenes de identidad desde vSphere Web Client.

Un origen de identidad puede ser un dominio de Active Directory nativo (autenticación integrada de Windows) o un servicio de directorio de OpenLDAP. Por razones de compatibilidad con versiones anteriores, Active Directory también está disponible como servidor LDAP. Consulte [Orígenes de identidad para vCenter Server con vCenter Single Sign-On](#)

Inmediatamente después de la instalación, quedan disponibles los siguientes orígenes de identidad y usuarios predeterminados:

### localos

Todos los usuarios locales del sistema operativo. Si realiza una actualización, los usuarios que ya pueden autenticarse continúan pudiendo hacerlo. El uso del origen de identidad localos no funciona en los entornos que utilizan un sistema Platform Services Controller.

### vsphere.local

Contiene los usuarios internos de vCenter Single Sign-On.

### Requisitos previos

El dominio que desea agregar como origen de identidad debe estar disponible en el equipo donde vCenter Single Sign-On se está ejecutando. Si está utilizando vCenter Server Appliance, consulte la documentación de *Configuración de vCenter Server Appliance*.

### Procedimiento

- 1 Inicie sesión en vSphere Web Client como administrator@vsphere.local u otro usuario con privilegios de administrador de vCenter Single Sign-On.

Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio vsphere.local.

- 2 Desplácese hasta **Administración > Single Sign-On > Configuración**.
- 3 En la pestaña **Orígenes de identidad**, haga clic en el icono **Agregar origen de identidad**.
- 4 Seleccione el tipo de origen de identidad y especifique la configuración de origen de identidad.

Opción	Descripción
<b>Active Directory (autenticación integrada de Windows)</b>	Utilice esta opción para las implementaciones nativas de Active Directory. Si desea utilizar esta opción, la máquina en la que se ejecuta el servicio vCenter Single Sign-On debe estar en un dominio de Active Directory. Consulte <a href="#">Configurar orígenes de identidad de Active Directory</a> .
<b>Active Directory como servidor LDAP</b>	Esta opción está disponible para brindar compatibilidad con versiones anteriores. Requiere que especifique la controladora de dominio y otra información. Consulte <a href="#">Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory</a> .

Opción	Descripción
OpenLDAP	Utilice esta opción para un origen de identidad OpenLDAP. Consulte <a href="#">Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory</a> .
LocalOS	Utilice esta opción para agregar el sistema operativo local como origen de identidad. Se solicita únicamente el nombre del sistema operativo local. Si selecciona esta opción, todos los usuarios de la máquina especificada quedan visibles para vCenter Single Sign-On, incluso si estos no forman parte de otro dominio.

**Nota** Si se bloquea o se deshabilita la cuenta, las autenticaciones y las búsquedas de grupos y de usuarios en el dominio Active Directory no funcionan. La cuenta del usuario debe tener acceso de solo lectura a la unidad organizativa del usuario y del grupo, y debe poder leer los atributos del usuario y del grupo. Esta es la configuración predeterminada del dominio de Active Directory para los permisos de autenticación. VMware recomienda utilizar un usuario de servicio especial.

- 5 Si configuró Active Directory como un servidor LDAP o un origen de identidad de OpenLDAP, haga clic en **Conexión de prueba** para garantizar que puede conectarse al origen de identidad.
- 6 Haga clic en **Aceptar**.

#### Pasos siguientes

Cuando se agrega un origen de identidad, todos los usuarios pueden autenticarse, pero tienen la función **Sin acceso**. Un usuario con privilegios vCenter Server **Modificar permisos** puede otorgar a usuarios o grupos de usuarios privilegios que los habiliten a iniciar sesión en vCenter Server, y ver y administrar objetos. Consulte la documentación de *Seguridad de vSphere*.

## Configurar orígenes de identidad de Active Directory

Si selecciona el tipo de origen de identidad de **Active Directory (autenticación de Windows integrada)**, puede usar la cuenta de equipo local como un nombre de entidad de seguridad de servicio (Service Principal Name, SPN) o especificar un SPN explícitamente. Puede usar esta opción únicamente si el servidor vCenter Single Sign-On está asociado a un dominio de Active Directory.

#### Requisitos previos para usar un origen de identidad de Active Directory

Puede configurar vCenter Single Sign-On para que use un origen de identidad de Active Directory solo si ese origen de identidad está disponible.

- Para una instalación de Windows, únase al equipo Windows en el dominio de Active Directory.

- Para vCenter Server Appliance, siga las instrucciones en la documentación de *Configuración de vCenter Server Appliance*.

**Nota** Active Directory (autenticación integrada de Windows) usa siempre la raíz del bosque de dominios de Active Directory. Para configurar un origen de identidad para Autenticación de Windows integrada con un dominio secundario dentro del bosque de Active Directory, consulte el artículo [2070433](#) de la base de conocimientos de VMware.

Seleccione **Usar cuenta de equipo** para acelerar la configuración. Si desea cambiar el nombre del equipo local en el que se ejecuta vCenter Single Sign-On, es preferible que especifique un SPN explícitamente.

**Nota** En vSphere 5.5, vCenter Single Sign-On usa la cuenta del equipo aunque se especifique el SPN. Consulte el artículo [2087978](#) de la base de conocimientos de VMware.

Tabla 2-5. Agregar opciones de orígenes de identidad

Cuadro de texto	Descripción
Nombre de dominio	FQDN del nombre de dominio (por ejemplo, mydomain.com). No incluya una dirección IP. El sistema vCenter Server debe poder resolver este nombre de dominio mediante DNS. Si utiliza vCenter Server Appliance, use la información sobre la configuración de parámetros de red para actualizar la configuración del servidor DNS.
Usar cuenta de equipo	Seleccione esta opción para usar la cuenta de equipo local como el SPN. Si selecciona esta opción, solo debe especificar el nombre de dominio. No seleccione esta opción si desea cambiar el nombre de este equipo.
Usar nombre de entidad de seguridad de servicio (SPN)	Seleccione esta opción si desea cambiar el nombre del equipo local. Debe especificar un SPN, un usuario que pueda autenticarse con el origen de identidad y una contraseña para el usuario.
Nombre de entidad de seguridad de servicio (SPN)	SPN ayuda a que Kerberos identifique el servicio de Active Directory. Incluya un dominio en el nombre (por ejemplo, STS/example.com).  El SPN debe ser único en todo el dominio. La ejecución de <code>setspn -S</code> comprueba que no se creen duplicados. Consulte la documentación de Microsoft para obtener información sobre <code>setspn</code> .
Nombre principal de usuario (UPN) Contraseña	Nombre y contraseña de un usuario que puede autenticarse con este origen de identidad. Utilice el formato de dirección de correo electrónico (por ejemplo, jchin@mydomain.com). Puede comprobar el nombre principal de usuario con el editor de interfaces del servicio de Active Directory (editor ADSI).

## Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory

Active Directory como origen de identidad de servidores LDAP está disponible para compatibilidad con versiones anteriores. Use la opción de Active Directory (autenticación integrada de Windows) para una configuración que requiera menos entrada de datos. El origen de identidad de servidores OpenLDAP está disponible para los entornos que usan OpenLDAP.

Si va a configurar un origen de identidad de OpenLDAP, consulte el artículo [2064977](#) de la base de conocimientos de VMware para obtener información sobre los requisitos adicionales.

**Tabla 2-6. Configuración de servidores OpenLDAP y LDAP de Active Directory**

Campo	Descripción
Nombre	Nombre del origen de identidad.
DN base para usuarios	El nombre distinguido base para los usuarios.
Nombre de dominio	FDQN del dominio (por ejemplo, ejemplo.com). No proporcione una dirección IP en este campo.
Alias de dominio	Para los orígenes de identidad de Active Directory, el nombre de NetBIOS del dominio. Si usa autenticaciones de SSPI, agregue el nombre de NetBIOS del dominio de Active Directory como alias del origen de identidad.  Para los orígenes de identidad de OpenLDAP, si no se especifica un alias, se agrega el nombre del dominio en mayúsculas.
DN base para grupos	El nombre distinguido base para grupos.
URL de servidor principal	El servidor LDAP de la controladora de dominio principal para el dominio.  Use el formato <code>ldap://nombre de host:puerto</code> o <code>ldaps://nombre de host:puerto</code> . Por lo general, el puerto es el 389 para las conexiones de ldap: y 636 para las conexiones de ldaps:. Para las implementaciones de controladoras de varios dominios de Active Directory, el puerto suele ser el 3268 para las conexiones de ldap: y el 3269 para las conexiones de ldaps:.  Se necesita un certificado que establezca la confianza para el extremo de LDAPS del servidor Active Directory cuando se usa ldaps:// en la URL del servidor LDAP principal o secundario.
URL de servidor secundario	Dirección de un servidor LDAP de controladora de dominio secundario que se usa para la conmutación por error.
Elegir certificado	Si desea utilizar LDAPS con el origen de identidad de servidor LDAP o servidor OpenLDAP de Active Directory, aparece el botón Elegir certificado después de escribir <b>ldaps://</b> en el campo Dirección URL. No se requiere una dirección URL secundaria.

Tabla 2-6. Configuración de servidores OpenLDAP y LDAP de Active Directory (continuación)

Campo	Descripción
Nombre de usuario	Identificador de un usuario del dominio que tiene, como mínimo, acceso de solo lectura al DN base para los usuarios y los grupos.
Contraseña	Contraseña del usuario especificado en el campo Nombre de usuario.

## Editar un origen de identidad de vCenter Single Sign-On

Los usuarios de vSphere se definen en un origen de identidad. Puede editar los detalles de un origen de identidad que está asociado con vCenter Single Sign-On.

### Procedimiento

- 1 Inicie sesión en vSphere Web Client como `administrator@vsphere.local` u otro usuario con privilegios de administrador de vCenter Single Sign-On.  
  
Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio `vsphere.local`.
- 2 Desplácese hasta **Administración > Single Sign-On > Configuración**.
- 3 Haga clic en la pestaña **Orígenes de identidad**.
- 4 Haga clic con el botón derecho en el origen de identidad que figura en la tabla y seleccione **Editar origen de identidad**.
- 5 Edite la configuración del origen de identidad. Las opciones disponibles dependerán del tipo de origen de identidad que seleccionó.

Opción	Descripción
<b>Active Directory (autenticación integrada de Windows)</b>	Utilice esta opción para las implementaciones nativas de Active Directory. Si desea utilizar esta opción, la máquina en la que se ejecuta el servicio vCenter Single Sign-On debe estar en un dominio de Active Directory. Consulte <a href="#">Configurar orígenes de identidad de Active Directory</a> .
<b>Active Directory como servidor LDAP</b>	Esta opción está disponible para brindar compatibilidad con versiones anteriores. Requiere que especifique la controladora de dominio y otra información. Consulte <a href="#">Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory</a> .
<b>OpenLDAP</b>	Utilice esta opción para un origen de identidad OpenLDAP. Consulte <a href="#">Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory</a> .
<b>LocalOS</b>	Utilice esta opción para agregar el sistema operativo local como origen de identidad. Se solicita únicamente el nombre del sistema operativo local. Si selecciona esta opción, todos los usuarios de la máquina especificada quedan visibles para vCenter Single Sign-On, incluso si estos no forman parte de otro dominio.



- 6 Haga clic en **Probar conexión** para garantizar que pueda conectarse al origen de identidad.
- 7 Haga clic en **Aceptar**.

## Quitar un origen de identidad de vCenter Single Sign-On

Los usuarios de vSphere se definen en un origen de identidad. Puede quitar un origen de identidad de la lista de orígenes de identidad registrados.

### Procedimiento

- 1 Inicie sesión en vSphere Web Client como `administrator@vsphere.local` u otro usuario con privilegios de administrador de vCenter Single Sign-On.  
  
Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio `vsphere.local`.
- 2 Desplácese hasta **Administración > Single Sign-On > Configuración**.
- 3 En la pestaña **Orígenes de identidad**, seleccione un origen de identidad y haga clic en el icono **Eliminar origen de identidad**.
- 4 Haga clic en **Sí** cuando el sistema solicite la confirmación.

## Usar vCenter Single Sign-On con autenticación de sesión de Windows

Puede usar vCenter Single Sign-On con la autenticación de sesión de Windows (SSPI). Para que la casilla de la página de inicio de sesión esté disponible, debe tener instalado el complemento de integración de clientes.

El uso de SSPI acelera el inicio de sesión del usuario que tiene una sesión abierta en una máquina.

### Requisitos previos

El dominio de Windows debe estar configurado correctamente. Consulte el artículo [2064250](#) de la base de conocimientos de VMware.

### Procedimiento

- 1 Desplácese hasta la página de inicio de sesión de vSphere Web Client.
- 2 Si la casilla **Utilizar autenticación de sesión de Windows** no está disponible, haga clic en **Descargar el complemento de integración de clientes** al final de la página de inicio de sesión.
- 3 Si el explorador bloquea la instalación mediante la emisión de errores de certificado o la ejecución de un bloqueador de elementos emergentes, siga las instrucciones de la Ayuda para solucionar el problema del explorador.
- 4 Si el sistema se lo solicita, cierre los demás exploradores.

Después de la instalación, el complemento queda disponible para todos los exploradores. Si el explorador lo requiere, es posible que deba permitir el complemento para sesiones individuales o para todas las sesiones.

## 5 Salga y reinicie el explorador.

Después del reinicio, puede activar la casilla **Utilizar autenticación de sesión de Windows**.

# Autenticación de dos factores con vCenter Server

vCenter Single Sign-On permite la autenticación de usuarios con nombre de usuario y contraseña en un origen de identidad conocido para vCenter Single Sign-On, o a través de la autenticación de sesión de Windows para orígenes de identidades de Active Directory. A partir de vSphere 6.0 Update 2, también puede autenticarse a través de una tarjeta inteligente (Tarjeta de acceso común basado en UPN o CAC), o a través de un token RSA SecurID.

## Métodos de autenticación de dos factores

Los métodos de autenticación de dos factores a menudo son requeridos por agencias gubernamentales o empresas de gran tamaño.

### Autenticación con tarjeta de acceso común (CAC)

La autenticación CAC solo permite el acceso a usuarios que adjuntan una tarjeta física a la unidad USB de la computadora en donde inician sesión. Si se implementa la PKI de manera que los certificados de tarjeta inteligente sean los únicos certificados del cliente emitidos por la CA, solo se presentan al usuario los certificados de tarjeta inteligente. El usuario selecciona un certificado, y luego se le solicita un PIN. Solo los usuarios que tienen tarjeta física y el PIN que coincide con el certificado pueden iniciar sesión.

### Autenticación de RSA SecurID

Para utilizar la autenticación de RSA SecureID, el entorno debe incluir una instancia de RSA Authentication Manager configurada correctamente. Si Platform Services Controller está configurado para apuntar al servidor RSA, y si la autenticación de RSA SecurID está habilitada, los usuarios pueden iniciar sesión con su nombre de usuario y su token.

---

**Nota** vCenter Single Sign-On solo admite SecurID nativo; no admite autenticación RADIUS.

---

## Especificar un método de autenticación no predeterminado

Los administradores pueden realizar la instalación desde la interfaz web de Platform Services Controller, o a través del script de `sso-config` (`sso-config.bat` en Windows y `sso-config.sh` en el dispositivo).

- Para la autenticación de tarjeta de acceso común, puede configurar el explorador web a través del script `desso-config` y puede configurar vCenter Single Sign-On desde la interfaz web de Platform Services Controller o a través de `sso-config`. La configuración incluye la autenticación CAC, la configuración de directivas de revocación de certificados y la configuración de un banner de inicio de sesión.

- En el caso de RSA SecureID, puede utilizar el script de `sso-config` para configurar RSA Authentication Manager para el dominio y para habilitar la autenticación de token de RSA. El método de autenticación se muestra en la interfaz web de Platform Services Controller (si está habilitada), pero no se puede configurar la autenticación RSA SecureID desde la interfaz web.

## Combinar diferentes métodos de autenticación

Los métodos de autenticación se pueden habilitar o deshabilitar en forma separada a través de `sso-config`. Tiene lógica, por ejemplo, inicialmente dejar habilitada la autenticación por nombre de usuario y contraseña mientras está probando uno de los métodos de autenticación de dos factores y, a continuación, configurar un solo método de autenticación como habilitado.

## Configuración de la autenticación de tarjeta inteligente para vCenter Single Sign-On

El entorno puede configurarse para que requiera autenticación de tarjeta inteligente cuando un usuario se conecta a vCenter Server o Platform Services Controller asociado desde vSphere Web Client.

### Inicio de sesión de autenticación de tarjeta inteligente

Una tarjeta inteligente es una tarjeta plástica pequeña con un chip de circuito integrado. Muchas agencias gubernamentales y empresas grandes utilizan tarjetas inteligentes como Tarjetas de acceso común (CAC) para incrementar la seguridad de los sistemas y cumplir con las normas de seguridad. Las tarjetas de acceso común se utilizan en entornos en donde cada máquina está equipada con un lector de tarjetas inteligentes, y en donde los controladores de hardware de las tarjetas inteligentes que administran las tarjetas de acceso común generalmente están preinstalados.

Al configurar la autenticación de tarjeta inteligente para vCenter Single Sign-On, se les solicita a los usuarios que inician sesión en vCenter Server o Platform Services Controller que se autenticquen con una combinación de tarjeta inteligente y PIN, como se indica a continuación:

- 1 Cuando se introduce la tarjeta inteligente en el lector de tarjetas inteligentes, vCenter Single Sign-On lee los certificados en la tarjeta.
- 2 vCenter Single Sign-On solicita al usuario que seleccione un certificado, y luego solicita el PIN correspondiente a dicho certificado.
- 3 vCenter Single Sign-On verifica si el certificado de la tarjeta inteligente es conocido y si el PIN es correcto. Si la verificación de revocación está activa, vCenter Single Sign-On también verifica si el certificado fue revocado.

- 4 Si el certificado es conocido y no es un certificado revocado, el usuario es autenticado y puede realizar las tareas para las que tiene permisos.

---

**Nota** En la mayoría de los casos, es lógico dejar la autenticación por nombre y contraseña activada durante las pruebas. Una vez completada la prueba, deshabilite la autenticación por nombre de usuario y contraseña, y habilite la autenticación de tarjeta inteligente. Luego, vSphere Client solo admitirá el inicio de sesión de tarjeta inteligente. Solo los usuarios con privilegios de raíz o administrador en la máquina podrán volver a habilitar la autenticación por nombre de usuario y contraseña, a través del inicio de sesión directo en Platform Services Controller

---

## Usar la línea de comandos para configurar la autenticación de tarjeta inteligente

La utilidad `sso-config` se puede utilizar para configurar la autenticación de tarjeta inteligente desde la línea de comandos. La utilidad admite todas las tareas de configuración de tarjeta inteligente.

Al configurar la autenticación de tarjeta inteligente desde la línea de comandos, siempre debe configurar primero Platform Services Controller mediante el comando `sso-config`. A continuación, puede realizar otras tareas mediante la interfaz web de Platform Services Controller.

- 1 Configure Platform Services Controller de modo que el explorador web solicite el envío del certificado de tarjeta inteligente cuando el usuario inicie sesión.
- 2 Configure la directiva de autenticación. Puede configurar la directiva mediante el script `sso-config` o la interfaz web de Platform Services Controller. La configuración de los tipos de autenticación admitidos y la configuración de revocación se almacenan en VMware Directory Service y se replican en todas las instancias de Platform Services Controller en un dominio de vCenter Single Sign-On.

Si se habilita la autenticación de tarjeta inteligente y se deshabilitan otros métodos de autenticación, se solicitará a los usuarios que inicien sesión con la autenticación de tarjeta inteligente.

Si el inicio de sesión desde vSphere Web Client no funciona, y si la autenticación por nombre de usuario y contraseña está desactivada, un usuario raíz o administrador puede volver a habilitar la autenticación por nombre de usuario y contraseña desde la línea de comandos Platform Services Controller a través del siguiente comando. El ejemplo se aplica a Windows; para Linux, utilice `sso-config.sh`.

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

Puede encontrar el script de `sso-config` en las siguientes ubicaciones:

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

---

## Requisitos previos

- Compruebe que el entorno utiliza Platform Services Controller versión 6.0 Update 2 o posteriores, y que usted usa vCenter Server versión 6.0 o posteriores. Actualice los nodos versión 5.5. a la versión 6.0.
- Compruebe que en su entorno se haya configurado una infraestructura de clave pública (PKI) empresarial, y que los certificados cumplan con los siguientes requerimientos:
  - Un nombre principal de usuario (UPN) que corresponda a una cuenta de Active Directory en la extensión del nombre alternativo de asunto (SAN).
  - La autenticación del cliente se debe especificar en el campo Directiva de aplicación o Utilización de clave mejorada de un certificado; de lo contrario, el explorador no mostrará el certificado.
- Compruebe que el certificado de la interfaz web de Platform Services Controller sea un certificado confiable para la workstation del usuario final; de lo contrario, el explorador no intentará la autenticación.
- Configure un origen de identidad de Active Directory y agréguelo a vCenter Single Sign-On como un origen de identidad.
- Asigne la función de Administrador de vCenter Server a uno o más usuarios en el origen de identidad de Active Directory. Los usuarios luego se pueden autenticar porque están en el grupo de Active Directory y poseen privilegios de administrador de vCenter Server. El usuario administrator@vsphere.local no puede realizar la autenticación de tarjeta inteligente.
- Si desea utilizar la solución Platform Services Controller HA en su entorno, complete toda la configuración de HA antes de configurar la autenticación de tarjeta inteligente. Consulte el artículo [2112085](#) (Windows) o [2113315](#) (vCenter Server Appliance) de la base de conocimientos de VMware.

## Procedimiento

- 1 Obtenga los certificados y cópielos en una carpeta que la utilidad `sso-config` pueda ver.

Opción	Descripción
Windows	Inicie sesión en la instancia de Platform Services Controller de la instalación de Windows y utilice WinSCP o una utilidad similar para copiar los archivos.
Dispositivo	<ol style="list-style-type: none"> <li>a Inicie sesión en la consola de dispositivos, ya sea directamente o a través de SSH.</li> <li>b Habilite el shell del dispositivo, como se indica a continuación. <pre>shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root</pre> </li> <li>c Utilice WinSCP o una utilidad similar para copiar los certificados en <code>/usr/lib/vmware-sso/vmware-sts/conf</code> en la instancia de Platform Services Controller.</li> <li>d Opcionalmente, deshabilite el shell del dispositivo, como se indica a continuación. <pre>chsh -s "bin/appliancesh" root</pre> </li> </ol>

- 2 En cada nodo de Platform Services Controller, configure la autenticación de tarjeta inteligente a través de la interfaz CLI de `sso-config`.

- a Desplácese hasta el directorio en donde se ubica el script de `sso-config`.

Opción	Descripción
Windows	C:\Archivos de programa\VMware\VCenter server\VMware Identity Services
Dispositivo	/opt/vmware/bin

- b Ejecute el siguiente comando:

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

Por ejemplo:

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

- c Reinicie la máquina virtual o física.

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

- 3 Para habilitar la autenticación de tarjeta inteligente para VMware Directory Service (vmdir), ejecute el siguiente comando.

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

Por ejemplo:

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

Si especifican varios certificados, no se permiten espacios entre los certificados.

- 4 Para deshabilitar todos los otros métodos de autenticación, ejecute los siguientes comandos.

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

Puede utilizar los siguientes comandos para habilitar y deshabilitar distintos métodos de autenticación, según sea necesario.

- 5 (opcional) Para establecer una lista de permitidos de directivas de certificado, ejecute el siguiente comando.

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

Para especificar varias directivas, sepárelas con un comando, por ejemplo:

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

La lista de permitidos especifica los identificadores de objeto de las directivas que están permitidas en la extensión de directiva de certificados del certificado. Los certificados X509 pueden tener una extensión de directiva de certificados.

- 6 (opcional) Para hacer una lista de la información de configuración, ejecute el siguiente comando.

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

## Usar la interfaz web de Platform Services Controller para administrar la autenticación de tarjeta inteligente

Puede habilitar o deshabilitar la autenticación de tarjeta inteligente, personalizar el banner de inicio de sesión y configurar la directiva de revocación desde la interfaz web de Platform Services Controller.

Al configurar la autenticación de tarjeta inteligente desde la línea de comandos, siempre debe configurar primero Platform Services Controller mediante el comando `sso-config`. A continuación, puede realizar otras tareas mediante la interfaz web de Platform Services Controller.

- 1 Configure Platform Services Controller de modo que el explorador web solicite el envío del certificado de tarjeta inteligente cuando el usuario inicie sesión.
- 2 Configure la directiva de autenticación. Puede configurar la directiva mediante el script `sso-config` o la interfaz web de Platform Services Controller. La configuración de los tipos de autenticación admitidos y la configuración de revocación se almacenan en VMware Directory Service y se replican en todas las instancias de Platform Services Controller en un dominio de vCenter Single Sign-On.

Si se habilita la autenticación de tarjeta inteligente y se deshabilitan otros métodos de autenticación, se solicitará a los usuarios que inicien sesión con la autenticación de tarjeta inteligente.

Si el inicio de sesión desde vSphere Web Client no funciona, y si la autenticación por nombre de usuario y contraseña está desactivada, un usuario raíz o administrador puede volver a habilitar la autenticación por nombre de usuario y contraseña desde la línea de comandos Platform Services Controller a través del siguiente comando. El ejemplo se aplica a Windows; para Linux, utilice `sso-config.sh`.

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

#### Requisitos previos

- Compruebe que el entorno utiliza Platform Services Controller versión 6.0 Update 2 o posteriores, y que usted usa vCenter Server versión 6.0 o posteriores. Actualice los nodos versión 5.5. a la versión 6.0.
- Compruebe que en su entorno se haya configurado una infraestructura de clave pública (PKI) empresarial, y que los certificados cumplan con los siguientes requerimientos:
  - Un nombre principal de usuario (UPN) que corresponda a una cuenta de Active Directory en la extensión del nombre alternativo de asunto (SAN).
  - La autenticación del cliente se debe especificar en el campo Directiva de aplicación o Utilización de clave mejorada de un certificado; de lo contrario, el explorador no mostrará el certificado.
- Compruebe que el certificado de la interfaz web de Platform Services Controller sea un certificado confiable para la workstation del usuario final; de lo contrario, el explorador no intentará la autenticación.
- Configure un origen de identidad de Active Directory y agréguelo a vCenter Single Sign-On como un origen de identidad.



- Asigne la función de Administrador de vCenter Server a uno o más usuarios en el origen de identidad de Active Directory. Los usuarios luego se pueden autenticar porque están en el grupo de Active Directory y poseen privilegios de administrador de vCenter Server. El usuario `administrator@vsphere.local` no puede realizar la autenticación de tarjeta inteligente.
- Si desea utilizar la solución Platform Services Controller HA en su entorno, complete toda la configuración de HA antes de configurar la autenticación de tarjeta inteligente. Consulte el artículo [2112085](#) (Windows) o [2113315](#) (vCenter Server Appliance) de la base de conocimientos de VMware.

## Procedimiento

- 1 Obtenga los certificados y cópielos en una carpeta que la utilidad `sso-config` pueda ver.

Opción	Descripción
Windows	Inicie sesión en la instancia de Platform Services Controller de la instalación de Windows y utilice WinSCP o una utilidad similar para copiar los archivos.
Dispositivo	<ol style="list-style-type: none"> <li>a Inicie sesión en la consola de dispositivos, ya sea directamente o a través de SSH.</li> <li>b Habilite el shell del dispositivo, como se indica a continuación. <pre>shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root</pre> </li> <li>c Utilice WinSCP o una utilidad similar para copiar los certificados en <code>/usr/lib/vmware-sso/vmware-sts/conf</code> en la instancia de Platform Services Controller.</li> <li>d Opcionalmente, deshabilite el shell del dispositivo, como se indica a continuación. <pre>chsh -s "bin/appliancesh" root</pre> </li> </ol>

- 2 En cada nodo de Platform Services Controller, configure la autenticación de tarjeta inteligente a través de la interfaz CLI de `sso-config`.

- a Desplácese hasta el directorio en donde se ubica el script de `sso-config`.

Opción	Descripción
Windows	C:\Archivos de programa\VMware\VCenter server\VMware Identity Services
Dispositivo	/opt/vmware/bin

- b Ejecute el siguiente comando:

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

Por ejemplo:

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

Separe los distintos certificados con comas, pero no incluya espacios después de la coma.

- c Reinicie la máquina virtual o física.

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

- 3 En un explorador web, especifique la siguiente dirección URL para conectarse a Platform Services Controller:

**`https://psc_hostname_or_IP/psc`**

En una implementación integrada, el nombre de host o la dirección IP de Platform Services Controller es igual al nombre de host o la dirección IP de vCenter Server.

- 4 Especifique el nombre de usuario y la contraseña para `administrator@vsphere.local` u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como `administrator@mydomain`.

- 5 Desplácese hasta **Single Sign-On > Configuración**.
- 6 Haga clic en **Configuración de tarjeta inteligente** y seleccione la pestaña **Certificados de CA confiables**.
- 7 Para agregar uno o más certificados de confianza, haga clic en **Agregar certificado**, luego haga clic en **Examinar** y seleccione todos los certificados de CA de confianza; por último, haga clic en **Aceptar**.

- 8 Para especificar la configuración de autenticación, haga clic en **Editar**, junto a **Configuración de autenticación**, y seleccione o anule la selección de los métodos de autenticación.

No puede habilitar o deshabilitar la autenticación de RSA SecurID desde esta interfaz web.

Sin embargo, si se habilitó RSA SecurID desde la línea de comandos, el estado aparece en la interfaz web.

## Configurar directivas de revocación para autenticación de tarjeta inteligente

Puede personalizar la verificación de revocación de certificados, así como especificar en qué lugar vCenter Single Sign-On busca información sobre certificados revocados.

Puede personalizar la conducta utilizando la interfaz web de Platform Services Controller o a través del script de `sso-config`. La configuración seleccionada depende en parte de lo que la CA admite.

- Si la verificación de revocación está deshabilitada, vCenter Single Sign-On ignora cualquier configuración de CRL o OCSP.
- Si la verificación de revocación está habilitada, la configuración recomendada depende de la configuración de la PKI.

### Solo OCSP

Si la CA emisora admite un respondedor OCSP, habilite OCSP y deshabilite la utilización de CRL para conmutación por error.

### Solo CRL

Si la CA emisora no admite OCSP, habilite la verificación de CRL y deshabilite la verificación de OCSP.

### Tanto OCSP como CRL

Si la CA emisora admite tanto un respondedor OCSP como CRL, vCenter Single Sign-On verifica el respondedor OCSP primero. Si el respondedor devuelve un estado desconocido o no está disponible, vCenter Single Sign-On verifica la CRL primero. En este caso, habilite la verificación de OCSP y la de CRL, y habilite CRL como conmutación por error para OCSP.

- Si la verificación de revocación está habilitada, los usuarios avanzados pueden especificar la siguiente configuración adicional.

### URL de OCSP

De forma predeterminada, vCenter Single Sign-On verifica la ubicación del respondedor OCSP que se define en el certificado que se está validando. Puede especificar una ubicación explícitamente si no se incluye la extensión Acceso a información de autoridad en el certificado, o si desea anularlo (por ejemplo, por no estar disponible en el entorno).

### Usar CRL del certificado

De forma predeterminada, vCenter Single Sign-On verifica la ubicación de CRL que se define en el certificado que se está validando. Deshabilite esta opción cuando el certificado no incluye la extensión del punto de distribución de CRL o si desea anular la que se define de forma predeterminada.

### Ubicación de CRL

Utilice esta propiedad si deshabilita **Usar CRL del certificado** y desea especificar una ubicación (archivo o URL HTTP) en donde se encuentra la CRL.

Además, se puede agregar una directiva de certificados para limitar aún más los certificados que acepta vCenter Single Sign-On.

### Requisitos previos

- Compruebe que el entorno esté utilizando Platform Services Controller versión 6.0 Update 2 o posteriores, y que se esté utilizando vCenter Server versión 6.0 o posteriores. Actualice los nodos versión 5.5. a la versión 6.0.
- Compruebe que en su entorno se haya configurado una infraestructura de clave pública (PKI) empresarial, y que los certificados cumplan con los siguientes requerimientos:
  - Un nombre principal de usuario (UPN) que corresponda a una cuenta de Active Directory en la extensión del nombre alternativo de asunto (SAN).
  - La autenticación del cliente se debe especificar en el campo Directiva de aplicación o Utilización de clave mejorada de un certificado; de lo contrario, el explorador no mostrará el certificado.
- Compruebe que el certificado de la interfaz web de Platform Services Controller sea un certificado confiable para la workstation del usuario final; de lo contrario, el explorador no intentará la autenticación.
- Configure un origen de identidad de Active Directory y agréguelo a vCenter Single Sign-On como un origen de identidad.
- Asigne la función de Administrador de vCenter Server a uno o más usuarios en el origen de identidad de Active Directory. Los usuarios luego se pueden autenticar porque están en el grupo de Active Directory y poseen privilegios de administrador de vCenter Server. El usuario administrator@vsphere.local no puede realizar la autenticación de tarjeta inteligente.
- Si desea utilizar la solución Platform Services Controller HA en su entorno, complete toda la configuración de HA antes de configurar la autenticación de tarjeta inteligente. Consulte el artículo [2113085](#) (Windows) o [2113315](#) (vCenter Server Appliance) para obtener más detalles.

### Procedimiento

- 1 En un explorador web, especifique la siguiente dirección URL para conectarse a Platform Services Controller:

**`https://psc_hostname_or_IP/psc`**

En una implementación integrada, el nombre de host o la dirección IP de Platform Services Controller es igual al nombre de host o la dirección IP de vCenter Server.

- 2 Especifique el nombre de usuario y la contraseña para `administrator@vsphere.local` u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como `administrator@mydomain`.

- 3 Desplácese hasta **Single Sign-On > Configuración**.
- 4 Haga clic en **Configuración de revocación de certificado** y habilite o deshabilite la verificación de revocación.
- 5 Si en su entorno hay directivas de certificados vigentes, puede agregar una directiva en el panel **Se aceptaron las directivas de certificado**.

## Configurar la autenticación de RSA SecurID

Se puede configurar el entorno de manera que se solicite a los usuarios iniciar sesión con un token RSA SecurID en lugar de con una contraseña. La configuración de SecurID solo es compatible desde la línea de comandos.

Para obtener más información, consulte las dos publicaciones del blog de vSphere sobre la [configuración de RSA SecurID](#).

---

**Nota** RSA Authentication Manager requiere que el identificador de usuario sea único, y que utilice entre 1 y 255 caracteres ASCII. Los caracteres Y comercial (&), porcentaje (%), mayor que (>), menor que (<) y apóstrofo (') no están permitidos.

---

### Requisitos previos

- Compruebe que el entorno esté utilizando Platform Services Controller versión 6.0 Update 2 o posteriores, y que se esté utilizando vCenter Server versión 6.0 o posteriores. Actualice los nodos versión 5.5. a la versión 6.0.
- Compruebe que RSA Authentication Manager se haya configurado correctamente en el entorno y que los usuarios disponen de tokens RSA. Compruebe que RSA Authentication Manager se haya configurado correctamente en el entorno y que los usuarios dispongan de tokens RSA. Se requiere RSA Authentication Manager versión 8.0 o posterior.
- Compruebe que el origen de identidad que utiliza RSA Manager se haya agregado a vCenter Single Sign-On. Consulte [Agregar un origen de identidad de vCenter Single Sign-On](#).
- Compruebe que el sistema RSA Authentication Manager pueda resolver el nombre de host de Platform Services Controller y que el sistema Platform Services Controller pueda resolver el nombre de host de RSA Authentication Manager.
- Exporte el archivo `sdconf.rec` desde la instancia de RSA Manager seleccionando **Acceso > Agentes de autenticación > Generar archivo de configuración**. Descomprima el archivo `AM_Config.zip` resultante para buscar el archivo `sdconf.rec`.
- Copie el archivo `sdconf.rec` en el nodo Platform Services Controller.

## Procedimiento

- 1 Pase al directorio donde se ubica el script de `sso-config`.

Opción	Descripción
Windows	C:\Archivos de programa\VMware\VCenter server\VMware Identity Services
Dispositivo	/opt/vmware/bin

- 2 Para habilitar la autenticación de RSA SecurID, ejecute el siguiente comando.

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

*tenantName* es el nombre del dominio vCenter Single Sign-On, `vsphere.local` en forma predeterminada.

- 3 (opcional) Para deshabilitar otros métodos de autenticación, ejecute el siguiente comando.

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

- 4 Para configurar el entorno de forma que el tenant del sitio actual utilice el sitio de RSA, ejecute el siguiente comando.

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

Por ejemplo:

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

Puede especificar las siguientes opciones.

Opción	Descripción
<b>siteID</b>	Identificador opcional del sitio de Platform Services Controller. Platform Services Controller admite una instancia de RSA Authentication Manager o clúster por sitio. Si no especifica esta opción de manera explícita, la configuración de RSA se destina al sitio de Platform Services Controller actual. Solo utilice esta opción si desea agregar un sitio diferente.
<b>agentName</b>	Definido en RSA Authentication Manager.
<b>sdConfFile</b>	Copia del archivo Se descargó una copia del archivo <code>sdconfig.rec</code> descargado desde RSA Manager, que incluye información de configuración de RSA Manager (por ejemplo, la dirección IP).descargado desde RSA Manager, que incluye información de configuración de RSA Manager (por ejemplo, la dirección IP).

- 5 (opcional) Para cambiar la configuración del tenant para que utilice valores distintos a los predeterminados, ejecute el siguiente comando.

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

El valor predeterminado suele ser adecuado, por ejemplo:

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

- 6 (opcional) Si el origen de identidad no utiliza el nombre de entidad de seguridad de usuario como identificador del usuario, configure el atributo userID del origen de identidad. Si el origen de identidad no utiliza el nombre principal de usuario como identificador del usuario, configure el atributo userID del origen de identidad.

El atributo userID determina qué atributo LDAP se utiliza como userID en RSA.

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

Por ejemplo:

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

- 7 Para mostrar la configuración actual, ejecute el siguiente comando.

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

## Resultados

Si la autenticación por nombre de usuario y contraseña está no está habilitada, pero la autenticación del token SecurID sí lo está, los usuarios deberán iniciar sesión con el nombre de usuario y el token SecurID. Si la autenticación por nombre de usuario y contraseña no está habilitada, pero la autenticación del token SecurID sí lo está, los usuarios deberán iniciar sesión con el nombre de usuario y el token SecurID. Ya no es posible iniciar sesión con el nombre de usuario y la contraseña.

## Administrar el banner de inicio de sesión

A partir de vSphere 6.0 Update 2, se puede incluir un banner de inicio de sesión en el entorno. Se puede mostrar texto o solicitar que el usuario haga clic en una casilla, por ejemplo, para indicar que aceptan los términos y las condiciones. Se puede habilitar o deshabilitar el banner de inicio de sesión, y se puede solicitar que los usuarios hagan clic en una casilla de consentimiento explícito.

**Procedimiento**

- 1 En un explorador web, especifique la siguiente dirección URL para conectarse a Platform Services Controller:

**`https://psc_hostname_or_IP/psc`**

En una implementación integrada, el nombre de host o la dirección IP de Platform Services Controller es igual al nombre de host o la dirección IP de vCenter Server.

- 2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como administrator@mydomain.

- 3 En Single Sign-On, seleccione **Configuración** y haga clic en la pestaña **Banner de inicio de sesión**.
- 4 Haga clic en **Editar** y configure el banner de inicio de sesión.

Opción	Descripción
Estado	Haga clic en la casilla <b>Habilitado</b> para habilitar el banner de inicio de sesión. Solo si se hace clic en esta casilla se podrán modificar los otros campos.
Consentimiento explícito	Haga clic en la casilla <b>Consentimiento explícito</b> para solicitar al usuario que haga clic en una casilla antes de iniciar sesión. También se puede mostrar un mensaje sin ninguna casilla.
Título	Título del banner. En forma predeterminada, el texto del banner de inicio de sesión es <code>I agree to the</code> . A este texto, se le puede agregar, por ejemplo <code>Terms and Conditions</code> .
Mensaje	Mensaje que ve el usuario al hacer clic en el banner. Por ejemplo, el texto de los términos y las condiciones. Si se utiliza consentimiento explícito, se debe mostrar este mensaje.

## Utilizar vCenter Single Sign-On como el proveedor de identidad para otro proveedor de servicios

vSphere Web Client se registra automáticamente como proveedor de servicios (SP) SAML 2.0 de confianza en vCenter Single Sign-On. Puede agregar otros proveedores de servicios de confianza a una federación de identidades en donde vCenter Single Sign-On actúa como proveedor de identidad (IDP) SAML. Los proveedores de servicios deben cumplir con el protocolo SAML 2.0. Tras configurar la federación, el proveedor de servicios permite el acceso a un usuario si este puede autenticarse en vCenter Single Sign-On.

**Nota** vCenter Single Sign-On puede ser el IDP para otros SP. vCenter Single Sign-On no puede ser un SP que use otro IDP.



Un proveedor de servicios SAML registrado puede permitir el acceso a otro usuario que ya tenga una sesión activa, es decir, un usuario que haya iniciado sesión en el proveedor de identidad. Por ejemplo, vRealize Automation 7.0 y versiones posteriores admiten vCenter Single Sign-On como un proveedor de identidad. Puede configurar una federación desde vCenter Single Sign-On y vRealize Automation. Después de esto, vCenter Single Sign-On puede realizar la autenticación cuando inicie sesión en vRealize Automation.

Para unir un proveedor de servicios SAML a la federación de identidades, tiene que configurar la confianza entre el SP y el IDP intercambiando los metadatos SAML entre ellos.

Tanto para vCenter Single Sign-On, como para el servicio que utiliza vCenter Single Sign-On, se deben realizar tareas de integración.

- 1 Exporte los metadatos del IDP a un archivo y después impórtelos en el SP.
- 2 Exporte los metadatos del SP e impórtelos en el IDP.

Puede usar la interfaz de vSphere Web Client para vCenter Single Sign-On para exportar los metadatos del IDP y para importar los del SP. Si está usando vRealize Automation como el SP, consulte la documentación de vRealize Automation para obtener detalles sobre cómo exportar los metadatos del SP e importar los del IDP.

---

**Nota** El servicio debe admitir completamente el estándar SAML 2.0, de lo contrario, la integración no funcionará.

---

## Agregar un proveedor de servicios SAML

Puede agregar un proveedor de servicios SAML a vCenter Single Sign-On y luego agregar vCenter Single Sign-On como el proveedor de identidades de ese servicio. Posteriormente, cuando los usuarios inicien sesión en el proveedor de servicios, este autenticará a los usuarios con vCenter Single Sign-On.

Utilice este proceso si desea integrar la solución Single Sign-On que se incluye en VMware vRealize Automation 7.0 y versiones posteriores con el proveedor de identidades de vCenter Single Sign-On, o bien si está trabajando con otro proveedor de servicios SAML externo.

El proceso implica importar los metadatos del proveedor de servicios SAML en vCenter Single Sign-On e importar los metadatos de vCenter Single Sign-On en el proveedor de servicios SAML de modo que los dos proveedores compartan todos los datos.

### Requisitos previos

El servicio de destino debe ser totalmente compatible con el estándar SAML 2.0.

Si los metadatos no siguen el esquema de metadatos de SAML 2.0 de forma precisa, puede que deba editar el esquema antes de importarlo. Por ejemplo, si está utilizando un proveedor de servicios SAML de Servicios de federación de Active Directory (AD FS), debe editar los metadatos para poder importarlos. Quite los siguientes elementos no estándar:

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

No puede importar los metadatos de IDP de SAML desde vSphere Web Client en este momento.

#### Procedimiento

- 1 Exporte los metadatos del proveedor de servicios a un archivo.
- 2 Importe los metadatos del proveedor de servicios en vCenter Single Sign-On.
  - a Inicie sesión en vSphere Web Client como `administrator@vsphere.local` u otro usuario con privilegios de administrador de vCenter Single Sign-On.

Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio `vsphere.local`.
  - b Desplácese hasta **Single Sign-On > Configuración**.
  - c Seleccione la pestaña **Proveedores de servicios SAML**.
  - d En el campo **Metadatos del proveedor de servicios SAML**, haga clic en **Importar** y pegue las cadenas XML en el cuadro de diálogo, o bien haga clic en **Importar desde archivo** para importar un archivo y, a continuación, haga clic en **Importar**.
- 3 Exporte los metadatos de vCenter Single Sign-On.
  - a En el campo **Metadatos para el proveedor de servicios SAML**, haga clic en **Descargar**.
  - b Especifique una ubicación de archivo.
- 4 Diríjase al proveedor de servicios SAML (por ejemplo, VMware vRealize Automation 7.0 o versiones posteriores) y siga las instrucciones del proveedor de servicios SAML para agregar los metadatos de vCenter Single Sign-On a ese proveedor de servicios.

Consulte la documentación de vRealize Automation para obtener más detalles acerca de la importación de los metadatos.

## Servicio de token de seguridad (STS)

El servicio de token de seguridad (STS) de vCenter Single Sign-On es un servicio web que emite, valida y renueva los tokens de seguridad.

Los usuarios presentan sus credenciales principales a la interfaz de STS para adquirir tokens SAML. La credencial principal depende del tipo de usuario.

#### Usuario

Nombre de usuario y contraseña disponibles en un origen de identidad de vCenter Single Sign-On.

#### Usuario de la aplicación

Certificado válido.

El STS autentica al usuario en función de las credenciales principales y crea un token SAML que contiene los atributos del usuario. El STS firma el token SAML con su certificado de firma de STS y asigna el token al usuario. De forma predeterminada, VMCA genera el certificado de firma del STS. Puede reemplazar el certificado de firma predeterminado del STS desde vSphere Web Client. No reemplace el certificado de firma STS a menos que la directiva de seguridad de la empresa exija que se reemplacen todos los certificados.

Una vez que el usuario tiene un token SAML, este se envía como parte de las solicitudes HTTP del usuario, posiblemente a través de varios proxy. Únicamente el destinatario previsto (el proveedor de servicios) puede utilizar la información del token SAML.

## Generar un nuevo certificado de firma de STS en el dispositivo

Si quiere reemplazar el certificado de firma del servicio de token de seguridad (STS) de vCenter Single Sign-On predeterminado, tiene que generar un certificado nuevo y agregarlo al almacén de claves de Java. Este procedimiento explica los pasos en un dispositivo de implementación integrado o un dispositivo de Platform Services Controller externo.

**Nota** Este certificado es válido durante diez años y no es un certificado externo. No reemplace este certificado a menos que la directiva de seguridad de su empresa así lo exija.

Consulte [Generar un nuevo certificado de firma de STS en una instalación de Windows de vCenter](#) si está ejecutando una instalación de Windows de Platform Services Controller.

### Procedimiento

- 1 Cree un directorio de nivel superior para mantener el nuevo certificado y compruebe la ubicación del directorio.

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

- 2 Copie el archivo `certtool.cfg` en el nuevo directorio.

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

- 3 Abra una copia del archivo `certtool.cfg` y edítela para usar el nombre de host y la dirección IP de Platform Services Controller local.

El país es obligatorio y tiene que ser de dos caracteres, como se muestra en el siguiente ejemplo.

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

# Country is needed and has to be 2 characters
Country = US
```

```
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

#### 4 Genere la clave.

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

#### 5 Genere el certificado.

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

#### 6 Convierta el certificado al formato PK12.

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

#### 7 Agregue el certificado al almacén de claves de Java (JKS).

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

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

#### 8 Cuando se le solicite, escriba **sí** para aceptar el certificado en el almacén de claves.

#### Pasos siguientes

Ahora puede importar el certificado nuevo. Consulte [Actualizar el certificado del servicio de token de seguridad](#).

## Generar un nuevo certificado de firma de STS en una instalación de Windows de vCenter

Si quiere reemplazar el certificado de firma de STS predeterminado, tiene que generar primero un certificado nuevo y agregarlo al almacén de claves de Java. Este procedimiento explica los pasos en una instalación de Windows.

---

**Nota** Este certificado es válido durante diez años y no es un certificado externo. No reemplace este certificado a menos que la directiva de seguridad de su empresa así lo exija.

---

Consulte [Generar un nuevo certificado de firma de STS en el dispositivo](#) si está usando un dispositivo virtual.

## Procedimiento

- 1 Cree un nuevo directorio para alojar el nuevo certificado.

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

- 2 Realice una copia del archivo `certtool.cfg` y colóquela en el nuevo directorio.

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

- 3 Abra una copia del archivo `certtool.cfg` y edítela para usar el nombre de host y la dirección IP de Platform Services Controller local.

El país es obligatorio y tiene que ser de dos caracteres. Esto se muestra en el siguiente ejemplo.

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

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

- 4 Genere la clave.

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

- 5 Genere el certificado.

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

- 6 Convierta el certificado al formato PK12.

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

## 7 Agregue el certificado al almacén de claves de Java (JKS).

```
"C:\Program Files\VMware\VCenter Server\jre\bin\keytool.exe" -v -importkeystore
-srckeystore newsts.pl2 -srcstoretype pkcs12 -srcstorepass changeme -srcalias
newstssigning -destkeystore root-trust.jks -deststoretype JKS -deststorepass testpassword
-destkeypass testpassword
"C:\Program Files\VMware\VCenter Server\jre\bin\keytool.exe" -v -importcert -keystore
root-trust.jks -deststoretype JKS -storepass testpassword -keypass testpassword
-file ..\ssoserverRoot.crt -alias root-ca
```

### Pasos siguientes

Ahora puede importar el certificado nuevo. Consulte [Actualizar el certificado del servicio de token de seguridad](#).

## Actualizar el certificado del servicio de token de seguridad

El servidor vCenter Single Sign-On incluye un servicio de token de seguridad (STS). El STS es un servicio web que emite, valida y renueva los tokens de seguridad. Puede actualizar manualmente el certificado actual del STS en vSphere Web Client cuando el certificado caduque o se modifique.

Para adquirir un token SAML, un usuario presenta las credenciales principales ante el STS. Las credenciales principales dependen del tipo de usuario:

### Usuario de solución

Certificado válido

### Otros usuarios

Nombre de usuario y contraseña disponibles en un origen de identidad de vCenter Single Sign-On.

El STS autentica al usuario mediante las credenciales principales y crea un token SAML que contiene los atributos del usuario. El servicio STS firma el token SAML con su certificado de firma de STS y, a continuación, asigna el token a un usuario. De forma predeterminada, VMCA genera el certificado de firma del STS.

Una vez que el usuario tiene un token SAML, este se envía como parte de las solicitudes HTTP del usuario, posiblemente a través de varios proxy. Únicamente el destinatario previsto (el proveedor de servicios) puede utilizar la información del token SAML.

Es posible reemplazar el certificado de firma de STS actual de vSphere Web Client si la directiva de la empresa así lo requiere, o si se desea actualizar un certificado caducado.

---

**Precaución** No reemplace el archivo en el sistema de archivos. Si lo hace, se generarán errores inesperados y difíciles de depurar.

---

**Nota** Después de reemplazar el certificado, debe reiniciar el nodo para reiniciar los servicios STS y vSphere Web Client.

---

## Requisitos previos

Copie el certificado que acaba de agregar al almacén de claves de Java desde Platform Services Controller en la estación de trabajo local.

## Dispositivo Platform Services Controller

`certificate_location/keys/root-trust.jks` Por ejemplo: `/keys/root-trust.jks`

Por ejemplo:

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

## Instalación de Windows

`certificate_location\root-trust.jks`

Por ejemplo:

`C:\Archivos de programa\VMware\vCenter Server\jre\bin\root-trust.jks`

## Procedimiento

- 1 Inicie sesión en vSphere Web Client como `administrator@vsphere.local` u otro usuario con privilegios de administrador de vCenter Single Sign-On.  
  
Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio `vsphere.local`.
- 2 Seleccione la pestaña **Certificados**, la subpestaña **Firma de STS** y, a continuación, haga clic en el icono **Agregar certificado de firma de STS**.
- 3 Agregue el certificado.
  - a Haga clic en **Examinar** para desplazarse hasta el archivo JKS de almacenamiento de claves que contiene el nuevo certificado y haga clic en **Abrir**.
  - b Escriba la contraseña cuando se le solicite.
  - c Haga clic en la parte superior de la cadena de alias de STS y haga clic en **Aceptar**.
  - d Escriba la contraseña nuevamente cuando se le solicite.
- 4 Haga clic en **Aceptar**.
- 5 Reinicie el nodo de Platform Services Controller para iniciar tanto el servicio STS como vSphere Web Client.

Antes de reiniciar, la autenticación no funciona correctamente, por lo que es esencial que reinicie.

## Determinar la fecha de caducidad de un certificado SSL de LDAPS

Si selecciona un origen de identidad de servidor LDAP y OpenLDAP de Active Directory, y decide usar LDAPS, puede cargar un certificado SSL para el tráfico LDAP. Los certificados SSL caducan después de un tiempo predefinido. Si se conoce la fecha de caducidad de un certificado, se puede reemplazar o renovar el certificado antes de que caduque.

Solo puede ver la información de caducidad del certificado si utiliza un servidor LDAP u OpenLDAP de Active Directory, y si especifica una dirección URL **ldaps://** URL para el servidor. La pestaña TrustStore de orígenes de identidad permanece vacía para los demás tipos de orígenes de identidad o para el tráfico **ldap://**.

#### Procedimiento

- 1 Inicie sesión en vSphere Web Client como administrator@vsphere.local u otro usuario con privilegios de administrador de vCenter Single Sign-On.  
  
Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio vsphere.local.
- 2 Desplácese hasta **Administración > Single Sign-On > Configuración**.
- 3 Haga clic en la pestaña **Certificados** y después en la subpestaña **TrustStore de orígenes de identidad**.
- 4 Busque el certificado y compruebe la fecha de caducidad en el cuadro de texto **Válida hasta**.  
  
Es posible que vea una advertencia en la parte superior de la pestaña que indica que un certificado está por caducar.

## Administrar directivas de vCenter Single Sign-On

Las directivas de vCenter Single Sign-On aplican las reglas de seguridad en el entorno. Puede ver y editar los valores predeterminados de las contraseñas, las directivas de bloqueo y las directivas de token de vCenter Single Sign-On.

### Editar la directiva de contraseñas de vCenter Single Sign-On

La directiva de contraseñas de vCenter Single Sign-On es un conjunto de reglas y restricciones sobre el formato y la caducidad de las contraseñas de usuario de vCenter Single Sign-On. La directiva de contraseñas se aplica solo a los usuarios del dominio vCenter Single Sign-On (vsphere.local).

De forma predeterminada, las contraseñas de vCenter Single Sign-On caducan a los 90 días. vSphere Web Client recuerda al usuario cuando la contraseña está a punto de caducar.

#### Procedimiento

- 1 Inicie sesión en vSphere Web Client como administrator@vsphere.local u otro usuario con privilegios de administrador de vCenter Single Sign-On.  
  
Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio vsphere.local.
- 2 Desplácese hasta **Administración > Single Sign-On > Configuración**.
- 3 Haga clic en la pestaña **Directivas** y seleccione **Directivas de contraseñas**.
- 4 Haga clic en **Editar**.



## 5 Edite los parámetros de directivas de contraseñas.

Opción	Descripción
Descripción	Descripción de directivas de contraseñas.
Duración máxima	Cantidad máxima de días de vigencia de la contraseña, antes de que el usuario deba cambiarla.
Reutilización restringida	Cantidad de contraseñas anteriores del usuario que no pueden seleccionarse. Por ejemplo, si un usuario no puede reutilizar ninguna de las últimas seis contraseñas, escriba 6.
Longitud máxima	Cantidad máxima de caracteres que se permiten en la contraseña.
Longitud mínima	Cantidad mínima de caracteres que se requiere en la contraseña. La longitud mínima no debe ser inferior a la cantidad mínima requerida de caracteres alfabéticos, numéricos y especiales combinados.
Requisitos de caracteres	<p>Cantidad mínima de tipos de caracteres diferentes que se requieren en la contraseña. Puede especificar la cantidad de caracteres de cada tipo de la siguiente manera:</p> <ul style="list-style-type: none"> <li>■ Especiales: &amp; # %</li> <li>■ Alfabéticos: A b c D</li> <li>■ Mayúsculas: A B C</li> <li>■ Minúsculas: a b c</li> <li>■ Numéricos: 1 2 3</li> </ul> <p>La cantidad mínima de caracteres alfabéticos no debe ser inferior a la cantidad requerida de mayúsculas y minúsculas combinadas.</p> <p>En vSphere 6.0 y versiones posteriores, las contraseñas admiten caracteres no ASCII. En versiones anteriores de vCenter Single Sign-On, hay limitaciones en los caracteres admitidos.</p>
Caracteres adyacentes idénticos	Cantidad máxima de caracteres adyacentes idénticos que se permiten en la contraseña. El número debe ser superior a 0. Por ejemplo, si escribe 1, la siguiente contraseña no se permite: p@\$\$word.

## 6 Haga clic en **Aceptar**.

## Editar la directiva de bloqueo de vCenter Single Sign-On

La directiva de bloqueo de vCenter Single Sign-On especifica las condiciones en las cuales se bloquea la cuenta de vCenter Single Sign-On de un usuario cuando intenta iniciar sesión con las credenciales equivocadas. La directiva de bloqueo puede editarse.

Si un usuario inicia sesión varias veces en vsphere.local con la contraseña incorrecta, su cuenta se bloqueará. La directiva de bloqueo permite especificar la cantidad máxima de intentos fallidos de inicio de sesión y el tiempo que puede transcurrir entre un error y otro. En la directiva también se especifica cuánto tiempo debe transcurrir antes de que la cuenta se desbloquee automáticamente.

**Nota** La directiva de bloqueo se aplica únicamente a las cuentas de usuario, no a las cuentas de sistema, como administrator@vsphere.local.

**Procedimiento**

- 1 Inicie sesión en vSphere Web Client como `administrator@vsphere.local` u otro usuario con privilegios de administrador de vCenter Single Sign-On.

Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio `vsphere.local`.

- 2 Desplácese hasta **Administración > Single Sign-On > Configuración**.
- 3 Haga clic en la pestaña **Directivas** y seleccione **Directiva de bloqueo**.
- 4 Haga clic en **Editar**.
- 5 Edite los parámetros.

Opción	Descripción
Descripción	Descripción opcional de la directiva de bloqueo.
Cantidad máxima de intentos fallidos de inicio de sesión	Cantidad máxima de intentos fallidos de inicio de sesión permitidos antes de que la cuenta se bloquee.
Intervalo entre errores	Período en el cual deben ocurrir los intentos fallidos de inicio de sesión para activar un bloqueo.
Tiempo de desbloqueo	Cantidad de tiempo durante la cual permanece bloqueada la cuenta. Si introduce 0, el administrador debe desbloquear la cuenta explícitamente.

- 6 Haga clic en **Aceptar**.

## Editar la directiva de tokens de vCenter Single Sign-On

La directiva de tokens de vCenter Single Sign-On especifica la tolerancia de reloj, el recuento de renovaciones y otras propiedades de tokens. Puede editar la directiva de tokens de vCenter Single Sign-On para que la especificación de los tokens se adapte a los estándares de seguridad de la empresa.

**Procedimiento**

- 1 Inicie sesión en vSphere Web Client.
- 2 Seleccione **Administración > Single Sign-On** y, a continuación, seleccione **Configuración**.
- 3 Haga clic en la pestaña **Directivas** y seleccione **Directiva de tokens**.

vSphere Web Client muestra las opciones de la configuración actual. vCenter Single Sign-On utiliza la configuración predeterminada si esta no se modificó.

#### 4 Edite los parámetros de configuración de la directiva de tokens.

Opción	Descripción
<b>Tolerancia de reloj</b>	Diferencia horaria, en milisegundos, que vCenter Single Sign-On tolera entre un reloj de cliente y el reloj de la controladora de dominio. Si la diferencia horaria es mayor que el valor especificado, vCenter Single Sign-On declara al token como no válido.
<b>Recuento máximo de renovaciones de token</b>	Es la máxima cantidad de veces que puede renovarse un token. Una vez alcanzada la cantidad máxima de intentos de renovación, se requiere un nuevo token de seguridad.
<b>Recuento máximo de delegaciones de token</b>	Los tokens HoK (Holder-of-key) pueden delegarse a servicios del entorno vSphere. Un servicio que emplea un token delegado ejecuta dicho servicio en nombre del servicio principal que proporcionó el token. La solicitud de un token especifica una identidad DelegateTo. El valor de DelegateTo puede ser el token de una solución o una referencia al token de la solución. Este valor especifica cuántas veces puede delegarse un mismo token HoK.
<b>Duración máxima de token de portador</b>	Los tokens de portador proporcionan autenticación basada únicamente en la posesión del token. Los tokens de portador están pensados para el uso a corto plazo y para una única operación. El token de portador no comprueba la identidad del usuario o de la entidad que envía la solicitud. Este valor especifica la duración del token de portador antes de que el token deba emitirse nuevamente.
<b>Duración máxima de token HoK</b>	<p>Los tokens HoK proporcionan autenticación basada en los artefactos de seguridad que están integrados en el token. Los tokens HoK pueden usarse para operaciones de delegación. Un cliente puede obtener un token HoK y delegarlo a otra entidad. El token contiene las notificaciones para identificar al originador y al delegado. En el entorno vSphere, un sistema vCenter Server obtiene tokens delegados en nombre de un usuario y los utiliza para realizar operaciones.</p> <p>Este valor determina la duración de un token HoK antes de que el token se marque como no válido.</p>

#### 5 Haga clic en **Aceptar**.

## Administrar usuarios y grupos de vCenter Single Sign-On

Un usuario administrador de vCenter Single Sign-On puede administrar usuarios y grupos en el dominio vsphere.local desde vSphere Web Client.

El usuario administrador de vCenter Single Sign-On puede realizar las siguientes tareas.

- [Agregar usuarios de vCenter Single Sign-On](#)

Los usuarios que aparecen en la pestaña **Usuarios** en vSphere Web Client son internos de vCenter Single Sign-On y pertenecen al dominio vsphere.local.

- [Deshabilitar y habilitar usuarios de vCenter Single Sign-On](#)

Cuando una cuenta de usuario de vCenter Single Sign-On está deshabilitada, el usuario no puede iniciar sesión en el servidor vCenter Single Sign-On hasta que un administrador la habilite. Puede deshabilitar y habilitar usuarios desde la interfaz de vSphere Web Client.

- **Eliminar un usuario de vCenter Single Sign-On**

Puede eliminar usuarios que se encuentran en el dominio vsphere.local desde vCenter Single Sign-On. No puede eliminar usuarios del sistema operativo local ni usuarios de otro dominio desde vSphere Web Client.

- **Editar un usuario de vCenter Single Sign-On**

Puede cambiar la contraseña u otros detalles de un usuario de vCenter Single Sign-On desde vSphere Web Client. No puede cambiar el nombre de los usuarios en el dominio vsphere.local. Esto significa que no puede cambiar el nombre de administrator@vsphere.local.

- **Agregar un grupo de vCenter Single Sign-On**

En vCenter Single Sign-On, los grupos se enumeran en la pestaña **Grupos** y son internos de vCenter Single Sign-On. Un grupo permite crear un contenedor para una recopilación de miembros de grupo (entidades de seguridad).

- **Agregar miembros a un grupo de vCenter Single Sign-On**

Los miembros de un grupo de vCenter Single Sign-On pueden ser usuarios u otros grupos de uno o más orígenes de identidad. Puede agregar miembros nuevos de vSphere Web Client.

- **Quitar miembros de un grupo de vCenter Single Sign-On**

Es posible eliminar miembros de un grupo de vCenter Single Sign-On de vSphere Web Client. Al eliminar un miembro (usuario o grupo) de un grupo local, el miembro no se elimina del sistema.

- **Eliminar usuarios de solución vCenter Single Sign-On**

vCenter Single Sign-On muestra a los usuarios de solución. Un usuario de solución es una recopilación de servicios. Como parte de la instalación, se definen de forma previa varios usuarios de solución vCenter Server que se autentican en vCenter Single Sign-On. En situaciones de solución de problemas, por ejemplo, si no se completó correctamente una desinstalación, es posible eliminar usuarios individuales de la solución desde vSphere Web Client.

- **Cambiar la contraseña de vCenter Single Sign-On**

Los usuarios del dominio local, vsphere.local de forma predeterminada, pueden cambiar las contraseñas de vCenter Single Sign-On desde una interfaz web. Los usuarios de otros dominios pueden cambiar la contraseña mediante las reglas de ese dominio.

## Agregar usuarios de vCenter Single Sign-On

Los usuarios que aparecen en la pestaña **Usuarios** en vSphere Web Client son internos de vCenter Single Sign-On y pertenecen al dominio vsphere.local.

Puede seleccionar otros dominios y ver en ellos información sobre los usuarios, pero lo que no puede hacer es agregar usuarios a otros dominios desde la interfaz de administración de vCenter Single Sign-On de vSphere Web Client.

## Procedimiento

- 1 Inicie sesión en vSphere Web Client como `administrator@vsphere.local` u otro usuario con privilegios de administrador de vCenter Single Sign-On.

Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio `vsphere.local`.

- 2 Haga clic en **Inicio** y desplácese hasta **Administración > Single Sign-On > Usuarios y grupos**.

- 3 Si el dominio actualmente seleccionado no es `vsphere.local`, selecciónelo en el menú desplegable.

No puede agregar usuarios a otros dominios.

- 4 En la pestaña **Usuarios**, haga clic en el icono **Usuario nuevo**.

- 5 Escriba un nombre de usuario y una contraseña para el usuario nuevo.

No puede cambiar el nombre de usuario una vez creado el usuario.

La contraseña debe cumplir con los requisitos de la directiva de contraseñas del sistema.

- 6 (opcional) Escriba el nombre de pila y el apellido del usuario nuevo.

- 7 (opcional) Introduzca una dirección de correo electrónico y una descripción del usuario.

- 8 Haga clic en **Aceptar**.

## Resultados

Cuando agrega un usuario, este en principio no tiene privilegios para realizar operaciones de administración.

## Pasos siguientes

Agregue el usuario a un grupo del dominio `vsphere.local`, por ejemplo, al grupo de usuarios que pueden administrar VMCA (Administradores de CA) o al grupo de usuarios que pueden administrar vCenter Single Sign-On (Administrators). Consulte [Agregar miembros a un grupo de vCenter Single Sign-On](#).

## Deshabilitar y habilitar usuarios de vCenter Single Sign-On

Cuando una cuenta de usuario de vCenter Single Sign-On está deshabilitada, el usuario no puede iniciar sesión en el servidor vCenter Single Sign-On hasta que un administrador la habilite. Puede deshabilitar y habilitar usuarios desde la interfaz de vSphere Web Client.

Las cuentas de usuario deshabilitadas permanecen disponibles en el sistema vCenter Single Sign-On, pero el usuario no puede iniciar sesión ni realizar operaciones en el servidor. Los usuarios con privilegios de administrador pueden deshabilitar y habilitar usuarios desde la página de usuarios y grupos de vCenter.

## Requisitos previos

Debe ser miembro del grupo de administradores de vCenter Single Sign-On para deshabilitar y habilitar usuarios de vCenter Single Sign-On.

## Procedimiento

- 1 Inicie sesión en vSphere Web Client como `administrator@vsphere.local` u otro usuario con privilegios de administrador de vCenter Single Sign-On.  
  
Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio `vsphere.local`.
- 2 Haga clic en **Inicio** y desplácese hasta **Administración > Single Sign-On > Usuarios y grupos**.
- 3 Seleccione un usuario, haga clic en el icono **Deshabilitar** y, a continuación, haga clic en **Sí** cuando el sistema se lo indique.
- 4 Para habilitar el usuario de nuevo, haga clic con el botón derecho en el usuario, seleccione **Habilitar** y haga clic en **Sí** cuando el sistema se lo indique.

## Eliminar un usuario de vCenter Single Sign-On

Puede eliminar usuarios que se encuentran en el dominio `vsphere.local` desde vCenter Single Sign-On. No puede eliminar usuarios del sistema operativo local ni usuarios de otro dominio desde vSphere Web Client.

---

**Precaución** Si elimina el usuario administrador del dominio `vsphere.local`, ya no podrá iniciar sesión en vCenter Single Sign-On. Reinstale vCenter Server y sus componentes.

---

## Procedimiento

- 1 Inicie sesión en vSphere Web Client como `administrator@vsphere.local` u otro usuario con privilegios de administrador de vCenter Single Sign-On.  
  
Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio `vsphere.local`.
- 2 Haga clic en **Inicio** y desplácese hasta **Administración > Single Sign-On > Usuarios y grupos**.
- 3 Seleccione la pestaña **Usuarios** y seleccione el dominio `vsphere.local`.
- 4 En la lista de usuarios, seleccione el usuario que desea eliminar y haga clic en el icono **Eliminar**.

Proceda con precaución: esta acción no se puede deshacer.

## Editar un usuario de vCenter Single Sign-On

Puede cambiar la contraseña u otros detalles de un usuario de vCenter Single Sign-On desde vSphere Web Client. No puede cambiar el nombre de los usuarios en el dominio `vsphere.local`. Esto significa que no puede cambiar el nombre de `administrator@vsphere.local`.

Puede crear usuarios adicionales con los mismos privilegios de `administrator@vsphere.local`.

Los usuarios de vCenter Single Sign-On se almacenan en el dominio vsphere.local de vCenter Single Sign-On.

Puede revisar las directivas sobre contraseñas de vCenter Single Sign-On desde vSphere Web Client. Inicie sesión como administrator@vsphere.local y seleccione **Configuración > Directivas > Directivas de contraseñas**.

#### Procedimiento

- 1 Inicie sesión en vSphere Web Client como administrator@vsphere.local u otro usuario con privilegios de administrador de vCenter Single Sign-On.

Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio vsphere.local.

- 2 Haga clic en **Inicio** y desplácese hasta **Administración > Single Sign-On > Usuarios y grupos**.
- 3 Haga clic en la pestaña **Usuarios**.
- 4 Haga clic con el botón derecho en el usuario y seleccione **Editar usuario**.
- 5 Realice los cambios en el usuario.

No puede cambiar el nombre de usuario.

La contraseña debe cumplir con los requisitos de la directiva de contraseñas del sistema.

- 6 Haga clic en **Aceptar**.

## Agregar un grupo de vCenter Single Sign-On

En vCenter Single Sign-On, los grupos se enumeran en la pestaña **Grupos** y son internos de vCenter Single Sign-On. Un grupo permite crear un contenedor para una recopilación de miembros de grupo (entidades de seguridad).

Cuando se agrega un grupo de vCenter Single Sign-On desde la interfaz de administración de vSphere Web Client, el grupo se agrega al dominio vsphere.local.

#### Procedimiento

- 1 Inicie sesión en vSphere Web Client como administrator@vsphere.local u otro usuario con privilegios de administrador de vCenter Single Sign-On.

Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio vsphere.local.

- 2 Haga clic en **Inicio** y desplácese hasta **Administración > Single Sign-On > Usuarios y grupos**.
- 3 Seleccione la pestaña **Grupos** y haga clic en el icono **Nuevo grupo**.
- 4 Introduzca un nombre y una descripción para el grupo.  
No puede cambiar el nombre de grupo una vez creado el grupo.
- 5 Haga clic en **Aceptar**.

**Pasos siguientes**

- Agregue miembros al grupo.

**Agregar miembros a un grupo de vCenter Single Sign-On**

Los miembros de un grupo de vCenter Single Sign-On pueden ser usuarios u otros grupos de uno o más orígenes de identidad. Puede agregar miembros nuevos de vSphere Web Client.

Puede agregar miembros de grupos de Microsoft Active Directory u OpenLDAP a un grupo de vCenter Single Sign-On. No puede agregar grupos de orígenes de identidad externos a un grupo de vCenter Single Sign-On.

Los grupos que se enumeran en la pestaña **Grupos** de vSphere Web Client son parte del dominio local vsphere.local. Consulte [Grupos del dominio vsphere.local](#).

**Procedimiento**

- 1 Inicie sesión en vSphere Web Client como administrator@vsphere.local u otro usuario con privilegios de administrador de vCenter Single Sign-On.  
  
Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio vsphere.local.
- 2 Haga clic en **Inicio** y desplácese hasta **Administración > Single Sign-On > Usuarios y grupos**.
- 3 Haga clic en la pestaña **Grupos** y, a continuación, en el grupo (por ejemplo, Administrators).
- 4 En el área Miembros del grupo, haga clic en el icono **Agregar miembros**.
- 5 Seleccione el origen de identidad que contenga el miembro que se va a agregar al grupo.
- 6 (opcional) Introduzca un término de búsqueda y haga clic en **Buscar**.
- 7 Seleccione el miembro y haga clic en **Agregar**.  
  
Puede agregar varios miembros a la vez.
- 8 Haga clic en **Aceptar**.

**Quitar miembros de un grupo de vCenter Single Sign-On**

Es posible eliminar miembros de un grupo de vCenter Single Sign-On de vSphere Web Client. Al eliminar un miembro (usuario o grupo) de un grupo local, el miembro no se elimina del sistema.

**Procedimiento**

- 1 Inicie sesión en vSphere Web Client como administrator@vsphere.local u otro usuario con privilegios de administrador de vCenter Single Sign-On.  
  
Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio vsphere.local.
- 2 Haga clic en **Inicio** y desplácese hasta **Administración > Single Sign-On > Usuarios y grupos**.
- 3 Seleccione la pestaña **Grupos** y haga clic en el grupo.



- 4 En la lista de miembros de grupo, seleccione el usuario o el grupo que desea eliminar y, a continuación, haga clic en el icono **Eliminar miembro**.
- 5 Haga clic en **Aceptar**.

#### Resultados

El usuario se elimina del grupo, pero sigue disponible en el sistema.

## Eliminar usuarios de solución vCenter Single Sign-On

vCenter Single Sign-On muestra a los usuarios de solución. Un usuario de solución es una recopilación de servicios. Como parte de la instalación, se definen de forma previa varios usuarios de solución vCenter Server que se autentican en vCenter Single Sign-On. En situaciones de solución de problemas, por ejemplo, si no se completó correctamente una desinstalación, es posible eliminar usuarios individuales de la solución desde vSphere Web Client.

Cuando se elimina el conjunto de servicios asociados con un usuario de solución vCenter Server o un usuario de una solución externa desde el entorno, el usuario de solución se elimina de la pantalla de vSphere Web Client. Si se elimina una aplicación de manera forzosa, o si no se puede recuperar el sistema mientras el usuario de solución sigue en el sistema, es posible eliminar el usuario de solución explícitamente desde vSphere Web Client.

---

**Importante** Si se elimina un usuario de solución, los servicios correspondientes ya no se pueden autenticar en vCenter Single Sign-On.

---

#### Procedimiento

- 1 Inicie sesión en vSphere Web Client como `administrator@vsphere.local` u otro usuario con privilegios de administrador de vCenter Single Sign-On.  
  
Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo de administradores del dominio `vsphere.local`.
- 2 Haga clic en **Inicio** y desplácese hasta **Administración > Single Sign-On > Usuarios y grupos**.
- 3 Haga clic en la pestaña **Usuarios de la solución** y seleccione el nombre de un usuario de solución.
- 4 Haga clic en el icono **Eliminar usuario de solución**.
- 5 Haga clic en **Sí**.

#### Resultados

Los servicios asociados con el usuario de solución ya no tendrán acceso a vCenter Server y no podrán funcionar como servicios de vCenter Server.

## Cambiar la contraseña de vCenter Single Sign-On

Los usuarios del dominio local, `vsphere.local` de forma predeterminada, pueden cambiar las contraseñas de vCenter Single Sign-On desde una interfaz web. Los usuarios de otros dominios pueden cambiar la contraseña mediante las reglas de ese dominio.

La directiva de bloqueo de vCenter Single Sign-On determina el momento en que caduca la contraseña. De forma predeterminada, las contraseñas de usuario de vCenter Single Sign-On caducan a los 90 días, pero las contraseñas de administrador, como la de `administrator@vsphere.local`, no caducan. Las interfaces de administración de vCenter Single Sign-On muestran una advertencia cuando la contraseña está por caducar.

---

**Nota** Solo puede cambiar una contraseña si no ha caducado.

---

Si la contraseña ha caducado, el administrador del dominio local, `administrator@vsphere.local` de forma predeterminada, puede restablecerla mediante el comando `dir-cli password reset`. Solo pueden restablecer contraseñas los miembros del grupo Administrador para el dominio de vCenter Single Sign-On.

### Procedimiento

- 1 En un explorador web, especifique la siguiente dirección URL para conectarse a Platform Services Controller:

**`https://psc_hostname_or_IP/psc`**

En una implementación integrada, el nombre de host o la dirección IP de Platform Services Controller es igual al nombre de host o la dirección IP de vCenter Server.

- 2 Especifique el nombre de usuario y la contraseña para `administrator@vsphere.local` u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como `administrator@mydomain`.

- 3 En el panel de navegación superior, a la izquierda del menú Ayuda, haga clic en su nombre de usuario para desplegar el menú.

Otra opción es seleccionar **Single Sign-On > Usuarios y grupos** y, a continuación, seleccionar **Editar usuario** desde el menú contextual.

- 4 Seleccione **Cambiar contraseña** y escriba la contraseña actual.

- 5 Escriba la nueva contraseña y confírmela.

La contraseña debe cumplir con la directiva de contraseñas.

- 6 Haga clic en **Aceptar**.

## Prácticas recomendadas de seguridad de vCenter Single Sign-On

Siga las prácticas recomendadas de seguridad de vCenter Single Sign-On para proteger el entorno de vSphere.

La infraestructura de autenticación y certificados de vSphere 6.0 optimiza la seguridad del entorno de vSphere. Para garantizar que la confiabilidad de la infraestructura no se vea comprometida, siga las prácticas recomendadas de vCenter Single Sign-On.

### Compruebe la caducidad de las contraseñas

La directiva predeterminada de contraseñas de vCenter Single Sign-On establece una duración de 90 días para las contraseñas. Una vez transcurridos los 90 días, la contraseña caduca y la capacidad de registro queda comprometida. Compruebe la fecha de caducidad y actualice las contraseñas oportunamente.

### Configure NTP

Compruebe que todos los sistemas tengan el mismo origen de hora relativo (incluida la correspondiente compensación por localización), y que este pueda ser correlativo con una hora estándar acordada (como la hora universal coordinada, UTC). La sincronización de los sistemas es fundamental para la validez de los certificados de vCenter Single Sign-On y de otros certificados de vSphere.

NTP también facilita el rastreo de intrusos en los archivos de registro. Una configuración incorrecta de la hora puede dificultar la inspección y la correlación de los archivos de registro a fin de detectar ataques; también puede hacer imprecisas las auditorías.

## Solucionar problemas en vCenter Single Sign-On

La configuración de vCenter Single Sign-On puede ser un proceso complejo.

Los siguientes temas ofrecen un punto de partida para la solución de problemas en vCenter Single Sign-On. Para más información, busque en este centro de documentación y en la base de conocimientos de VMware.

### Determinar la causa de un error de Lookup Service

La instalación de vCenter Single Sign-On muestra un error relacionado con vCenter Server o vSphere Web Client.

#### Problema

Los instaladores de vCenter Server y Web Client muestran el error `No se pudo establecer contacto con Lookup Service. Revise VM_ssoreg.log....`

## Causa

Este problema tiene varias causas, como relojes no sincronizados en los equipos host, bloqueos de firewall y servicios que deben iniciarse.

## Solución

- 1 Compruebe que los relojes de los equipos host que ejecutan vCenter Single Sign-On, vCenter Server y Web Client estén sincronizados.
- 2 Vea el archivo de registro específico que se encuentra en el mensaje de error.

En el mensaje, la carpeta temporal del sistema hace referencia a %TEMP%.

- 3 En el archivo de registro, busque los siguientes mensajes.

El archivo de registro contiene una salida de todos los intentos de instalación. Busque el último mensaje que muestra `Initializing registration provider...`

Mensaje	Causa y solución
<b>java.net.ConnectException: Connection timed out: connect</b>	<p>La dirección IP es incorrecta, hay un firewall bloqueando el acceso a vCenter Single Sign-On o vCenter Single Sign-On está sobrecargado.</p> <p>Asegúrese de que no haya un firewall bloqueando el puerto de vCenter Single Sign-On (de forma predeterminada, 7444) y que el equipo en el que está instalado vCenter Single Sign-On tenga capacidad libre de CPU, E/S y RAM.</p>
<b>java.net.ConnectException: Connection refused: connect</b>	<p>La dirección IP o el FQDN son incorrectos y el servicio vCenter Single Sign-On no se inició o se inició dentro del último minuto.</p> <p>Compruebe que vCenter Single Sign-On funcione. Para ello, consulte el estado del servicio vCenter Single Sign-On (Windows) y el daemon vmware-ssso (Linux).</p> <p>Reinicie el servicio. Si esto no soluciona el problema, consulte la sección de recuperación de la guía de solución de problemas de vSphere.</p>
<b>Unexpected status code: 404. SSO Server failed during initialization</b>	<p>Reinicie vCenter Single Sign-On. Si esto no soluciona el problema, consulte la sección sobre recuperación de la <i>Guía de solución de problemas de vSphere</i>.</p>
<b>El error que se muestra en la interfaz del usuario comienza con Could not connect to vCenter Single Sign-on.</b>	<p>También se observa el código de retorno <code>SslHandshakeFailed</code>. Este error no es común. Indica que la dirección IP o el FQDN proporcionados que se resuelven en el host de vCenter Single Sign-On no son los que se usaron cuando se instaló vCenter Single Sign-On.</p> <p>En %TEMP%\VM_ssoreg.log, busque la línea que contiene el siguiente mensaje.</p> <pre>host name in certificate did not match: &lt;install-configured FQDN or IP&gt; != &lt;A&gt; o &lt;B&gt; o &lt;C&gt; donde A era el FQDN que se introdujo durante la instalación de vCenter Single Sign-On, y B y C eran las alternativas permitidas generadas por el sistema.</pre> <p>Corrija la configuración para utilizar el FQDN a la derecha del signo != del archivo de registro. En la mayoría de los casos, utilice el FQDN que especificó durante la instalación de vCenter Single Sign-On.</p> <p>Si ninguna de las alternativas es posible en la configuración de la red, recupere la configuración de SSL de vCenter Single Sign-On.</p>

## No se puede iniciar sesión con la autenticación del dominio de Active Directory

Se inicia sesión en un componente de vCenter Server desde vSphere Web Client. Se utiliza el nombre de usuario y la contraseña de Active Directory. Se produce un error en la autenticación.

### Problema

Se agrega el origen de identidad de Active Directory a vCenter Single Sign-On, pero los usuarios no pueden iniciar sesión en vCenter Server.

### Causa

Los usuarios utilizan su nombre de usuario y contraseña para iniciar sesión en el dominio predeterminado. Para los demás dominios, los usuarios deben incluir el nombre de dominio (usuario@dominio o DOMINIO\usuario).

Si está utilizando vCenter Server Appliance, es posible que se produzcan otros problemas.

### Solución

En todas las implementaciones de vCenter Single Sign-On, se puede cambiar el origen de identidad predeterminado. Después de ese cambio, los usuarios pueden iniciar sesión en el origen de identidad predeterminado únicamente con el nombre de usuario y la contraseña.

Para configurar un origen de identidad para Autenticación de Windows integrada con un dominio secundario dentro del bosque de Active Directory, consulte el artículo [2070433](#) de la base de conocimientos de VMware. De forma predeterminada, la autenticación integrada de Windows utiliza el dominio raíz del bosque de Active Directory.

Si utiliza vCenter Server Appliance y el cambio del origen de identidad predeterminado no soluciona el problema, siga estos pasos adicionales de solución de problemas.

- 1 Sincronice los relojes entre vCenter Server Appliance y las controladoras de dominio de Active Directory.
- 2 Compruebe que cada controladora de dominio tenga un registro de marcador (PTR) en el servicio DNS del dominio de Active Directory y que la información de registro de PTR coincida con el nombre DNS de la controladora. Al utilizar vCenter Server Appliance, puede ejecutar los siguientes comandos para realizar la tarea:
  - a Para enumerar las controladoras de dominio, ejecute el comando siguiente:

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

Las direcciones relevantes aparecen en la sección de respuestas, como en el ejemplo siguiente:

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

- b Para cada controladora de dominio, compruebe la resolución de nombres en las direcciones IP (conocida como forward) y la resolución inversa mediante el comando siguiente:

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

Las direcciones relevantes aparecen en la sección de respuestas, como en el ejemplo siguiente:

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

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

Las direcciones relevantes aparecen en la sección de respuestas, como en el ejemplo siguiente:

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

- 3 Si esto no soluciona el problema, quite vCenter Server Appliance del dominio de Active Directory y vuelva a asociar el dominio. Consulte la documentación de *Configuración de vCenter Server Appliance*.
- 4 Cierre todas las sesiones del explorador que estén conectadas a vCenter Server Appliance y reinicie los servicios.

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

## Se produce un error en el inicio de sesión en vCenter Server porque la cuenta de usuario está bloqueada

Al iniciar sesión en vCenter Server desde la página de inicio de sesión de vSphere Web Client, un error indica que la cuenta está bloqueada.

### Problema

Después de varios intentos con errores, no puede iniciar sesión en vSphere Web Client mediante vCenter Single Sign-On. Aparece un mensaje que indica que la cuenta está bloqueada.

### Causa

Se supera la cantidad máxima de intentos de inicio de sesión con errores.

### Solución

- ◆ Si inicia sesión como usuario desde el dominio del sistema (vsphere.local), solicítele al administrador de vCenter Single Sign-On que desbloquee la cuenta. O bien puede esperar hasta que la cuenta se desbloquee si el bloqueo está configurado para caducar en la directiva de contraseñas. Los administradores de vCenter Single Sign-On pueden utilizar los comandos de CLI para desbloquear la cuenta.
- ◆ Si inicia sesión como usuario desde el dominio de Active Directory o de LDAP, solicítele al administrador de Active Directory o LDAP que desbloquee la cuenta.

## La replicación de VMware Directory Service puede tardar mucho

Si el entorno incluye varias instancias de Platform Services Controller, y si una de las instancias de Platform Services Controller deja de estar disponible, el entorno continúa funcionando. Cuando Platform Services Controller vuelve a estar disponible, se suelen replicar los datos del usuario y demás información en un plazo de 60 segundos. Sin embargo, ante algunas circunstancias especiales, la replicación puede tardar mucho.

### Problema

En ciertas situaciones, por ejemplo, cuando el entorno incluye varias instancias de Platform Services Controller en diferentes ubicaciones, y se realizan cambios significativos mientras una instancia de Platform Services Controller no está disponible, no se ve de inmediato la replicación en todas las instancias de VMware Directory Service. Por ejemplo, el usuario nuevo que se agregó a la instancia disponible de Platform Services Controller no se puede ver en la otra instancia hasta que la replicación está completa.

### Causa

En condiciones de funcionamiento normal, los cambios que se realizan en la instancia de VMware Directory Service (vmdir) en una instancia de Platform Services Controller (nodo) aparecen en su partner de replicación directo en un plazo de 60 segundos. Según la topología de la replicación, es posible que los cambios realizados en un nodo deban propagarse por nodos intermedios antes de llegar a cada instancia de vmdir en cada nodo. La información que se replica incluye información del usuario, de certificados, de licencias para máquinas virtuales creadas, clonadas o migradas con VMware VMotion, entre otras.

Cuando se rompe el vínculo de replicación, por ejemplo, debido a una interrupción de la red o porque un nodo dejó de estar disponible, los cambios en la federación no convergen. Una vez que se restaura el nodo no disponible, cada nodo intenta actualizarse con todos los cambios. Finalmente, todas las instancias de vmdir convergen en un estado coherente, pero puede llevar un tiempo alcanzar ese estado si se produjeron muchos cambios mientras un nodo no estaba disponible.

### Solución

El entorno funciona con normalidad mientras se lleva a cabo la replicación. No intente resolver el problema a menos que persista durante más de una hora.

# Certificados de seguridad de vSphere

## 3

Los componentes de vSphere utilizan SSL para comunicarse de forma segura entre sí y con ESXi. Las comunicaciones SSL garantizan la confidencialidad y la integridad de los datos. Los datos están protegidos y no se pueden modificar cuando están en tránsito sin que esto se detecte.

Los servicios de vCenter Server también utilizan certificados, como vSphere Web Client para la autenticación inicial en vCenter Single Sign-On. vCenter Single Sign-On aprovisiona cada componente con un token SAML que el componente utiliza para la autenticación de ahora en adelante.

En vSphere 6.0 y posteriores, VMware Certificate Authority (VMCA) aprovisiona cada host ESXi y cada servicio de vCenter Server con un certificado firmado por VMCA de forma predeterminada.

Es posible reemplazar los certificados existentes por certificados nuevos firmados por VMCA, convertir a VMCA en una entidad de certificación subordinada, o bien reemplazar todos los certificados por certificados personalizados. Existen varias opciones:

**Tabla 3-1. Diferentes enfoques de reemplazo de certificados**

Opción	Consulte
Utilice la interfaz web de Platform Services Controller (vSphere 6.0 Update 1 y posteriores).	<a href="#">Administrar certificados con la interfaz web de Platform Services Controller</a>
Ejecute la utilidad vSphere Certificate Manager desde la línea de comandos.	<a href="#">Administrar certificados con la utilidad vSphere Certificate Manager</a>
Utilice los comandos de la CLI para el reemplazo manual de certificados.	<a href="#">Administrar certificados y servicios con comandos de CLI</a>



Administración de certificados de vSphere

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

Este capítulo incluye los siguientes temas:

- [Requisitos de certificados para distintas rutas de acceso de la solución](#)
- [Descripción general de la administración de certificados](#)
- [Administrar certificados con la interfaz web de Platform Services Controller](#)
- [Administrar certificados con la utilidad vSphere Certificate Manager](#)



- Reemplazar certificados de forma manual
- Administrar certificados y servicios con comandos de CLI
- Ver certificados de vCenter con vSphere Web Client
- Establecer el umbral para las advertencias de caducidad de certificados de vCenter

## Requisitos de certificados para distintas rutas de acceso de la solución

Los requisitos de certificados dependen de si se usa VMCA como entidad de certificación intermedia o si se usan certificados personalizados. Los requisitos también son diferentes para los certificados de máquina y los certificados de usuario de solución.

Antes de comenzar, asegúrese de que la hora de todos los nodos del entorno esté sincronizada.

### Requisitos para todos los certificados importados

- Tamaño de clave: 2.048 bits o más (formato codificado PEM)
- Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
- x509 versión 3
- SubjectAltName debe contener DNS Name=*machine\_FQDN*
- Formato CRT
- Contiene los siguientes usos de claves: firma digital, sin rechazo, cifrado de clave.
- La autenticación de cliente y la autenticación de servidor no pueden estar presentes en el uso mejorado de claves.

VMCA no admite los siguientes certificados.

- Certificados con comodines
- No se recomiendan los algoritmos md2WithRSAEncryption 1.2.840.113549.1.1.2, md5WithRSAEncryption 1.2.840.113549.1.1.4 ni sha1WithRSAEncryption 1.2.840.113549.1.1.5.
- El algoritmo RSASSA-PSS con el OID 1.2.840.113549.1.1.10 no es compatible.

### Cumplimiento del certificado con RFC 2253

El certificado debe cumplir con RFC 2253.

Si no genera solicitudes de firma de certificados (Certificate Signature Request, CSR) con Certificate Manager, asegúrese de que la CSR incluya los siguientes campos.

Cadena	Tipo de atributo X.500
CN	commonName
L	localityName

Cadena	Tipo de atributo X.500
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
CALLE	streetAddress
DC	domainComponent
UID	userid

Si genera CSR mediante Certificate Manager, se le pedirá la siguiente información y Certificate Manager agregará los campos correspondientes al archivo de CSR.

- La contraseña del usuario `administrator@vsphere.local` o del administrador del dominio de vCenter Single Sign-On al que se va a conectar.
- Cuando se desea generar una CSR en un entorno con una instancia externa de Platform Services Controller, se solicita el nombre de host o la dirección IP de Platform Services Controller.
- Información que Certificate Manager almacena en el archivo `certtool.cfg`. En la mayoría de los campos, se puede aceptar el valor predeterminado o proporcionar valores específicos del sitio. Se requiere el FQDN de la máquina.
  - Contraseña de `administrator@vsphere.local`.
  - Código de país de dos letras
  - Nombre de empresa
  - Nombre de organización
  - Unidad de organización
  - Estado
  - Localidad
  - Dirección IP (opcional)
  - Correo electrónico
  - Nombre del host, es decir, el nombre de dominio completo de la máquina para la que se desea reemplazar el certificado. Si el nombre del host no coincide con el FQDN, el reemplazo de los certificados no se completa correctamente y el entorno puede quedar en un estado inestable.
  - Dirección IP de Platform Services Controller si se ejecuta el comando en un nodo de vCenter Server (administración)

## Requisitos al usar VMCA como entidad de certificación intermedia

Cuando se utiliza VMCA como entidad de certificación intermedia, los certificados deben cumplir los siguientes requisitos.

Tipo de certificado	Requisitos de certificados
Certificado raíz	<ul style="list-style-type: none"> <li>■ Se puede utilizar vSphere Certificate Manager para crear la CSR. Consulte <a href="#">Generar una CSR con vSphere Certificate Manager y preparar certificados raíz (CA intermedia)</a></li> <li>■ Si prefiere crear la CSR de forma manual, el certificado que envíe para firmar debe cumplir con los siguientes requisitos. <ul style="list-style-type: none"> <li>■ Tamaño de clave: 2.048 bits o más</li> <li>■ Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8</li> <li>■ x509 versión 3</li> <li>■ Si utiliza certificados personalizados, la extensión CA debe establecerse con el valor true para certificados de raíz, y el signo cert debe estar en la lista de requisitos.</li> <li>■ La firma CRL debe estar habilitada.</li> <li>■ El uso mejorado de clave no debe contener autenticación de cliente ni autenticación de servidor.</li> <li>■ No hay límite explícito a la longitud de la cadena de certificados. VMCA utiliza el valor predeterminado de OpenSSL, que es de diez certificados.</li> <li>■ No se admiten los certificados con comodines o con más de un nombre DNS.</li> <li>■ No se pueden crear CA subsidiarias de VMCA.</li> </ul> </li> </ul> <p>Para obtener un ejemplo de uso de Microsoft Certificate Authority, consulte el artículo 2112009 de la base de conocimientos de VMware, <a href="#">Cómo crear una plantilla de Microsoft Certificate Authority para la creación de certificados SSL en vSphere 6.0.</a></p>
Certificado SSL de máquina	<p>Se puede utilizar vSphere Certificate Manager para crear la solicitud CSR o crear manualmente la CSR.</p> <p>Si crea manualmente la CSR, esta debe cumplir con los requisitos enumerados en la sección <i>Requisitos para todos los certificados importados</i> que se muestra arriba. También tendrá que especificar el FQDN del host.</p>
Certificado de usuario de solución	<p>Se puede utilizar vSphere Certificate Manager para crear la solicitud CSR o crear manualmente la CSR.</p> <hr/> <p><b>Nota</b> Debe utilizar un valor diferente en el nombre para cada usuario de solución. Si genera el certificado manualmente, es posible que esto se muestre como <b>CN</b> en el <b>asunto</b>, según la herramienta que utilice.</p>

Tipo de certificado	Requisitos de certificados
	Si utiliza vSphere Certificate Manager, la herramienta le solicitará información del certificado para cada usuario de solución. vSphere Certificate Manager almacena la información en <code>certtool.cfg</code> . Consulte la <i>información que solicita Certificate Manager</i> .

## Requisitos de certificados personalizados

Si desea utilizar certificados personalizados, los certificados deben cumplir los siguientes requisitos.

Tipo de certificado	Requisitos de certificados
Certificado SSL de máquina	<p>El certificado SSL de máquina en cada nodo debe tener un certificado independiente de la entidad de certificación empresarial o externa.</p> <ul style="list-style-type: none"> <li>■ Puede generar la CSR mediante vSphere Certificate Manager o crearla de forma manual. La CSR debe cumplir con los requisitos enumerados en <i>Requisitos para todos los certificados importados</i> que se muestra arriba.</li> <li>■ Si utiliza vSphere Certificate Manager, la herramienta le solicitará información del certificado para cada usuario de solución. vSphere Certificate Manager almacena la información en <code>certtool.cfg</code>. Consulte la <i>información que solicita Certificate Manager</i>.</li> <li>■ En la mayoría de los campos, se puede aceptar el valor predeterminado o proporcionar valores específicos del sitio. Se requiere el FQDN de la máquina.</li> </ul>
Certificado de usuario de solución	<p>Cada usuario de solución en cada nodo debe tener un certificado independiente de la entidad de certificación empresarial o externa.</p> <ul style="list-style-type: none"> <li>■ Puede generar la CSR mediante vSphere Certificate Manager o prepararla usted mismo. La CSR debe cumplir con los requisitos enumerados en <i>Requisitos para todos los certificados importados</i> que se muestra arriba.</li> <li>■ Si utiliza vSphere Certificate Manager, la herramienta le solicitará información del certificado para cada usuario de solución. vSphere Certificate Manager almacena la información en <code>certtool.cfg</code>. Consulte la <i>información que solicita Certificate Manager</i>.</li> </ul> <p><b>Nota</b> Debe utilizar un valor diferente en el nombre para cada usuario de solución. Si genera el certificado manualmente, es posible que esto se muestre como <b>CN</b> en el <b>asunto</b>, según la herramienta que utilice.</p> <p>Cuando reemplace posteriormente los certificados de usuario de solución por certificados personalizados, proporcione la cadena de certificados de firma completa de la entidad de certificación externa.</p>

**Nota** No utilice los puntos de distribución de CRL, el acceso a la información de autoridad o la información de la plantilla de certificado en ningún certificado personalizado.

## Descripción general de la administración de certificados

El impacto que tenga la nueva infraestructura de certificados depende de los requisitos del entorno, si se está realizando una instalación nueva o una actualización, y si está considerando ESXi o vCenter Server.

## Administradores que no reemplazan certificados de VMware

Si es administrador y actualmente no reemplaza certificados de VMware, VMCA puede encargarse de la administración completa de los certificados. VMCA aprovisiona a vCenter Server con componentes y hosts ESXi con certificados que usan VMCA como entidad de certificación raíz. Si está actualizando a vSphere 6 desde una versión anterior de vSphere, todos los certificados autofirmados se reemplazan con certificados firmados por VMCA.

## Administradores que reemplazan certificados de VMware por certificados personalizados

En el caso de una instalación nueva, los administradores tienen estas opciones si la directiva de la empresa establece que los certificados tienen que estar firmados por una entidad de certificación externa o empresarial, o bien necesita información sobre certificados personalizados.

- Reemplace el certificado raíz de VMCA por un certificado firmado por la entidad de certificación. En este caso, el certificado de VMCA es un certificado intermedio de esta entidad de certificación externa. VMCA aprovisiona a los componentes de vCenter Server y a los hosts ESXi con certificados que incluyen la cadena completa de certificados.
- Si la directiva de la empresa no permite certificados intermedios en la cadena, debe reemplazarlos de manera explícita. Puede usar la utilidad vSphere Certificate Manager o realizar el reemplazo manual de certificados mediante la CLI de administración de certificados.

Cuando actualice un entorno que usa certificados personalizados, puede retener algunos.

- Los hosts ESXi mantienen sus certificados personalizados durante la actualización. Asegúrese de que el proceso de actualización de vCenter Server agregue todos los certificados raíz relevantes al almacén TRUSTED\_ROOTS en VECS en vCenter Server.

Después de actualizar vCenter Server, los administradores pueden establecer el modo de certificación en Personalizado (consulte [Cambiar el modo de certificado](#)). Si el modo de certificación es el predeterminado, VMCA, y el usuario actualiza el certificado desde vSphere Web Client, los certificados firmados por VMCA reemplazan a los certificados personalizados.

- En el caso de los componentes de vCenter Server, lo que suceda dependerá del entorno actual.
  - Si actualiza una instalación simple a una implementación integrada, se conservarán las certificaciones personalizadas de vCenter Server. Después de la actualización, el entorno funcionará como antes.
  - Si actualiza una implementación en varios sitios donde vCenter Single Sign-On se encuentra en una máquina diferente que otros componentes de vCenter Server, el proceso de actualización crea una implementación en varios nodos que incluye un nodo de Platform Services Controller y uno o más nodos de administración.

En este caso, los certificados actuales de vCenter Server y de vCenter Single Sign-On se conservan y se usan como certificados SSL de máquina. VMCA asigna un certificado firmado por VMCA a cada usuario de solución (recopilación de servicios de vCenter). Un usuario de solución utiliza este certificado únicamente para autenticarse en vCenter Single Sign-On, por lo que puede resultar innecesario reemplazar los certificados del usuario de solución.

Ya no podrá usar la herramienta de reemplazo de certificados de vSphere 5.5, que estaba disponible para las instalaciones de vSphere 5.5, ya que la nueva arquitectura resulta en una selección y distribución diferentes de los servicios. Una nueva utilidad de la línea de comandos, vSphere Certificate Manager, está disponible para la mayoría de las tareas de administración de certificados.

## Interfaces de certificados de vCenter

En el caso de vCenter Server, es posible ver y reemplazar certificados con las siguientes herramientas e interfaces.

### utilidad vSphere Certificate Manager

Realice todas las tareas de reemplazo de certificados comunes desde la línea de comandos.

### CLI de administración de certificados

Realice todas las tareas de administración de certificados con `dir-cli`, `certool` y `vecs-cli`.

### Administración de certificados de vSphere Web Client

Vea los certificados, incluida la información de caducidad.

En el caso de ESXi, puede realizar la administración de certificados desde vSphere Web Client. Los certificados son aprovisionados por VMCA y almacenados solo de manera local en el host ESXi, ni en vmdir ni en VECS. Consulte [Administrar certificados para hosts ESXi](#).

## Certificados de vCenter admitidos

En el caso de vCenter Server, Platform Services Controller, y las máquinas y los servicios relacionados, se admiten los siguientes certificados:

- Certificados generados y firmados por la entidad de certificación VMware Certificate Authority (VMCA).
- Certificados personalizados.
  - Certificados empresariales que se generan desde su propia PKI interna.
  - Certificados externos firmados por una entidad de certificación que se genera mediante una PKI externa como Verisign, GoDaddy, etc.

No se admiten los certificados autofirmados que se crearon mediante OpenSSL donde no existe una entidad de certificación raíz.



## Descripción general del reemplazo de certificados

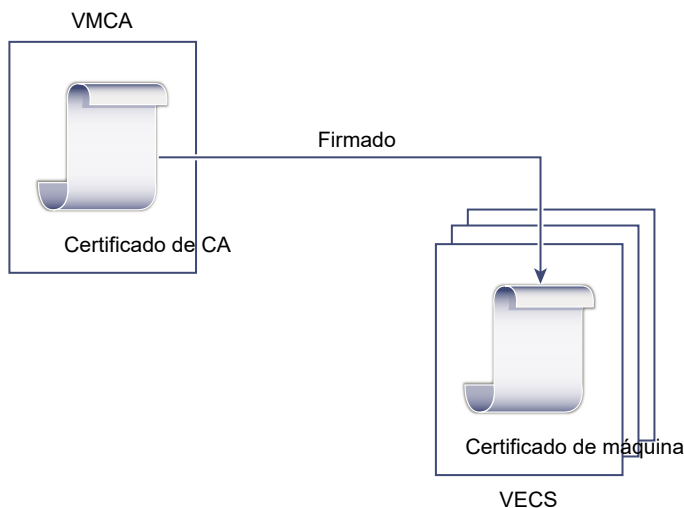
Es posible realizar distintos tipos de reemplazo de certificados según los requisitos y la directiva de la empresa para el sistema que va a configurar. Puede realizar cada reemplazo con la utilidad vSphere Certificate Manager o manualmente mediante las CLI que se incluyen con la instalación.

Es posible reemplazar los certificados predeterminados. Para los componentes de vCenter Server, puede usar un conjunto de herramientas de línea de comandos que se incluyen en la instalación. Existen varias opciones.

### Reemplazar con certificados firmados por VMCA

Si su certificado de VMCA vence o si quiere reemplazarlo por otros motivos, puede usar las CLI de administración de certificados para realizar ese proceso. De forma predeterminada, el certificado raíz de VMCA vence después de diez años y todos los certificados que firma VMCA vencen cuando vence el certificado raíz, es decir, después de un máximo de diez años.

Figura 3-1. Los certificados firmados por VMCA se almacenan en VECS



### Conversión de VMCA en una CA intermediaria

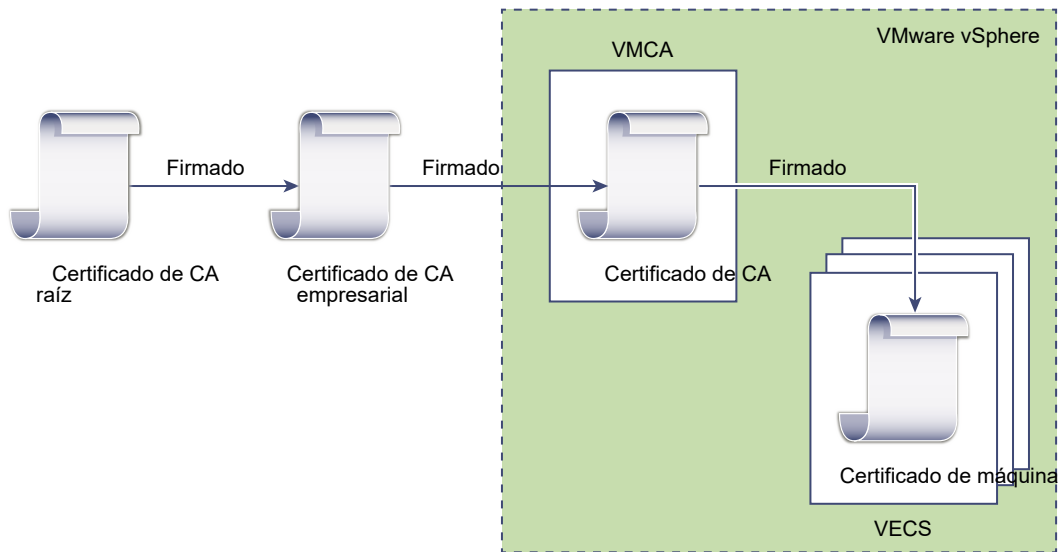
Puede reemplazar el certificado raíz de VMCA por un certificado firmado por una CA empresarial o externa. VMCA firma el certificado raíz cada vez que aprovisiona certificados, lo que convierte a VMCA en una CA intermediaria.

---

**Nota** Si realiza una instalación nueva que incluye una instancia de Platform Services Controller externa, instale el primer Platform Services Controller y reemplace el certificado raíz de VMCA. Luego, instale otros servicios o agregue hosts ESXi al entorno. Si realiza una instalación nueva que incluye una instancia de Platform Services Controller integrada, reemplace el certificado raíz de VMCA antes de agregar hosts ESXi. Si lo hace, la cadena completa firma todos los certificados y no es necesario generar certificados nuevos.

---

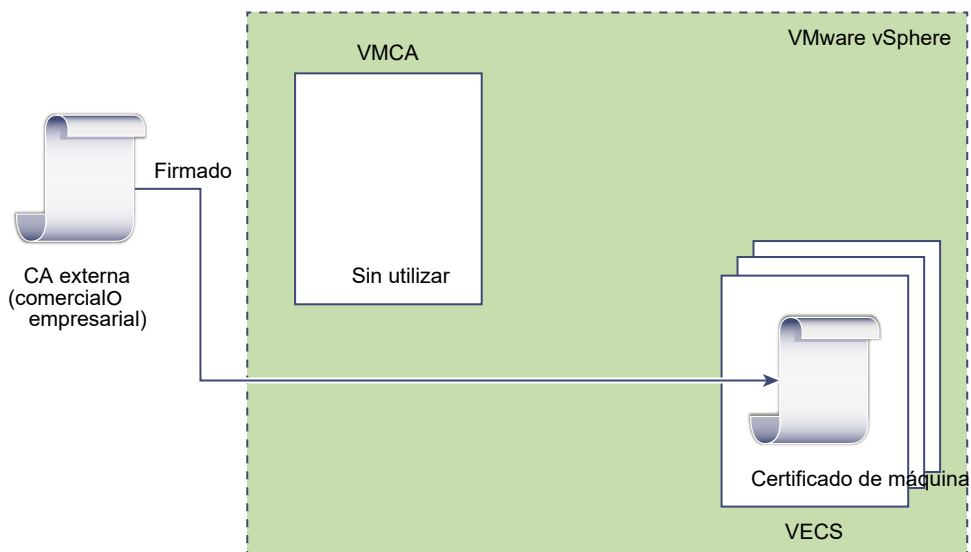
Figura 3-2. Los certificados firmados por una CA empresarial o externa usan VMCA como CA intermediaria



### No use VMCA; aprovisione certificados personalizados

Puede reemplazar los certificados firmados por VMCA existentes con certificados personalizados. Si emplea este enfoque, asume la responsabilidad del aprovisionamiento y la supervisión de todos los certificados.

Figura 3-3. Los certificados externos se almacenan directamente en VECS



## Implementación híbrida

Puede hacer que VMCA proporcione algunos de los certificados, pero, al mismo tiempo, certificados personalizados para otras partes de la infraestructura. Por ejemplo, dado que los certificados de usuarios de soluciones se usan solo para autenticar vCenter Single Sign-On, considere la posibilidad de hacer que VMCA aprovisione esos certificados. Reemplace los certificados de SSL de máquinas con certificados personalizados para proteger todo el tráfico de SSL.

## Reemplazar certificados de ESXi

Para los hosts ESXi, puede cambiar el comportamiento de aprovisionamiento de certificados desde vSphere Web Client.

### Modo VMware Certificate Authority (valor predeterminado)

Quando se renuevan certificados desde vSphere Web Client, VMCA emite los certificados para los hosts. Si cambió el certificado raíz de VMCA para incluir una cadena de certificados, los certificados del host incluyen la cadena completa.

### Modo de entidad de certificación personalizada

Permite actualizar y usar manualmente certificados que no han sido firmados o emitidos por VMCA.

### Modo de huella digital

Puede usarse para conservar los certificados de la versión 5.5 durante la actualización. Use este modo únicamente de manera temporal en situaciones de depuración.

## Casos en que vSphere 6.0 utiliza certificados

En vSphere 6.0 y versiones posteriores, VMware Certificate Authority (VMCA) aprovisiona el entorno con certificados. Entre ellos se incluyen certificados SSL de máquina para conexiones seguras, certificados de usuarios de solución para autenticarse en vCenter Single Sign-On y certificados para hosts ESXi que se agregan a vCenter Server.

Los siguientes certificados están en uso.

**Tabla 3-2. Certificados de vSphere 6.0**

Certificado	Aprovisionado por	Almacenado
Certificados de ESXi	VMCA (valor predeterminado)	Localmente en el host ESXi
Certificados SSL de máquina	VMCA (valor predeterminado)	VECS
Certificados de usuarios de solución	VMCA (valor predeterminado)	VECS

Tabla 3-2. Certificados de vSphere 6.0 (continuación)

Certificado	Aprovisionado por	Almacenado
Certificado de firma SSL vCenter Single Sign-On	Aprovisionado durante la instalación.	Administre este certificado desde vSphere Web Client.  <b>Advertencia</b> No cambie este certificado en el sistema de archivos, ya que podría producirse un comportamiento impredecible.
Certificado SSL de VMware Directory Service (vmdir)	Aprovisionado durante la instalación.	En algunos casos extremos, es posible que tenga que reemplazar este certificado. Consulte <a href="#">Reemplazar certificado para VMware Directory Service</a> .

## ESXi

Los certificados de ESXi se almacenan localmente en cada host del directorio `/etc/vmware/ssl`. Los certificados de ESXi son aprovisionados por VMCA de manera predeterminada, pero se pueden utilizar certificados personalizados. Los certificados de ESXi se aprovisionan cuando se agrega el host por primera vez a vCenter Server y cuando el host se vuelve a conectar.

## Certificados SSL de máquina

El certificado SSL de máquina de cada nodo se utiliza para crear un socket de SSL en el lado del servidor al cual se conectan los clientes SSL. El certificado se utiliza para comprobar el servidor y establecer una comunicación segura mediante los protocolos HTTPS o LDAPS.

Todos los servicios se comunican mediante el proxy inverso. Por cuestiones de compatibilidad, los servicios que estaban disponibles en versiones anteriores de vSphere también utilizan puertos específicos. Por ejemplo, el servicio `vpzd` utiliza `MACHINE_SSL_CERT` para exponer su extremo.

Cada nodo (de implementación integrada, de administración o Platform Services Controller), tiene su propio certificado SSL de máquina. Todos los servicios que se ejecutan en ese nodo utilizan este certificado SSL de máquina para exponer sus extremos SSL.

El certificado SSL de máquina se utiliza del siguiente modo:

- Mediante el servicio de proxy inverso en cada nodo de Platform Services Controller. Las conexiones SSL a los servicios individuales de vCenter siempre van al proxy inverso. El tráfico no va a los servicios en sí.
- Mediante el servicio de vCenter (`vpzd`) en los nodos de administración y los nodos integrados.
- Mediante VMware Directory Service (`vmdir`) en los nodos de infraestructura y los nodos integrados.

Los productos de VMware utilizan certificados estándar de la versión X.509 3 (X.509v3) para cifrar la información de la sesión que se envía entre los componentes por medio de SSL.

## Certificados de usuarios de solución

Un usuario de solución agrupa uno o más servicios de vCenter Server y utiliza certificados para autenticarse en vCenter Single Sign-On mediante el intercambio de token SAML. Cada usuario de solución debe estar autenticado en vCenter Single Sign-On.

Los certificados de usuarios de solución se utilizan para efectuar la autenticación en vCenter Single Sign-On. Un usuario de solución presenta el certificado ante vCenter Single Sign-On cuando debe autenticarse por primera vez, después de un reinicio y de transcurrido un tiempo de espera.

El tiempo de espera (tiempo de espera Holder-of-Key) puede establecerse desde vSphere Web Client y su valor predeterminado es 2.592.000 segundos (30 días).

Por ejemplo, el usuario de solución vpxd presenta su certificado en vCenter Single Sign-On al conectarse a vCenter Single Sign-On. El usuario de solución vpxd recibe un token SAML de vCenter Single Sign-On y, a continuación, puede utilizarlo para autenticarse en otros servicios y usuarios de solución.

Los siguientes almacenes de certificados de usuarios de solución se incluyen en VECS en cada nodo de administración y en cada implementación integrada:

- `machine`: lo utilizan el administrador de componentes, el servidor de licencias y el servicio de registro.

---

**Nota** El certificado de usuario de solución de la máquina no tiene relación alguna con el certificado SSL de máquina. El certificado de usuario de solución de la máquina se utiliza para el intercambio de tokens SAML, mientras que el certificado SSL de máquina se utiliza para las conexiones SSL seguras de una máquina.

---

- `vpxd`: almacén de daemon del servicio vCenter (vpxd) de los nodos de administración y las implementaciones integradas. vpxd utiliza el certificado de usuario de solución que está en este almacén para autenticarse en vCenter Single Sign-On.
- `vpxd-extensions`: almacén de extensiones de vCenter. Incluye el servicio de Auto Deploy, el servicio de inventario u otros servicios que no forman parte de otros usuarios de solución.
- `vsphere-webclient`: almacén de vSphere Web Client. También incluye algunos servicios adicionales como el servicio de gráficos de rendimiento.

El almacén `machine` también se incluye en cada nodo de Platform Services Controller.

## Certificados de vCenter Single Sign-On

Los certificados de vCenter Single Sign-On no se almacenan en VECS y no se administran con herramientas de administración de certificados. Como regla general, no es necesario hacer cambios, pero en situaciones especiales, estos certificados se pueden reemplazar.

### Certificado de firma de vCenter Single Sign-On

El servicio vCenter Single Sign-On incluye un servicio de proveedor de identidad que emite tokens SAML utilizados para la autenticación en todo el sistema vSphere. Un token SAML representa la identidad del usuario y, a su vez, contiene información sobre la pertenencia a los grupos. Cuando vCenter Single Sign-On emite tokens SAML, firma cada token con su certificado de firma, de modo que los clientes de vCenter Single Sign-On pueden comprobar que el token SAML proviene de un origen confiable.

vCenter Single Sign-On emite tokens SAML HoK para los usuarios de solución y tokens de portador para otros usuarios, que inician sesión con un nombre de usuario y una contraseña.

Este certificado se puede reemplazar desde vSphere Web Client. Consulte [Actualizar el certificado del servicio de token de seguridad](#).

### Certificado SSL de VMware Directory Service

Si utiliza certificados personalizados, es posible que deba reemplazar explícitamente el certificado SSL de VMware Directory Service. Consulte [Reemplazar certificado para VMware Directory Service](#).

## Servicios básicos de identidad de VMware y VMCA

Los servicios básicos de identidad forman parte de toda implementación integrada y todo nodo de servicios de plataforma. VMCA forma parte de cada grupo de servicios básicos de identidad de VMware. Utilice las CLI de administración y vSphere Web Client para interactuar con estos servicios.

Los servicios básicos de identidad de VMware incluyen varios componentes.

**Tabla 3-3. Servicios básicos de identidad**

Servicio	Descripción	Incluidos en
VMware Directory Service (vmdir)	Controla la administración de certificados SAML para la autenticación junto con vCenter Single Sign-On.	Platform Services Controller Implementación integrada
VMware Certificate Authority (VMCA)	Emite certificados para usuarios de soluciones de VMware, certificados para las máquinas en las que se ejecutan servicios y certificados para hosts ESXi. VMCA puede utilizarse en el estado en que se encuentra o como entidad de certificación intermediaria.  VMCA emite certificaciones únicamente a los clientes que pueden autenticarse en vCenter Single Sign-On en el mismo dominio.	Platform Services Controller Implementación integrada
VMware Authentication Framework Daemon (VMAFD)	Incluye VMware Endpoint Certificate Store (VECS) y otros servicios de autenticación. Los administradores de VMware interactúan con VECS; los otros servicios se utilizan de manera interna.	Platform Services Controller vCenter Server Implementación integrada

## Descripción general de VMware Endpoint Certificate Store

VMware Endpoint Certificate Store (VECS) sirve de repositorio local (del lado del cliente) para certificados, claves privadas y cualquier información de certificados que pueda guardarse en un almacén de claves. Puede optar por no usar VMCA como entidad de certificación y firmante de certificados, pero debe usarlo para almacenar todos los certificados, las claves y demás elementos de vCenter. Los certificados de ESXi se almacenan de forma local en cada host y no en VECS.

VECS se ejecuta como parte de VMware Authentication Framework Daemon (VMAFD). VECS se ejecuta en todas las implementaciones integradas, el nodo de Platform Services Controller y el nodo de administración, y conserva todos los almacenes de claves que contienen certificados y claves.

VECS sondea VMware Directory Service (vmdir) de forma periódica en busca de actualizaciones del almacén TRUSTED\_ROOTS. También puede administrar certificados de forma explícita en VECS mediante los comandos `vecs-cli`. Consulte [Referencia de comandos vecs-cli](#).

VECS incluye los siguientes almacenes.

**Tabla 3-4. Almacenes en VECS**

Almacén	Descripción
Almacén SSL de máquina (MACHINE_SSL_CERT)	<ul style="list-style-type: none"> <li>■ El servicio de proxy inverso lo utiliza en cada nodo de vSphere.</li> <li>■ VMware Directory Service (vmdir) lo utiliza en implementaciones integradas y en cada nodo de Platform Services Controller.</li> </ul> <p>Todos los servicios de vSphere 6.0 se comunican mediante un proxy inverso que utiliza el certificado SSL de máquina. Por razones de compatibilidad con versiones anteriores, los servicios de la versión 5.x todavía utilizan puertos específicos. Como resultado, algunos servicios como vpxd todavía tienen su propio puerto abierto.</p>
Almacén raíz de confianza (TRUSTED_ROOTS)	Contiene todos los certificados raíz de confianza.

Tabla 3-4. Almacenes en VECS (continuación)

Almacén	Descripción
<p>Almacenes de usuarios de solución</p> <ul style="list-style-type: none"> <li>■ virtual</li> <li>■ vpxd</li> <li>■ vpxd-extensions</li> <li>■ vsphere-webclient</li> </ul>	<p>VECS incluye un almacén para cada usuario de solución. El asunto de cada certificado de usuario de solución debe ser único, por ejemplo, el certificado de máquina no puede tener el mismo asunto que el certificado de vpxd.</p> <p>Los certificados de usuarios de solución se utilizan para la autenticación con vCenter Single Sign-On. vCenter Single Sign-On comprueba que el certificado sea válido, pero no comprueba otros atributos del certificado. En una implementación integrada, todos los certificados de usuarios de solución están en el mismo sistema.</p> <p>Los siguientes almacenes de certificados de usuarios de solución se incluyen en VECS en cada nodo de administración y en cada implementación integrada:</p> <ul style="list-style-type: none"> <li>■ <code>machine</code>: lo utilizan el administrador de componentes, el servidor de licencias y el servicio de registro.</li> </ul> <hr/> <p><b>Nota</b> El certificado de usuario de solución de la máquina no tiene relación alguna con el certificado SSL de máquina. El certificado de usuario de solución de la máquina se utiliza para el intercambio de tokens SAML, mientras que el certificado SSL de máquina se utiliza para las conexiones SSL seguras de una máquina.</p> <hr/> <ul style="list-style-type: none"> <li>■ <code>vpxd</code>: almacén de daemon del servicio vCenter (<code>vpxd</code>) de los nodos de administración y las implementaciones integradas. <code>vpxd</code> utiliza el certificado de usuario de solución que está en este almacén para autenticarse en vCenter Single Sign-On.</li> <li>■ <code>vpxd-extensions</code>: almacén de extensiones de vCenter. Incluye el servicio de Auto Deploy, el servicio de inventario u otros servicios que no forman parte de otros usuarios de solución.</li> <li>■ <code>vsphere-webclient</code>: almacén de vSphere Web Client. También incluye algunos servicios adicionales como el servicio de gráficos de rendimiento.</li> </ul> <p>El almacén <code>machine</code> también se incluye en cada nodo de Platform Services Controller.</p>



Tabla 3-4. Almacenes en VECS (continuación)

Almacén	Descripción
Almacén de copias de seguridad de la utilidad vSphere Certificate Manager (BACKUP_STORE)	VMCA (VMware Certificate Manager) lo utiliza para admitir la reversión de certificados. Solo el estado más reciente se almacena como copia de seguridad; no se puede volver más de un paso.
Otros almacenes	<p>Las soluciones pueden agregar otros almacenes. Por ejemplo, la solución Virtual Volumes agrega un almacén SMS. No modifique los certificados de estos almacenes a menos que lo indique la documentación de VMware o un artículo de la base de conocimientos de VMware.</p> <p><b>Nota</b> Las CRL no son compatibles con vSphere 6.0. Sin embargo, si se elimina el almacén TRUSTED_ROOTS_CRLS, se puede dañar la infraestructura de certificados. No elimine ni modifique el almacén TRUSTED_ROOTS_CRLS.</p>

El servicio de vCenter Single Sign-On almacena el certificado de firma de tokens y su certificado SSL en el disco. Puede cambiar el certificado de firma de tokens desde vSphere Web Client.

**Nota** No cambie ningún archivo de certificado en el disco a menos que se indique en la documentación de VMware o en los artículos de la base de conocimientos. De lo contrario, se puede producir un comportamiento inesperado.

Algunos certificados se almacenan en el sistema de archivos, ya sea de forma temporal durante el arranque o de forma permanente. No cambie los certificados en el sistema de archivos. Use `vecs-cli` para realizar operaciones en los certificados almacenados en VECS.

## Administrar la revocación de certificados

Si sospecha que la confiabilidad de uno de los certificados está comprometida, reemplace todos los certificados actuales, incluido el certificado raíz de VMCA.

vSphere 6.0 admite el reemplazo de los certificados, pero no aplica su revocación en los hosts ESXi o en los sistemas vCenter Server.

Quite los certificados revocados de todos los nodos. Si no los quita, un ataque de tipo "Man in the middle" (intermedio) podría comprometerlos al habilitarse una suplantación con las credenciales de la cuenta.

## Reemplazar certificados en implementaciones de gran tamaño

El reemplazo de certificados en implementaciones que incluyen varios nodos de administración y uno o más nodos de Platform Services Controller es similar al reemplazo en implementaciones integradas. En ambos casos, puede usar la utilidad vSphere Certificate Management o reemplazar los certificados a mano. Algunas prácticas recomendadas sirven como guía para el proceso de reemplazo.

## Reemplazar certificados en entornos de alta disponibilidad que incluyen un equilibrador de carga

En los entornos con menos de ocho sistemas vCenter Server, VMware generalmente recomienda una única instancia de Platform Services Controller y un servicio vCenter Single Sign-On asociado. En los entornos más grandes, considere la posibilidad de usar varias instancias de Platform Services Controller, protegidas por un equilibrador de carga. En el informe técnico *Guía de implementación de vCenter Server 6.0*, disponible en el sitio web de VMware, se describe esta configuración.

## Reemplazo de certificados SSL de máquina en entornos con varios nodos de administración

Si el entorno incluye varios nodos de administración y una única instancia de Platform Services Controller, puede reemplazar los certificados con la utilidad vSphere Certificate Manager o manualmente con los comandos de la CLI de vSphere.

### vSphere Certificate Manager

Ejecute vSphere Certificate Manager en cada máquina. En los nodos de administración, se le solicitará la dirección IP de Platform Services Controller. Según la tarea que realice, también se le solicitará información del certificado.

### Reemplazar certificados de forma manual

Para reemplazar un certificado manualmente, ejecute los comandos de reemplazo de los certificados en cada máquina. En los nodos de administración, debe especificar Platform Services Controller con el parámetro `--server`. Consulte los siguientes temas para obtener más detalles:

- [Reemplazar certificados SSL de máquina por certificados firmados por VMCA](#)
- [Reemplazar certificados SSL de máquina \(entidad de certificación intermedia\)](#)
- [Reemplazar certificados SSL de máquina por certificados personalizados](#)

## Reemplazo de certificados del usuario de solución en entornos con varios nodos de administración

Si el entorno incluye varios nodos de administración y una única instancia de Platform Services Controller, siga estos pasos para reemplazar los certificados.

---

**Nota** Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

---

### vSphere Certificate Manager

Ejecute vSphere Certificate Manager en cada máquina. En los nodos de administración, se le solicitará la dirección IP de Platform Services Controller. Según la tarea que realice, también se le solicitará información del certificado.

### Reemplazar certificados de forma manual

- 1 Genere o solicite un certificado. Necesita los siguientes certificados:
  - Un certificado para el usuario de solución de la máquina en Platform Services Controller.
  - Un certificado para el usuario de solución de la máquina en cada nodo de administración.
  - Un certificado para cada uno de los siguientes usuarios de solución en cada nodo de administración:
    - usuario de solución vpxd
    - usuario de solución vpxd-extension
    - usuario de solución vsphere-webclient
- 2 Reemplace los certificados en cada nodo. El proceso en particular depende del tipo de reemplazo de certificados que esté realizando. Consulte [Administrar certificados con la utilidad vSphere Certificate Manager](#)

Consulte los siguientes temas para obtener más detalles:

- [Reemplazar los certificados de usuario de solución por certificados nuevos firmados por VMCA](#)
- [Reemplazar certificados de usuarios de solución \(entidad de certificación intermedia\)](#)
- [Reemplazar los certificados de usuarios de soluciones con certificados personalizados](#)

Si la directiva de la empresa establece que se deben reemplazar todos los certificados, también tendrá que reemplazar el certificado de VMware Directory Service (vmdir) en Platform Services Controller. Consulte [Reemplazar certificado para VMware Directory Service](#).

### Reemplazar certificados en entornos donde se incluyen soluciones externas

Algunas soluciones, como VMware vCenter Site Recovery Manager o VMware vSphere Replication se instalan siempre en una máquina diferente a la del sistema vCenter Server o Platform Services Controller. Si se reemplaza el certificado SSL predeterminado de una máquina en el sistema vCenter Server o Platform Services Controller, se produce un error de conexión cuando la solución intenta conectarse al sistema vCenter Server.

Es posible ejecutar el script `ls_update_certs` para solucionar el problema. Consulte [el artículo 2109074 de la base de conocimientos de VMware](#) para obtener más detalles.

## Administrar certificados con la interfaz web de Platform Services Controller

Es posible ver y administrar certificados al iniciar sesión en la interfaz web de Platform Services Controller. Puede realizar muchas tareas de administración de certificados con la utilidad vSphere Certificate Manager o mediante la interfaz web.

La interfaz web de Platform Services Controller permite realizar las siguientes tareas de administración.

- Ver los almacenes de certificados actuales y agregar o eliminar entradas de almacenes de certificados.
- Ver la instancia de VMware Certificate Authority (VMCA) asociada con esta instancia de Platform Services Controller.
- Ver certificados generados por VMware Certificate Authority.
- Renovar los certificados actuales o reemplazarlos.

La mayoría de las partes de los flujos de trabajo de reemplazo de certificados se admiten completamente desde la interfaz web de Platform Services Controller. Para generar CSR, se puede usar la utilidad vSphere Certificate Manager.

### Flujos de trabajos compatibles

Después de instalar una instancia de Platform Services Controller, VMware Certificate Authority en ese nodo aprovisiona todos los demás nodos del entorno con certificados predeterminados. Se puede utilizar cualquiera de los siguientes flujos de trabajo para renovar o reemplazar certificados.

#### Renovar certificados

Puede hacer que VMCA genere un nuevo certificado raíz y renueve todos los certificados en el entorno desde la interfaz web de Platform Services Controller.

#### Conversión de VMCA en una CA intermediaria

Puede generar una CSR mediante la utilidad vSphere Certificate Manager, editar el certificado que recibe de CSR para que se agregue VMCA a la cadena y, a continuación, agregar la cadena de certificados y la clave privada al entorno. Al renovar todos los certificados, VMCA aprovisiona todas las máquinas y los usuarios de la solución con certificados firmados por la cadena completa.

#### Reemplazar certificados por certificados personalizados

Si no desea utilizar VMCA, puede generar CSR para los certificados que desea reemplazar. La CA devuelve un certificado raíz y un certificado firmado para cada CSR. Se puede cargar el certificado raíz y los certificados personalizados desde Platform Services Controller.

Si debe reemplazar el certificado raíz de VMware Directory Service (vmdir), o bien si la directiva de la empresa exige que reemplace el certificado de vCenter Single Sign-On en un entorno de modo mixto, puede usar los comandos de la CLI para reemplazar esos certificados después de reemplazar los otros certificados. Consulte [Reemplazar certificado para VMware Directory Service](#) y [Reemplazar el certificado de VMware Directory Service en entornos de modo mixto](#).

## Explorar almacenes de certificados desde la interfaz web de Platform Services Controller

En cada nodo de Platform Services Controller y en cada nodo de vCenter Server se incluye una instancia de VMware Endpoint Certificate Store (VECS). Puede explorar los diferentes almacenes en VMware Endpoint Certificate Store desde la interfaz web de Platform Services Controller.

Consulte [Descripción general de VMware Endpoint Certificate Store](#) para obtener detalles sobre los diferentes almacenes incluidos en VECS.

### Requisitos previos

Para la mayoría de las tareas de administración, debe contar con la contraseña del administrador de la cuenta de dominio local, administrator@vsphere.local o un dominio diferente si cambió el dominio durante la instalación.

### Procedimiento

- 1 En un explorador web, especifique la siguiente dirección URL para conectarse a Platform Services Controller:

**`https://psc_hostname_or_IP/psc`**

En una implementación integrada, el nombre de host o la dirección IP de Platform Services Controller es igual al nombre de host o la dirección IP de vCenter Server.

- 2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como administrator@mydomain.

- 3 En Certificados, haga clic en **Almacén de certificados** y explore el almacén.
- 4 Seleccione el almacén de VMware Endpoint Certificate Store (VECS) que desea explorar desde el menú desplegable.

[Descripción general de VMware Endpoint Certificate Store](#) explica cuál es el contenido de los almacenes individuales.

- 5 Para ver detalles sobre el certificado, seleccione el certificado y haga clic en el icono **Mostrar detalles**.
- 6 Para eliminar una entrada del almacén seleccionado, haga clic en el icono **Eliminar entrada**.

Por ejemplo, si reemplaza el certificado existente, puede quitar el certificado raíz anterior posteriormente. Quite los certificados únicamente si está seguro de que ya no están en uso.

## Reemplazar certificados por certificados firmados por VMCA desde la interfaz web de Platform Services Controller

Todos los certificados firmados por VMCA se pueden reemplazar por nuevos certificados firmados por VMCA; este proceso se denomina renovación de certificados. Puede renovar los certificados seleccionados o todos los certificados del entorno desde la interfaz web de Platform Services Controller.

### Requisitos previos

Para la administración de certificados, debe proporcionar la contraseña del administrador del dominio local (administrator@vsphere.local de forma predeterminada). Si está renovando certificados para un sistema vCenter Server, también puede proporcionar las credenciales de vCenter Single Sign-On para un usuario con privilegios de administrador en el sistema vCenter Server.

### Procedimiento

- 1 En un explorador web, especifique la siguiente dirección URL para conectarse a Platform Services Controller:

**`https://psc_hostname_or_IP/psc`**

En una implementación integrada, el nombre de host o la dirección IP de Platform Services Controller es igual al nombre de host o la dirección IP de vCenter Server.

- 2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como administrator@mydomain.

- 3 En Certificados, seleccione **Administración de certificados** y especifique la dirección IP o el nombre de host para Platform Services Controller, así como el nombre de usuario y la contraseña para el administrador del dominio local (administrator@vsphere.local de forma predeterminada), y haga clic en **Enviar**.

- 4 Renueve el certificado SSL de máquina del sistema local.

- a Haga clic en la pestaña **Certificados de máquina**.
- b Seleccione el certificado, haga clic en **Renovar** y responda **Sí** a la solicitud.

- 5 (Opcional) Renueve los certificados de usuarios de solución del sistema local.

- a Haga clic en la pestaña **Certificados de usuarios de solución**.
- b Seleccione un certificado y haga clic en **Renovar** para renovar los certificados individuales seleccionados o haga clic en **Renovar todos** para renovar todos los certificados de usuarios de la solución.
- c Responda **Sí** a la solicitud.

- 6 Si el entorno incluye una instancia de Platform Services Controller externa, es posible renovar los certificados para cada uno de los sistemas vCenter Server.
  - a Haga clic en el botón **Cerrar sesión** en el panel Administración de certificados.
  - b Cuando se lo solicite el sistema, especifique la dirección IP o el FQDN del sistema vCenter Server y el nombre de usuario y la contraseña del administrador de vCenter Server que se puede autenticar en vCenter Single Sign-On.
  - c Renueve el certificado SSL de máquina en vCenter Server y, de manera opcional, cada certificado de usuario de solución.
  - d Si existen varios sistemas vCenter Server en el entorno, repita el proceso para cada sistema.

### Pasos siguientes

Reinicie los servicios de Platform Services Controller. Puede reiniciar la instancia de Platform Services Controller o ejecutar los siguientes comandos desde la línea de comandos:

### Windows

En Windows, el comando service-control está ubicado en

*RUTA\_DE\_INSTALACIÓN\_DE\_VCENTER\bin.*

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

### vCenter Server Appliance

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

## Convertir una VMCA en una entidad de certificación intermedia desde la interfaz web de Platform Services Controller

Otra CA puede firmar el certificado VMCA, de manera que VMCA se convierta en una CA intermedia. Posteriormente, todos los certificados generados por VMCA incluirán la cadena completa.

Para realizar esta configuración, puede ejecutar la utilidad vSphere Certificate Manager, utilizar las CLI, o bien usar la interfaz web de Platform Services Controller.

### Requisitos previos

- 1 Genere la CSR.
- 2 Edite el certificado que recibe y coloque el certificado raíz de VMCA actual al final.

Generar una CSR con vSphere Certificate Manager y preparar certificados raíz (CA intermedia) explica ambos pasos.

### Procedimiento

- 1 En un explorador web, especifique la siguiente dirección URL para conectarse a Platform Services Controller:

**`https://psc_hostname_or_IP/psc`**

En una implementación integrada, el nombre de host o la dirección IP de Platform Services Controller es igual al nombre de host o la dirección IP de vCenter Server.

- 2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como administrator@mydomain.

- 3 Para reemplazar el certificado existente con el certificado encadenado, siga estos pasos:

- a En Certificados, haga clic en **Entidad de certificación** y seleccione la pestaña **Certificado raíz**.
- b Haga clic en **Reemplazar certificado**. agregue el archivo de clave privada y el archivo de certificado (cadena completa) y haga clic en **Aceptar**.
- c En el cuadro de diálogo **Reemplazar certificado raíz**, haga clic en **Examinar** y seleccione la clave privada; luego, haga clic en **Examinar** y seleccione el certificado, y haga clic en **Aceptar**.

Posteriormente, VMCA firma todos los certificados que emite con el nuevo certificado raíz encadenado.

- 4 Renueve el certificado SSL de máquina del sistema local.

- a En Certificados, haga clic en **Administración de certificados** y seleccione la pestaña **Certificados de máquina**.
- b Seleccione el certificado, haga clic en **Renovar** y responda **Sí** a la solicitud.

VMCA reemplaza el certificado SSL de máquina por un certificado firmado por la nueva entidad de certificación.

- 5 (opcional) Renueve los certificados de usuarios de solución del sistema local.

- a Haga clic en la pestaña **Certificados de usuarios de solución**.
- b Seleccione un certificado y haga clic en **Renovar** para renovar los certificados individuales seleccionados o haga clic en **Renovar todo** para reemplazar todos los certificados y, a continuación, responda **Sí** a la solicitud.

VMCA reemplaza los certificados de usuarios de solución por certificados firmados por la nueva entidad de certificación.



- 6 Si el entorno incluye una instancia de Platform Services Controller externa, es posible renovar los certificados para cada uno de los sistemas vCenter Server.
  - a Haga clic en el botón **Cerrar sesión** en el panel Administración de certificados.
  - b Cuando se lo solicite el sistema, especifique la dirección IP o el FQDN del sistema vCenter Server y el nombre de usuario y la contraseña del administrador de vCenter Server que se puede autenticar en vCenter Single Sign-On.
  - c Renueve el certificado SSL de máquina en vCenter Server y, de manera opcional, cada certificado de usuario de solución.
  - d Si existen varios sistemas vCenter Server en el entorno, repita el proceso para cada sistema.

### Pasos siguientes

Reinicie los servicios de Platform Services Controller. Puede reiniciar la instancia de Platform Services Controller o ejecutar los siguientes comandos desde la línea de comandos:

### Windows

En Windows, el comando service-control está ubicado en

*RUTA\_DE\_INSTALACIÓN\_DE\_VCENTER\bin.*

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

### vCenter Server Appliance

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

## Configurar el sistema para utilizar certificados personalizados desde Platform Services Controller

Puede utilizar Platform Services Controller para configurar el entorno de manera que utilice certificados personalizados.

Puede generar Solicitudes de firma de certificados (CSR) para cada máquina y para cada usuario de la solución que use la utilidad Administrador de certificados. Cuando entrega las CSR a su CA interna o externa, la CA devuelve certificados firmados y el certificado raíz. Se puede cargar el certificado raíz y los certificados firmados desde la UI de Platform Services Controller.

## Generar solicitudes de firma de certificado con vSphere Certificate Manager (certificados personalizados)

Es posible utilizar vSphere Certificate Manager para generar solicitudes de firma de certificado (CSR) y, a continuación, enviarlas a la entidad de certificación empresarial o a una entidad de certificación externa. Los certificados se pueden utilizar en los diversos procesos de reemplazo de certificados compatibles.

Puede ejecutar la herramienta Certificate Manager en la línea de comandos de la siguiente manera:

### Windows

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

### Linux

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

### Requisitos previos

vSphere Certificate Manager solicita información. La solicitud depende del entorno y del tipo de certificado que se desea reemplazar.

- Para cualquier tipo de generación de CSR, se solicita la contraseña del usuario administrator@vsphere.local o el administrador del dominio de vCenter Single Sign-On con el que se desea establecer la conexión.
- Cuando se desea generar una CSR en un entorno con una instancia externa de Platform Services Controller, se solicita el nombre de host o la dirección IP de Platform Services Controller.
- Para generar una CSR para un certificado SSL de máquina, se solicitan las propiedades del certificado, que están almacenadas en el archivo `certtool.cfg`. En la mayoría de los campos, se puede aceptar el valor predeterminado o proporcionar valores específicos del sitio. Se requiere el FQDN de la máquina.

### Procedimiento

- 1 En cada máquina del entorno, inicie vSphere Certificate Manager y seleccione la opción 1.
- 2 Si el sistema lo solicita, proporcione la contraseña y la dirección IP o el nombre de host de Platform Services Controller.
- 3 Seleccione la opción 1 para generar la CSR, responda las solicitudes del sistema y salga de Certificate Manager.

Es necesario especificar un directorio como parte de este proceso. Certificate Manager colocará el certificado y los archivos de claves en el directorio.

- 4 Si también desea reemplazar todos los certificados de usuario de solución, reinicie Certificate Manager.

- 5 Seleccione la opción 5.
- 6 Si el sistema lo solicita, proporcione la contraseña y la dirección IP o el nombre de host de Platform Services Controller.
- 7 Seleccione la opción 1 para generar las CSR, responda las solicitudes del sistema y salga de Certificate Manager.

Es necesario especificar un directorio como parte de este proceso. Certificate Manager colocará el certificado y los archivos de claves en el directorio.

En cada nodo de Platform Services Controller, Certificate Manager generará un certificado y un par de claves. En cada nodo de vCenter Server, Certificate Manager generará cuatro certificados y pares de claves.

#### Pasos siguientes

Realice el reemplazo de certificados.

### Agregar un certificado raíz de confianza al almacén de certificados

Si desea utilizar certificados de terceros en su entorno, debe agregar un certificado raíz de confianza al almacén de certificados.

#### Requisitos previos

Obtenga el certificado raíz personalizado de la entidad de certificación interna o de terceros.

#### Procedimiento

- 1 En un explorador web, especifique la siguiente dirección URL para conectarse a Platform Services Controller:

**`https://psc_hostname_or_IP/psc`**

En una implementación integrada, el nombre de host o la dirección IP de Platform Services Controller es igual al nombre de host o la dirección IP de vCenter Server.

- 2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como administrator@mydomain.

- 3 En Certificados, seleccione **Administración de certificados** y especifique la dirección IP o el nombre de host para Platform Services Controller, así como el nombre de usuario y la contraseña para el administrador del dominio local (administrator@vsphere.local de forma predeterminada), y haga clic en **Enviar**.

- 4 Seleccione **Certificados raíz de confianza** y haga clic en **Agregar certificado**.

- 5 Haga clic en **Examinar** y seleccione la ubicación de la cadena de certificados.

Puede usar un archivo del tipo CER, PEM o CRT.

## Pasos siguientes

Reemplace los certificados SSL de equipo y, opcionalmente, los certificados de usuarios de solución que firmó la entidad de certificación.

## Agregar certificados personalizados desde Platform Services Controller

Los certificados SSL de máquina y los certificados de usuarios de solución se pueden agregar al almacén de certificados desde Platform Services Controller

En la mayoría de los casos, reemplazar el certificado SSL de máquina para cada componente es suficiente. El certificado de usuarios de solución permanece detrás de un proxy.

## Requisitos previos

Genere solicitudes de firma de certificado (CSR) para cada certificado que desea reemplazar. Las CSR se pueden generar mediante la utilidad Certificate Manager. Coloque el certificado y la clave privada en una ubicación accesible para Platform Services Controller.

## Procedimiento

- 1 En un explorador web, especifique la siguiente dirección URL para conectarse a Platform Services Controller:

**`https://psc_hostname_or_IP/psc`**

En una implementación integrada, el nombre de host o la dirección IP de Platform Services Controller es igual al nombre de host o la dirección IP de vCenter Server.

- 2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como administrator@mydomain.

- 3 En Certificados, seleccione **Administración de certificados** y especifique la dirección IP o el nombre de host para Platform Services Controller, así como el nombre de usuario y la contraseña para el administrador del dominio local (administrator@vsphere.local de forma predeterminada), y haga clic en **Enviar**.

- 4 Para reemplazar un certificado de máquina, siga estos pasos:

- a Seleccione la pestaña **Certificados de máquina** y haga clic en el certificado que desea reemplazar.
- b Haga clic en **Reemplazar** y en **Examinar** para reemplazar la cadena de certificados; a continuación, haga clic en **Examinar** para reemplazar la clave privada.

5 Para reemplazar los certificados de usuarios de solución, siga estos pasos:

- a Seleccione la pestaña **Certificados de usuarios de solución** y haga clic en el primero de los cuatro certificados de un componente, por ejemplo, **máquina**.
- b Haga clic en **Reemplazar** y en **Examinar** para reemplazar la cadena de certificados; a continuación, haga clic en **Examinar** para reemplazar la clave privada.
- c Repita el proceso para los otros tres certificados del mismo componente.

#### Pasos siguientes

Reinicie los servicios de Platform Services Controller. Puede reiniciar la instancia de Platform Services Controller o ejecutar los siguientes comandos desde la línea de comandos:

#### Windows

En Windows, el comando service-control está ubicado en

*RUTA\_DE\_INSTALACIÓN\_DE\_VCENTER\bin.*

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

#### vCenter Server Appliance

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

## Administrar certificados con la utilidad vSphere Certificate Manager

La utilidad vSphere Certificate Manager permite realizar la mayoría de las tareas de administración de certificados de forma interactiva desde la línea de comandos. vSphere Certificate Manager solicita que se lleve a cabo una tarea, pide las ubicaciones de los certificados y otra información necesaria y, a continuación, detiene e inicia los servicios para reemplazar los certificados.

Si se utiliza vSphere Certificate Manager, el usuario no es responsable de colocar los certificados en VECS (VMware Endpoint Certificate Store) ni de iniciar y detener los servicios.

Antes de ejecutar vSphere Certificate Manager, asegúrese de comprender el proceso de reemplazo y consiga los certificados que desea utilizar.

---

**Precaución** vSphere Certificate Manager admite un nivel de reversión. Si se ejecuta vSphere Certificate Manager dos veces y se observa que el entorno se dañó de forma inesperada, la herramienta no puede revertir la primera de las dos ejecuciones.

---

La herramienta en la línea de comandos se ejecuta de la siguiente manera:

## Windows

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

## Linux

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

## Procedimiento

### 1 Revertir la última operación realizada volviendo a publicar certificados antiguos

Cuando se realiza una operación de administración de certificados mediante vSphere Certificate Manager, primero se almacena el estado actual del certificado en BACKUP\_STORE, en VECS, antes del reemplazo de los certificados. Es posible revertir la última operación realizada y regresar al estado anterior.

### 2 Restablecer todos los certificados

Puede usar la opción `Reset All Certificates` (Restablecer todos los certificados) para reemplazar los certificados de vCenter existentes por los certificados firmados por VMCA.

### 3 Regenerar un certificado raíz de VMCA nuevo y reemplazo de todos los certificados

Puede volver a generar el certificado raíz de VMCA para reemplazar el certificado SSL de máquina local, y reemplazar los certificados de usuarios de soluciones locales por certificados firmados por VMCA. En implementaciones de varios nodos, ejecute vSphere Certificate Manager con esta opción en Platform Services Controller y, a continuación, ejecute la utilidad nuevamente en los demás nodos y seleccione `Replace Machine SSL certificate with VMCA Certificate` y `Replace Solution user certificates with VMCA certificates`.

### 4 Convertir a VMCA en una entidad de certificación intermedia (Certificate Manager)

Es posible convertir a VMCA en una entidad de certificación intermedia si se siguen las solicitudes del sistema desde la utilidad Certificate Manager. Una vez completado el proceso, VMCA firmará todos los certificados nuevos con la cadena completa. Si lo desea, puede utilizar Certificate Manager para reemplazar todos los certificados existentes por nuevos certificados firmados por VMCA.

### 5 Reemplazar todos los certificados por certificados personalizados (Certificate Manager)

Es posible usar la utilidad vSphere Certificate Manager para reemplazar todos los certificados por certificados personalizados. Antes de iniciar el proceso, es necesario enviar solicitudes de firma de certificado (CSR) a la entidad de certificación. Se puede utilizar Certificate Manager para generar las CSR.

## Revertir la última operación realizada volviendo a publicar certificados antiguos

Cuando se realiza una operación de administración de certificados mediante vSphere Certificate Manager, primero se almacena el estado actual del certificado en `BACKUP_STORE`, en `VECS`, antes del reemplazo de los certificados. Es posible revertir la última operación realizada y regresar al estado anterior.

---

**Nota** La operación de reversión restablece lo que actualmente se encuentra en `BACKUP_STORE`. Si ejecuta vSphere Certificate Manager con dos opciones diferentes y, a continuación, intenta hacer la reversión, solo se revierte la última operación.

---

## Restablecer todos los certificados

Puede usar la opción `Reset All Certificates` (Restablecer todos los certificados) para reemplazar los certificados de vCenter existentes por los certificados firmados por VMCA.

Cuando utiliza esta opción, se sobrescriben todos los certificados personalizados que actualmente figuran en `VECS`.

- En un nodo de Platform Services Controller, vSphere Certificate Manager puede volver a generar el certificado raíz, y reemplazar el certificado SSL de máquina y el certificado del usuario de solución de la máquina.
- En un nodo de administración, vSphere Certificate Manager puede reemplazar el certificado SSL de máquina y todos los certificados de los usuarios de solución.
- En una implementación integrada, vSphere Certificate Manager puede reemplazar todos los certificados.

Qué certificados se reemplacen dependerá de las opciones que se seleccionen.

## Regenerar un certificado raíz de VMCA nuevo y reemplazo de todos los certificados

Puede volver a generar el certificado raíz de VMCA para reemplazar el certificado SSL de máquina local, y reemplazar los certificados de usuarios de soluciones locales por certificados firmados por VMCA. En implementaciones de varios nodos, ejecute vSphere Certificate Manager con esta opción en Platform Services Controller y, a continuación, ejecute la utilidad nuevamente en los demás nodos y seleccione `Replace Machine SSL certificate with VMCA Certificate` y `Replace Solution user certificates with VMCA certificates`.

Al ejecutar este comando, vSphere Certificate Manager solicita la contraseña y la información de certificado, y almacena toda la información, excepto la contraseña, en el archivo `certtool.cfg`. Después de eso, la detención de servicios, el reemplazo de todos los certificados y el reinicio de los procesos son tareas automáticas. Se le solicita la siguiente información:

- Contraseña de `administrator@vsphere.local`.
- Código de país de dos letras

- Nombre de empresa
- Nombre de organización
- Unidad de organización
- Estado
- Localidad
- Dirección IP (opcional)
- Correo electrónico
- Nombre del host, es decir, el nombre de dominio completo de la máquina para la que desea reemplazar el certificado
- Dirección IP de Platform Services Controller si ejecuta el comando en un nodo de administración

#### Requisitos previos

Es necesario saber cuál es el FQDN de la máquina para la que se desea generar un certificado firmado por VMCA nuevo. Las demás propiedades tienen los valores predeterminados. La dirección IP es opcional.

#### Pasos siguientes

Después de reemplazar el certificado raíz en una implementación de varios nodos, debe reiniciar los servicios en todas las instancias de vCenter Server con nodos de Platform Services Controller externo.

## Convertir a VMCA en una entidad de certificación intermedia (Certificate Manager)

Es posible convertir a VMCA en una entidad de certificación intermedia si se siguen las solicitudes del sistema desde la utilidad Certificate Manager. Una vez completado el proceso, VMCA firmará todos los certificados nuevos con la cadena completa. Si lo desea, puede utilizar Certificate Manager para reemplazar todos los certificados existentes por nuevos certificados firmados por VMCA.

## Generar una CSR con vSphere Certificate Manager y preparar certificados raíz (CA intermedia)

Se puede utilizar vSphere Certificate Manager para generar solicitudes de firma del certificado (CSR). Envíe esas CSR a la CA de la empresa o a una entidad de certificación externa para su firma. Los certificados firmados se pueden utilizar en los diversos procesos de reemplazo de certificados compatibles.

- Se puede utilizar vSphere Certificate Manager para crear la CSR.



- Si prefiere crear la CSR de forma manual, el certificado que envíe para firmar debe cumplir con los siguientes requisitos.
  - Tamaño de clave: 2.048 bits o más
  - Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8
  - x509 versión 3
  - Si utiliza certificados personalizados, la extensión CA debe establecerse con el valor true para certificados de raíz, y el signo cert debe estar en la lista de requisitos.
  - La firma CRL debe estar habilitada.
  - El uso mejorado de clave no debe contener autenticación de cliente ni autenticación de servidor.
  - No hay límite explícito a la longitud de la cadena de certificados. VMCA utiliza el valor predeterminado de OpenSSL, que es de diez certificados.
  - No se admiten los certificados con comodines o con más de un nombre DNS.
  - No se pueden crear CA subsidiarias de VMCA.

Para obtener un ejemplo de uso de Microsoft Certificate Authority, consulte el artículo 2112009 de la base de conocimientos de VMware, Cómo crear una plantilla de Microsoft Certificate Authority para la creación de certificados SSL en vSphere 6.0.

### Requisitos previos

vSphere Certificate Manager solicita información. Las solicitudes dependen del entorno y del tipo de certificado que se desea reemplazar.

Para cualquier tipo de generación de CSR, se solicita la contraseña del usuario administrator@vsphere.local o el administrador del dominio de vCenter Single Sign-On con el que se desea establecer la conexión.

### Procedimiento

- 1 Inicie vSphere Certificate Manager y seleccione la opción 2.

Inicialmente, esta opción se utiliza para generar la CSR, no para reemplazar los certificados.

- 2 Si el sistema lo solicita, proporcione la contraseña y la dirección IP o el nombre de host de Platform Services Controller.

- 3 Seleccione la opción 1 para generar la CSR y responda las solicitudes.

Es necesario especificar un directorio como parte de este proceso. Certificate Manager coloca el certificado para su firma (archivo \*.csr) y el archivo de clave correspondiente (archivo \*.key) en el directorio.

- 4 Envíe el certificado para su firma a la CA externa o de la empresa. El archivo debe tener el nombre root\_signing\_cert.cer.

5 En un editor de texto, combine el certificado de la siguiente manera.

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

6 Guarde el archivo como `root_signing_chain.cer`.

### Pasos siguientes

Reemplace el certificado raíz existente por el certificado raíz en cadena. Consulte [Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazo de todos los certificados](#).

## Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazo de todos los certificados

Se puede reemplazar el certificado raíz de VMCA por un certificado firmado por una entidad de certificación en el que se incluya VMCA como certificado intermedio en la cadena de certificados. Más adelante, todos los certificados generados por VMCA incluirán la cadena completa.

vSphere Certificate Manager se ejecuta en una instalación integrada o en una instancia externa de Platform Services Controller para reemplazar el certificado raíz de VMCA por un certificado de firma personalizado.

vSphere Certificate Manager solicita la siguiente información:

### Requisitos previos

- Genere la CSR.
  - Se puede utilizar vSphere Certificate Manager para crear la CSR. Consulte [Generar una CSR con vSphere Certificate Manager y preparar certificados raíz \(CA intermedia\)](#)
  - Si prefiere crear la CSR de forma manual, el certificado que envíe para firmar debe cumplir con los siguientes requisitos:
    - Tamaño de clave: 2.048 bits o más
    - Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8
    - x509 versión 3
    - Si utiliza certificados personalizados, la extensión CA debe establecerse con el valor true para certificados de raíz, y el signo cert debe estar en la lista de requisitos.
    - La firma CRL debe estar habilitada.

- El uso mejorado de clave no debe contener autenticación de cliente ni autenticación de servidor.
- No hay límite explícito a la longitud de la cadena de certificados. VMCA utiliza el valor predeterminado de OpenSSL, que es de diez certificados.
- No se admiten los certificados con comodines o con más de un nombre DNS.
- No se pueden crear CA subsidiarias de VMCA.

Para obtener un ejemplo de uso de Microsoft Certificate Authority, consulte el artículo 2112009 de la base de conocimientos de VMware, [Cómo crear una plantilla de Microsoft Certificate Authority para la creación de certificados SSL en vSphere 6.0](#).

- Una vez que reciba el certificado de una entidad de certificación empresarial o externa, combínelo con el certificado raíz inicial de VMCA para generar una cadena completa con el certificado raíz de VMCA en la parte inferior. Consulte [Generar una CSR con vSphere Certificate Manager y preparar certificados raíz \(CA intermedia\)](#).
- Recopile la información necesaria.
  - Contraseña de administrator@vsphere.local.
  - Un certificado personalizado válido para la raíz (archivo .crt).
  - Clave personalizada válida para la raíz (archivo .key).

## Procedimiento

- 1 Inicie vSphere Certificate Manager en una instalación integrada o en una instancia de Platform Services Controller externa y seleccione la opción 2.
- 2 Seleccione la opción 2 para iniciar el reemplazo de certificados y responder a las solicitudes.
  - a Especifique la ruta de acceso completa al certificado raíz cuando se le solicite.
  - b Si es la primera vez que reemplaza los certificados, se le solicitará información que se utilizará para el certificado SSL de máquina.
 

Esta información incluye el FQDN obligatorio de la máquina y se almacena en el archivo `certtool.cfg`.
- 3 Si se reemplaza el certificado raíz en una implementación de varios nodos, debe reiniciar los servicios en todas las instancias de vCenter Server.
- 4 En implementaciones de varios nodos, para regenerar todos los certificados en cada instancia de vCenter Server, utilice la opción 3 (Reemplazar certificado SSL de máquina por certificado de VMCA) y la opción 6 (Reemplazar certificados de usuario de solución por certificados de VMCA).

Al reemplazar los certificados, VMCA firma con la cadena completa.

## Pasos siguientes

Según el entorno, es posible que sea necesario reemplazar de forma explícita otros certificados.

- Si la directiva de la empresa requiere que se reemplacen todos los certificados, reemplace el certificado raíz vmdir. Consulte [Reemplazar certificado para VMware Directory Service](#)
- Si desea realizar una actualización desde un entorno de vSphere 5.x, es posible que deba reemplazar el certificado de vCenter Single Sign-On dentro de vmdir. Consulte [Reemplazar el certificado de VMware Directory Service en entornos de modo mixto](#)

## Reemplazar un certificado SSL de máquina por un certificado de VMCA (entidad de certificación intermedia)

En una implementación de varios nodos donde se utiliza VMCA como entidad de certificación intermedia, es necesario reemplazar de forma explícita el certificado SSL de máquina. Primero, se debe reemplazar el certificado raíz de VMCA en el nodo de Platform Services Controller y, a continuación, se pueden reemplazar los certificados en los nodos de vCenter Server para tener la firma de la cadena completa en los certificados. También se puede utilizar esta opción para reemplazar certificados SSL de máquina que se encuentren dañados o a punto de caducar.

Al reemplazar el certificado SSL de máquina existente por un nuevo certificado firmado por VMCA, vSphere Certificate Manager solicita información e introduce todos los valores, excepto la contraseña y la dirección IP de Platform Services Controller, en el archivo `certtool.cfg`.

- Contraseña de administrator@vsphere.local.
- Código de país de dos letras
- Nombre de empresa
- Nombre de organización
- Unidad de organización
- Estado
- Localidad
- Dirección IP (opcional)
- Correo electrónico
- Nombre del host, es decir, el nombre de dominio completo de la máquina para la que se desea reemplazar el certificado. Si el nombre del host no coincide con el FQDN, el reemplazo de los certificados no se completa correctamente y el entorno puede quedar en un estado inestable.
- Dirección IP de Platform Services Controller si ejecuta el comando en un nodo de administración

## Requisitos previos

- Si reemplazó el certificado raíz de VMCA en una implementación de varios nodos, reinicie de forma explícita todos los nodos de vCenter Server.

- Para ejecutar Certificate Manager con esta opción, se necesita la siguiente información.
  - Contraseña de administrator@vsphere.local.
  - FQDN de la máquina para la cual se desea generar un nuevo certificado firmado por VMCA. Las demás propiedades tienen los valores predeterminados, pero pueden cambiarse.
  - Nombre de host o dirección IP de Platform Services Controller si se ejecuta en un sistema vCenter Server con una instancia de Platform Services Controller externa.

#### Procedimiento

- 1 Inicie vSphere Certificate Manager y seleccione la opción 3.
- 2 Responda las solicitudes del sistema.

Certificate Manager almacenará la información en el archivo `certtool.cfg`.

#### Resultados

vSphere Certificate Manager reemplazará el certificado SSL de máquina.

### Reemplazar certificados de usuario de solución por certificados de VMCA (entidad de certificación intermedia)

En una implementación de varios nodos donde se utiliza VMCA como entidad de certificación intermedia, es necesario reemplazar de forma explícita los certificados de usuario de solución. Primero, se debe reemplazar el certificado raíz de VMCA en el nodo de Platform Services Controller y, a continuación, se pueden reemplazar los certificados en los nodos de vCenter Server para tener la firma de la cadena completa en los certificados. También se puede utilizar esta opción para reemplazar certificados de usuario de solución que se encuentren dañados o a punto de caducar.

#### Requisitos previos

- Si reemplazó el certificado raíz de VMCA en una implementación de varios nodos, reinicie de forma explícita todos los nodos de vCenter Server.
- Para ejecutar Certificate Manager con esta opción, se necesita la siguiente información.
  - Contraseña de administrator@vsphere.local.
  - Nombre de host o dirección IP de Platform Services Controller si se ejecuta en un sistema vCenter Server con una instancia de Platform Services Controller externa.

#### Procedimiento

- 1 Inicie vSphere Certificate Manager y seleccione la opción 6.
- 2 Responda las solicitudes del sistema.

#### Resultados

vSphere Certificate Manager reemplazará todos los certificados de usuario de solución.

## Reemplazar todos los certificados por certificados personalizados (Certificate Manager)

Es posible usar la utilidad vSphere Certificate Manager para reemplazar todos los certificados por certificados personalizados. Antes de iniciar el proceso, es necesario enviar solicitudes de firma de certificado (CSR) a la entidad de certificación. Se puede utilizar Certificate Manager para generar las CSR.

Una opción es reemplazar solamente los certificados SSL de máquina y utilizar los certificados de usuario de solución que proporciona VMCA. Los certificados de usuario de solución se utilizan únicamente entre los componentes de vSphere.

Si utiliza certificados personalizados, usted será el responsable de aprovisionar cada nodo que agregue al entorno con certificados personalizados. VMCA seguirá aprovisionando los certificados firmados por VMCA, pero usted será el responsable de reemplazar esos certificados. Puede usar la utilidad vSphere Certificate Manager o realizar el reemplazo manual de certificados mediante la CLI. Los certificados se almacenarán en VECS.

### Generar solicitudes de firma de certificado con vSphere Certificate Manager (certificados personalizados)

Es posible utilizar vSphere Certificate Manager para generar solicitudes de firma de certificado (CSR) y, a continuación, enviarlas a la entidad de certificación empresarial o a una entidad de certificación externa. Los certificados se pueden utilizar en los diversos procesos de reemplazo de certificados compatibles.

Puede ejecutar la herramienta Certificate Manager en la línea de comandos de la siguiente manera:

#### Windows

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

#### Linux

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

#### Requisitos previos

vSphere Certificate Manager solicita información. La solicitud depende del entorno y del tipo de certificado que se desea reemplazar.

- Para cualquier tipo de generación de CSR, se solicita la contraseña del usuario administrator@vsphere.local o el administrador del dominio de vCenter Single Sign-On con el que se desea establecer la conexión.
- Cuando se desea generar una CSR en un entorno con una instancia externa de Platform Services Controller, se solicita el nombre de host o la dirección IP de Platform Services Controller.

- Para generar una CSR para un certificado SSL de máquina, se solicitan las propiedades del certificado, que están almacenadas en el archivo `certtool.cfg`. En la mayoría de los campos, se puede aceptar el valor predeterminado o proporcionar valores específicos del sitio. Se requiere el FQDN de la máquina.

#### Procedimiento

- 1 En cada máquina del entorno, inicie vSphere Certificate Manager y seleccione la opción 1.
- 2 Si el sistema lo solicita, proporcione la contraseña y la dirección IP o el nombre de host de Platform Services Controller.
- 3 Seleccione la opción 1 para generar la CSR, responda las solicitudes del sistema y salga de Certificate Manager.

Es necesario especificar un directorio como parte de este proceso. Certificate Manager colocará el certificado y los archivos de claves en el directorio.

- 4 Si también desea reemplazar todos los certificados de usuario de solución, reinicie Certificate Manager.
- 5 Seleccione la opción 5.

- 6 Si el sistema lo solicita, proporcione la contraseña y la dirección IP o el nombre de host de Platform Services Controller.

- 7 Seleccione la opción 1 para generar las CSR, responda las solicitudes del sistema y salga de Certificate Manager.

Es necesario especificar un directorio como parte de este proceso. Certificate Manager colocará el certificado y los archivos de claves en el directorio.

En cada nodo de Platform Services Controller, Certificate Manager generará un certificado y un par de claves. En cada nodo de vCenter Server, Certificate Manager generará cuatro certificados y pares de claves.

#### Pasos siguientes

Realice el reemplazo de certificados.

### Reemplazar un certificado SSL de máquina por un certificado personalizado

El certificado SSL de máquina se utiliza en el servicio de proxy inverso de cada nodo de administración, en Platform Services Controller y en la implementación integrada. Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. Puede reemplazar el certificado de cada nodo por un certificado personalizado.

#### Requisitos previos

Antes de comenzar, se necesita una CSR para cada máquina del entorno. La CSR se puede generar mediante vSphere Certificate Manager o de forma explícita.

- 1 Para generar la CSR mediante vSphere Certificate Manager, consulte [Generar solicitudes de firma de certificado con vSphere Certificate Manager \(certificados personalizados\)](#).

- 2 Para generar la CSR de forma explícita, solicite un certificado para cada máquina a la entidad de certificación empresarial o externa. El certificado debe cumplir con los siguientes requisitos:

- Tamaño de clave: 2.048 bits o más (formato codificado PEM)
- Formato CRT
- x509 versión 3
- SubjectAltName debe contener DNS Name=<machine\_FQDN>
- Contiene los siguientes usos de claves: firma digital, no repudio, cifrado de clave

Consulte también el artículo de la base de conocimientos de VMware [Obtaining vSphere certificates from a Microsoft Certificate Authority \(2112014\)](#).

#### Procedimiento

- 1 Inicie vSphere Certificate Manager y seleccione la opción 1.
- 2 Seleccione la opción 2 para iniciar el reemplazo de certificados y responder a las solicitudes. vSphere Certificate Manager solicita la siguiente información:
  - Contraseña de administrator@vsphere.local.
  - Un certificado SSL de máquina personalizado y válido (archivo .crt).
  - Una clave SSL de máquina personalizada y válida (archivo .key).
  - Un certificado de firma válido para el certificado SSL de máquina personalizado (archivo .crt).
  - La dirección IP de Platform Services Controller si el comando se ejecuta en un nodo de administración dentro de una implementación de varios nodos.

#### Pasos siguientes

Según el entorno, es posible que sea necesario reemplazar de forma explícita otros certificados.

- Si la directiva de la empresa requiere que se reemplacen todos los certificados, reemplace el certificado raíz vmdir. Consulte [Reemplazar certificado para VMware Directory Service](#)
- Si desea realizar una actualización desde un entorno de vSphere 5.x, es posible que deba reemplazar el certificado de vCenter Single Sign-On dentro de vmdir. Consulte [Reemplazar el certificado de VMware Directory Service en entornos de modo mixto](#)

### Reemplazar los certificados de usuarios de soluciones con certificados personalizados

Muchas empresas solo requieren que reemplace los certificados de los servicios a los que se puede acceder externamente. Sin embargo, Certificate Manager también permite reemplazar certificados de usuarios de solución. Los usuarios de solución son recopilaciones de servicios, por ejemplo, todos los servicios que están asociados con vSphere Web Client. En las implementaciones de varios nodos debe reemplazar el certificado de usuario de solución del



equipo en la instancia de Platform Services Controller y el conjunto completo de usuarios de solución en cada nodo de administración.

Cuando se le solicite un certificado de usuario de solución, proporcione la cadena de certificados de firma completa de la entidad de certificación externa.

El formato debe ser similar al siguiente mensaje.

```
-----BEGIN CERTIFICATE-----
Signing certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

### Requisitos previos

Antes de comenzar, se necesita una CSR para cada máquina del entorno. La CSR se puede generar mediante vSphere Certificate Manager o de forma explícita.

- 1 Para generar la CSR mediante vSphere Certificate Manager, consulte [Generar solicitudes de firma de certificado con vSphere Certificate Manager \(certificados personalizados\)](#).
- 2 Solicite un certificado para cada usuario de solución en cada nodo a la CA empresarial o externa. Puede generar la CSR mediante vSphere Certificate Manager o prepararla usted mismo. La CSR debe cumplir con los siguientes requisitos:
  - Tamaño de clave: 2.048 bits o más (formato codificado PEM)
  - Formato CRT
  - x509 versión 3
  - SubjectAltName debe contener DNS Name=<machine\_FQDN>
  - Cada certificado de usuario de solución debe tener un `Subject` diferente. Por ejemplo, considere incluir el nombre de usuario de solución (como `vpzd`) u otro identificador único.
  - Contiene los siguientes usos de claves: firma digital, no repudio, cifrado de clave

Consulte también el artículo de la base de conocimientos de VMware [Obtaining vSphere certificates from a Microsoft Certificate Authority \(2112014\)](#).

### Procedimiento

- 1 Inicie vSphere Certificate Manager y seleccione la opción 5.
- 2 Seleccione la opción 2 para iniciar el reemplazo de certificados y responder a las solicitudes. vSphere Certificate Manager solicita la siguiente información:
  - Contraseña de `administrator@vsphere.local`.

- Certificado y clave del usuario de solución de la máquina.
- Si se ejecuta vSphere Certificate Manager en un nodo de Platform Services Controller, se solicita el certificado y la clave (`vpzd.crt` y `vpzd.key`) del usuario de solución de la máquina.
- Si se ejecuta vSphere Certificate Manager en un nodo de administración o en una implementación integrada, se solicita el conjunto completo de certificados y claves (`vpzd.crt` y `vpzd.key`) de todos los usuarios de solución.

#### Pasos siguientes

Si desea realizar una actualización desde un entorno de vSphere 5.x, es posible que deba reemplazar el certificado de vCenter Single Sign-On dentro de vmdir. Consulte [Reemplazar el certificado de VMware Directory Service en entornos de modo mixto](#).

## Reemplazar certificados de forma manual

En algunos casos especiales, por ejemplo, si desea reemplazar solo un tipo de certificado de usuario de solución, no puede utilizar la utilidad vSphere Certificate Manager. En ese caso, puede usar las CLI incluidas en la instalación para el reemplazo de certificados.

### Descripción general de cómo iniciar y detener servicios

Para determinadas partes del reemplazo manual de certificados, se deben detener todos los servicios y, a continuación, iniciar únicamente los servicios que administran la infraestructura de certificados. Al detener los servicios solo cuando es necesario, se reduce el tiempo de inactividad.

Siga estas reglas generales.

- No detenga los servicios para generar nuevos pares de claves públicas/privadas o nuevos certificados.
- Si es el único administrador, no es necesario que detenga los servicios al agregar un nuevo certificado raíz. El certificado raíz anterior sigue disponible y todos los servicios pueden seguir autenticándose con ese certificado. Una vez que se haya agregado el certificado raíz, detenga y reinicie de inmediato todos los servicios para evitar problemas con los hosts.
- Si el entorno incluye varios administradores, detenga los servicios antes de agregar un nuevo certificado raíz y reinícelos una vez que se haya agregado el nuevo certificado.
- Detenga los servicios justo antes de realizar estas tareas:
  - Eliminar un certificado SSL de máquina o cualquier certificado de usuario de solución en VECS.
  - Reemplazar un certificado de usuario de solución en vmdir (VMware Directory Service).

## Reemplazar certificados firmados por VMCA existentes por certificados firmados por VMCA nuevos

Si el certificado raíz de VMCA está por caducar, o si desea reemplazarlo por otros motivos, puede generar un certificado raíz nuevo y agregarlo a VMware Directory Service. A continuación, puede generar certificados SSL de máquina y certificados de usuarios de solución nuevos mediante el certificado raíz nuevo.

Use la utilidad vSphere Certificate Manager para reemplazar certificados en la mayoría de los casos.

Si necesita tener un control detallado, este caso ofrece instrucciones detalladas paso a paso para reemplazar el conjunto completo de certificados mediante comandos de CLI. O bien puede reemplazar certificados individuales mediante el procedimiento de la tarea correspondiente.

### Requisitos previos

Solo `administrator@vsphere.local` u otros usuarios del grupo Administradores de CA pueden realizar tareas de administración de certificados. Consulte [Agregar miembros a un grupo de vCenter Single Sign-On](#).

### Procedimiento

#### 1 Generar un nuevo certificado raíz firmado por VMCA

Puede generar nuevos certificados firmados por VMCA con la CLI `certool` y publicarlos en `vmdir`.

#### 2 Reemplazar certificados SSL de máquina por certificados firmados por VMCA

Después de generar un nuevo certificado raíz firmado por VMCA, puede reemplazar todos los certificados SSL de máquina en el entorno.

#### 3 Reemplazar los certificados de usuario de solución por certificados nuevos firmados por VMCA

Después de reemplazar los certificados SSL de máquina, puede reemplazar todos los certificados de usuarios de solución. Los certificados de usuario de solución deben ser válidos, es decir, que no estén caducados, pero la infraestructura de certificados no utiliza ninguna otra información del certificado.

#### 4 Reemplazar el certificado de VMware Directory Service en entornos de modo mixto

Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

## Generar un nuevo certificado raíz firmado por VMCA

Puede generar nuevos certificados firmados por VMCA con la CLI `certool` y publicarlos en `vmdir`.

En una implementación de varios nodos, los comandos para generar certificados raíz se ejecutan en Platform Services Controller.

### Procedimiento

- 1 Genere un nuevo certificado autofirmado y una clave privada.

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config <config_file>
```

- 2 Reemplace el certificado raíz existente con el nuevo certificado.

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

El comando genera el certificado, lo agrega a vmdir y, a continuación, lo agrega a VECS.

- 3 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

### Windows

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

### vCenter Server Appliance

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

- 4 (opcional) Publique el nuevo certificado raíz en vmdir.

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

Al ejecutar este comando, todas las instancias de vmdir se actualizan inmediatamente. De otro modo, la propagación a todas las instancias puede demorar un poco.

- 5 Reinicie todos los servicios.

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

**Ejemplo: Generar un nuevo certificado raíz firmado por VMCA**

El siguiente ejemplo muestra el conjunto completo de pasos para comprobar la información de la entidad de certificación raíz actual y volver a generar la certificación raíz.

- 1 (Opcional) Enumere el certificado raíz de VMCA para asegurarse de que se encuentre en el almacén de certificados.

- En una instalación integrada o un nodo de Platform Services Controller:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca
```

- En un nodo de administración (instalación externa):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca --server=<psc-  
ip-or-fqdn>
```

La salida se parece a esto:

```
output:
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      cf:2d:ff:49:88:50:e5:af
    ...
```

- 2 (Opcional) Enumere el almacén TRUSTED\_ROOTS de VECS y compare el número de serie del certificado con la salida del paso 1.

Este comando funciona tanto en nodos de Platform Services Controller como de administración, ya que VECS mide vmdir.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry list --store TRUSTED_ROOTS  
--text
```

En el caso más simple con un solo certificado raíz, la salida se parece a esto:

```
Number of entries in store :    1
Alias : 960d43f31eb95211ba3a2487ac840645a02894bd
Entry type :    Trusted Cert
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      cf:2d:ff:49:88:50:e5:af
```

- 3 Genere un nuevo certificado raíz de VMCA. El certificado se agrega al almacén TRUSTED\_ROOTS en VECS y en vmdir (VMware Directory Service).

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program  
Files\VMware\vCenter Server\vmcad\certool.cfg"
```

En Windows, `--config` es opcional porque el comando usa el archivo predeterminado `certool.cfg`.

## Reemplazar certificados SSL de máquina por certificados firmados por VMCA

Después de generar un nuevo certificado raíz firmado por VMCA, puede reemplazar todos los certificados SSL de máquina en el entorno.

Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. En una implementación de varios nodos, debe ejecutar los comandos de generación de certificados SSL de máquina en cada nodo. Use el parámetro `--server` para apuntar a Platform Services Controller desde vCenter Server con Platform Services Controller externo.

### Requisitos previos

Prepárese para detener todos los servicios e iniciar los servicios que controlan la propagación y el almacenamiento de certificados.

### Procedimiento

- 1 Haga una copia de `certool.cfg` para cada máquina que necesite un certificado nuevo.

Puede encontrar `certool.cfg` en las siguientes ubicaciones:

Sistema operativo	Ruta de acceso
Windows	C:\Archivos de programa\VMware\vCenter Server\vmcad
Linux	/usr/lib/vmware-vmca/share/config/

- 2 Editar archivo de configuración personalizado de cada máquina a fin de incluir el FQDN de la máquina.

Ejecute `NSLookup` sobre la dirección IP de la máquina a fin de ver el listado de DNS del nombre y usar ese nombre en el campo Nombre de host del archivo.

- 3 Genere un par de archivos de clave pública/privada y un certificado para cada archivo pasando el archivo de configuración que acaba de personalizar.

Por ejemplo:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --
config machine1.cfg
```

- 4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

### Windows

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

### vCenter Server Appliance

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

- 5 Agregue el certificado nuevo a VECS.

Todas las máquinas necesitan el certificado nuevo en el almacén de certificados local para comunicarse mediante SSL. Primero debe eliminar la entrada existente y, a continuación, agregar la nueva.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

- 6 Reinicie todos los servicios.

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

### Ejemplo: Reemplazo de certificados de una máquina por certificados firmados por VMCA

- 1 Cree un archivo de configuración para el certificado SSL y guárdelo como `ssl-config.cfg` en el directorio actual.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

- 2 Genere un par de claves para el certificado SSL de máquina. Ejecute este comando en cada nodo de administración y en el nodo de Platform Services Controller. No se requiere la opción `--server`.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

Los archivos `ssl-key.priv` y `ssl-key.pub` se crean en el directorio actual.

- 3 Genere el nuevo certificado SSL de máquina. Este certificado está firmado por VMCA. Si reemplazó el certificado raíz de VMCA por un certificado personalizado, VMCA firma todos los certificados con la cadena completa.

- En una instalación integrada o un nodo de Platform Services Controller:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- En vCenter Server (instalación externa):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

El archivo `new-vmca-ssl.crt` se crea en el directorio actual.

- 4 (Opcional) Enumere el contenido de VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli store list
```

- Establezca Platform Services Controller como salida:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Establezca vCenter Server como salida:

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



- 5 Reemplace el certificado SSL de máquina en VECS por el nuevo certificado SSL de máquina. Los valores `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados.

- En Platform Services Controller, ejecute el siguiente comando para actualizar el certificado SSL de máquina en el almacén MACHINE\_SSL\_CERT.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- En cada nodo de administración o en la implementación integrada, ejecute el siguiente comando para actualizar el certificado SSL de máquina en el almacén MACHINE\_SSL\_CERT. Debe actualizar el certificado para cada máquina por separado, ya que cada una de ellas tiene un FQDN diferente.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

### Pasos siguientes

También puede reemplazar los certificados de sus hosts ESXi. Consulte la publicación *Seguridad de vSphere*.

Después de reemplazar el certificado raíz en una implementación de varios nodos, debe reiniciar los servicios en todas las instancias de vCenter Server con nodos de Platform Services Controller externo.

### Reemplazar los certificados de usuario de solución por certificados nuevos firmados por VMCA

Después de reemplazar los certificados SSL de máquina, puede reemplazar todos los certificados de usuarios de solución. Los certificados de usuario de solución deben ser válidos, es decir, que no estén caducados, pero la infraestructura de certificados no utiliza ninguna otra información del certificado.

Debe reemplazar el certificado de usuario de solución de la máquina en cada nodo de administración y en cada nodo de Platform Services Controller. Debe reemplazar los certificados de usuarios de solución solo en cada nodo de administración. Utilice el parámetro `--server` para apuntar a Platform Services Controller cuando ejecute comandos en un nodo de administración con una instancia externa de Platform Services Controller.

**Nota** Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

### Requisitos previos

Prepárese para detener todos los servicios e iniciar los servicios que controlan la propagación y el almacenamiento de certificados.

### Procedimiento

- 1 Haga una copia de `certtool.cfg`, quite los campos Nombre, Dirección IP, Correo electrónico y Nombre DNS, y cambie el nombre del archivo: por ejemplo, a `sol_usr.cfg`.

Se pueden nombrar los certificados desde la línea de comandos como parte de la generación. La otra información no es necesaria para los usuarios de solución. Si se deja la información predeterminada, los certificados generados podrían resultar confusos.

- 2 Genere un par de archivos de clave pública/privada y un certificado para cada usuario de solución y pase el archivo de configuración que recién personalizó.

Por ejemplo:

```
certtool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certtool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

- 3 Busque el nombre de cada usuario de solución.

```
dir-cli service list
```

Puede usar el identificador único que se devuelve al reemplazar los certificados. La entrada y la salida deben verse de la siguiente manera.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Cuando enumera certificados de usuario de solución en implementaciones de varios nodos, el resultado de la lista de `dir-cli` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

- 4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

### Windows

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

### vCenter Server Appliance

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

- 5 En cada usuario de solución, reemplace el certificado actual en `vmdir` y, a continuación, en `VECS`.

El siguiente ejemplo muestra cómo reemplazar los certificados del servicio `vpzd`.

```
dir-cli service update --name <vpzd-xxxx-xxx-7c7b769cd9f4> --cert ./vpzd.crt
vecs-cli entry delete --store vpzd --alias vpzd
vecs-cli entry create --store vpzd --alias vpzd --cert vpzd.crt --key vpzd.priv
```

---

**Nota** Los usuarios de solución no podrán autenticarse en vCenter Single Sign-On si no se reemplaza el certificado en `vmdir`.

---

- 6 Reinicie todos los servicios.

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

**Ejemplo: Usar los certificados de usuarios de solución firmados por VMCA**

- 1 Genere un par de claves pública/privada para cada usuario de solución. Esto incluye un par para el usuario de solución de la máquina en cada instancia de Platform Services Controller y en cada nodo de administración, y un par para cada usuario de solución adicional (vpxd, vpxd-extension, vsphere-webclient) en cada nodo de administración.
  - a Genere un par de claves para el usuario de solución de la máquina de una implementación integrada o para el usuario de solución de la máquina de Platform Services Controller.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- b (Opcional) Para implementaciones con una instancia de Platform Services Controller externa, genere un par de claves para el usuario de solución de la máquina en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- c Genere un par de claves para el usuario de solución vpxd en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

- d Genere un par de claves para el usuario de solución vpxd-extension en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

- e Genere un par de claves para el usuario de solución vsphere-webclient en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

- 2 Genere certificados de usuarios de solución que estén firmados con el nuevo certificado raíz de VMCA para el usuario de solución de la máquina en cada instancia de Platform Services Controller y en cada nodo de administración, así como para cada usuario de solución adicional (vpxd, vpxd-extension, vsphere-webclient) en cada nodo de administración.

---

**Nota** El parámetro `--Name` tiene que ser único. Al incluir el nombre del almacén del usuario de solución (por ejemplo, vpxd o vpxd-extension) resulta más fácil ver qué certificado se asigna a cada usuario de solución.

---

- a Ejecute el siguiente comando en el nodo de Platform Services Controller a fin de generar un certificado de usuario de solución de la máquina en ese nodo.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

- b Genere un certificado para el usuario de solución de la máquina en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

- c Genere un certificado para el usuario de solución vpxd en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

- d Genere un certificado para el usuario de solución vpxd-extensions en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

- e Ejecute el siguiente comando para generar un certificado para el usuario de solución vsphere-webclient en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

- 3 Reemplace los certificados de usuario de solución en VECS por los nuevos certificados de usuario de solución.

---

**Nota** Los parámetros `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados de los servicios.

---

- a En el nodo de Platform Services Controller, ejecute el siguiente comando para reemplazar el certificado de usuario de solución de la máquina.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b Reemplace el certificado de usuario de solución de la máquina en cada nodo de administración:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c Reemplace el certificado de usuario de solución vpxd en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

- d Reemplace el certificado de usuario de solución vpxd-extension en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

- e Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

- 4 Actualice VMware Directory Service (vmdir) con los nuevos certificados de usuarios de solución. Se solicita una contraseña de administrador de vCenter Single Sign-On.

- a Ejecute `dir-cli service list` para obtener el sufijo de identificador único de servicio para cada usuario de solución. Puede ejecutar este comando en un sistema Platform Services Controller o vCenter Server.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

**Nota** Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

- b Reemplace el certificado de máquina en vmdir de Platform Services Controller. Por ejemplo, si `machine-29a45d00-60a7-11e4-96ff-00505689639a` es el usuario de solución de la máquina en Platform Services Controller, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

- c Reemplace el certificado de la máquina en vmdir en cada nodo de administración. Por ejemplo, si `machine-6fd7f140-60a9-11e4-9e28-005056895a69` es el usuario de solución de la máquina en vCenter Server, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

- d Reemplace el certificado de usuario de solución vpxd en vmdir en cada nodo de administración. Por ejemplo, si `vpxd-6fd7f140-60a9-11e4-9e28-005056895a69` es el identificador de usuario de solución vpxd, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

- e Reemplace el certificado de usuario de solución vpxd-extension en vmdir en cada nodo de administración. Por ejemplo, si `vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69` es el identificador de usuario de solución vpxd-extension, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

- f Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo de administración. Por ejemplo, si vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vsphere-webclient, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name  
vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vmware-webclient.crt
```

### Pasos siguientes

Reinicie todos los servicios de cada nodo de Platform Services Controller y cada nodo de administración.

## Reemplazar el certificado de VMware Directory Service en entornos de modo mixto

Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

El vmdir utiliza el certificado SSL de VMware Directory Service para realizar negociaciones entre los nodos de Platform Services Controller que realizan la replicación de vCenter Single Sign-On.

Estos pasos no son necesarios para un entorno de modo mixto que incluya los nodos de vSphere 6.0 y vSphere 6.5. Estos pasos son necesarios solo si:

- El entorno incluye servicios tanto de vCenter Single Sign-On 5.5 como de vCenter Single Sign-On 6.x.
- Los servicios de vCenter Single Sign-On se configuran para replicar datos de vmdir.
- Planea reemplazar los certificados firmados por VMCA predeterminados por certificados personalizados del nodo en el que se ejecuta el servicio de vCenter Single Sign-On 6.x.

---

**Nota** Actualizar el entorno al completo antes de reiniciar los servicios es una práctica recomendada. Generalmente, el reemplazo del certificado de VMware Directory Service no se recomienda.

---

### Procedimiento

- 1 En el nodo en el que se ejecuta el servicio de vCenter Single Sign-On 6.x, reemplace el certificado SSL de vmdir y la clave.

Consulte [Reemplazar certificado para VMware Directory Service](#).



- 2 En el nodo en el que se ejecuta el servicio de vCenter Single Sign-On 5.5, configure el entorno para que se reconozca el servicio de vCenter Single Sign-On 6.x.
  - a Haga una copia de seguridad de todos los archivos  
`C:\ProgramData\VMware\CIS\cfg\vmldird.`
  - b Haga una copia del archivo `vmldircert.pem` en el nodo 6.x y cámbiele el nombre por `<sso_node2.domain.com>.pem`, donde `<sso_node2.domain.com>` es el FQDN del nodo 6.x.
  - c Copie el certificado con nombre nuevo en `C:\ProgramData\VMware\CIS\cfg\vmldird` para reemplazar el certificado de replicación existente.
- 3 Reinicie VMware Directory Service en todas las máquinas en las que reemplazó certificados.  
 Puede reiniciar el servicio desde vSphere Web Client o utilizar el comando `service-control`.

## Utilizar VMCA como entidad de certificación intermedia

Puede reemplazar el certificado raíz de VMCA por un certificado externo firmado por una entidad de certificación en la que se incluya VMCA en la cadena de certificados. Más adelante, todos los certificados generados por VMCA incluirán la cadena completa. Puede reemplazar los certificados existentes por certificados generados recientemente. Este método combina la seguridad de los certificados externos firmados por la entidad de certificación con la comodidad de la administración automática de certificados.

### Procedimiento

- 1 **Reemplazar el certificado raíz (entidad de certificación intermedia)**  
 El primer paso para reemplazar los certificados VMCA por certificados personalizados es generar una solicitud de firma de certificados (CSR) y agregar el certificado que se devuelve a VMCA como certificado raíz.
- 2 **Reemplazar certificados SSL de máquina (entidad de certificación intermedia)**  
 Después de recibir el certificado firmado de la CA y convertirlo en el certificado raíz de VMCA, puede reemplazar todos los certificados SSL de máquina.
- 3 **Reemplazar certificados de usuarios de solución (entidad de certificación intermedia)**  
 Después de reemplazar los certificados SSL de máquina, puede reemplazar los certificados de los usuarios de solución.
- 4 **Reemplazar certificado para VMware Directory Service**  
 Si decide usar un nuevo certificado raíz de VMCA, y anula la publicación del certificado raíz de VMCA que se utilizó al aprovisionar el entorno, deberá reemplazar los certificados SSL de máquina, los certificados de usuario de solución y los certificados de algunos servicios internos.

## 5 Reemplazar el certificado de VMware Directory Service en entornos de modo mixto

Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

### Reemplazar el certificado raíz (entidad de certificación intermedia)

El primer paso para reemplazar los certificados VMCA por certificados personalizados es generar una solicitud de firma de certificados (CSR) y agregar el certificado que se devuelve a VMCA como certificado raíz.

El certificado que se envía para firmar debe cumplir con los siguientes requisitos:

- Tamaño de clave: 2.048 bits o más
- Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8
- x509 versión 3
- Si utiliza certificados personalizados, la extensión CA debe establecerse con el valor true para certificados de raíz, y el signo cert debe estar en la lista de requisitos.
- La firma CRL debe estar habilitada.
- El uso mejorado de clave no debe contener autenticación de cliente ni autenticación de servidor.
- No hay límite explícito a la longitud de la cadena de certificados. VMCA utiliza el valor predeterminado de OpenSSL, que es de diez certificados.
- No se admiten los certificados con comodines o con más de un nombre DNS.
- No se pueden crear CA subsidiarias de VMCA.

Para obtener un ejemplo de uso de Microsoft Certificate Authority, consulte el artículo 2112009 de la base de conocimientos de VMware, *Cómo crear una plantilla de Microsoft Certificate Authority para la creación de certificados SSL en vSphere 6.0*.

VMCA valida los siguientes atributos de certificados al reemplazar el certificado raíz:

- Tamaño de clave de 2048 bits o más
- Uso de clave: firma de certificado
- Restricción básica: entidad de certificación de tipo sujeto

#### Procedimiento

- 1 Genere una CSR y envíela a la entidad de certificación.

Siga las instrucciones de la entidad de certificación.

- 2 Prepare un archivo de certificados que incluya el certificado VMCA firmado junto con la cadena completa de la entidad de certificación externa o empresarial y guarde el archivo, como `rootcal.crt`.

Para hacerlo, se pueden copiar todos los certificados de la entidad de certificación en formato PEM en un solo archivo. Debe empezar por el certificado raíz de VMCA y finalizar con el certificado raíz PEM de la entidad de certificación. Por ejemplo:

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

- 3 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

### Windows

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

### vCenter Server Appliance

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

- 4 Reemplace la entidad de certificación raíz VMCA existente.

```
certool --rootca --cert=rootcal.crt --privkey=root1.key
```

Al ejecutarse, este comando realiza lo siguiente:

- Agrega el nuevo certificado raíz personalizado a la ubicación de certificados en el sistema de archivos.
- Anexa el certificado raíz personalizado al almacén TRUSTED\_ROOTS en VECS (después de una demora).
- Agrega el certificado raíz personalizado a vmdir (después de una demora).

- 5 (opcional) Para propagar el cambio a todas las instancias de vmdir (VMware Directory Service), publique el nuevo certificado raíz en vmdir suministrando la ruta de acceso para cada archivo.

Por ejemplo:

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

Cada 30 segundos se produce la replicación entre los nodos de vmdir. No se necesita agregar el certificado raíz a VECS explícitamente, ya que VECS sondea vmdir cada 5 minutos en busca de nuevos archivos de certificados raíz.

- 6 (opcional) Si fuera necesario, se puede forzar la actualización de VECS.

```
vecs-cli force-refresh
```

- 7 Reinicie todos los servicios.

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

### Ejemplo: Reemplazo del certificado raíz

Reemplace el certificado raíz de VMCA por el certificado raíz personalizado de la entidad de certificación mediante el comando certtool con la opción `--rootca`.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certtool" --rootca --cert=C:\custom-  
certs\root.pem --privkey=C:\custom-certs\root.key
```

Al ejecutarse, este comando realiza lo siguiente:

- Agrega el nuevo certificado raíz personalizado a la ubicación de certificados en el sistema de archivos.
- Anexa el certificado raíz personalizado al almacén TRUSTED\_ROOTS en VECS.
- Agrega el certificado raíz personalizado a vmdir.

### Pasos siguientes

Se puede quitar el certificado raíz original de VMCA del almacén de certificados si así lo establece la directiva de la empresa. En caso de hacerlo, deberá actualizar estos certificados internos:

- Reemplace el certificado de firma de vCenter Single Sign-On. Consulte [Actualizar el certificado del servicio de token de seguridad](#).
- Reemplace el certificado de VMware Directory Service. Consulte [Reemplazar certificado para VMware Directory Service](#).

### Reemplazar certificados SSL de máquina (entidad de certificación intermedia)

Después de recibir el certificado firmado de la CA y convertirlo en el certificado raíz de VMCA, puede reemplazar todos los certificados SSL de máquina.

Estos pasos son prácticamente los mismos que los pasos para reemplazar un certificado por otro que utilice VMCA como entidad de certificación. Sin embargo, en este caso, VMCA firma todos los certificados con la cadena completa.

Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. En una implementación de varios nodos, debe ejecutar los comandos de generación de certificados SSL de máquina en cada nodo. Use el parámetro `--server` para apuntar a Platform Services Controller desde vCenter Server con Platform Services Controller externo.

### Requisitos previos

Para el certificado SSL de máquina, el `SubjectAltName` debe contener `DNS Name=<Machine FQDN>`.

### Procedimiento

- 1 Haga una copia de `certtool.cfg` para cada máquina que necesite un certificado nuevo.

Puede encontrar `certtool.cfg` en las siguientes ubicaciones:

#### Windows

`C:\Archivos de programa\VMware\vCenter Server\vmcad`

#### Linux

`/usr/lib/vmware-vmca/share/config/`

- 2 Editar archivo de configuración personalizado de cada máquina a fin de incluir el FQDN de la máquina.

Ejecute `NSLookup` sobre la dirección IP de la máquina a fin de ver el listado de DNS del nombre y usar ese nombre en el campo Nombre de host del archivo.

- 3 Genere un par de archivos de clave pública/privada y un certificado para cada máquina pasando el archivo de configuración que acaba de personalizar.

Por ejemplo:

```
certtool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certtool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

- 4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

### Windows

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

### vCenter Server Appliance

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

- 5 Agregue el certificado nuevo a VECS.

Todas las máquinas necesitan el certificado nuevo en el almacén de certificados local para comunicarse mediante SSL. Primero debe eliminar la entrada existente y, a continuación, agregar la nueva.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

- 6 Reinicie todos los servicios.

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

### Ejemplo: Reemplazo de certificados SSL de máquina (VMCA es la CA intermedia)

- 1 Cree un archivo de configuración para el certificado SSL y guárdelo como `ssl-config.cfg` en el directorio actual.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

- 2 Genere un par de claves para el certificado SSL de máquina. Ejecute este comando en cada nodo de administración y en el nodo de Platform Services Controller. No se requiere la opción `--server`.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

Los archivos `ssl-key.priv` y `ssl-key.pub` se crean en el directorio actual.

- 3 Genere el nuevo certificado SSL de máquina. Este certificado está firmado por VMCA. Si reemplazó el certificado raíz de VMCA por un certificado personalizado, VMCA firma todos los certificados con la cadena completa.

- En una instalación integrada o un nodo de Platform Services Controller:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- En vCenter Server (instalación externa):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

El archivo `new-vmca-ssl.crt` se crea en el directorio actual.

- 4 (Opcional) Enumere el contenido de VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli store list
```

- Establezca Platform Services Controller como salida:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Establezca vCenter Server como salida:

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

- 5 Reemplace el certificado SSL de máquina en VECS por el nuevo certificado SSL de máquina. Los valores `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados.

- En Platform Services Controller, ejecute el siguiente comando para actualizar el certificado SSL de máquina en el almacén MACHINE\_SSL\_CERT.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- En cada nodo de administración o en la implementación integrada, ejecute el siguiente comando para actualizar el certificado SSL de máquina en el almacén MACHINE\_SSL\_CERT. Debe actualizar el certificado para cada máquina por separado, ya que cada una de ellas tiene un FQDN diferente.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

### Pasos siguientes

También puede reemplazar los certificados de sus hosts ESXi. Consulte la publicación *Seguridad de vSphere*.

Después de reemplazar el certificado raíz en una implementación de varios nodos, debe reiniciar los servicios en todas las instancias de vCenter Server con nodos de Platform Services Controller externo.

### Reemplazar certificados de usuarios de solución (entidad de certificación intermedia)

Después de reemplazar los certificados SSL de máquina, puede reemplazar los certificados de los usuarios de solución.

Debe reemplazar el certificado de usuario de solución de la máquina en cada nodo de administración y en cada nodo de Platform Services Controller. Debe reemplazar los certificados de usuarios de solución solo en cada nodo de administración. Utilice el parámetro `--server` para apuntar a Platform Services Controller cuando ejecute comandos en un nodo de administración con una instancia externa de Platform Services Controller.

---

**Nota** Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

---



## Requisitos previos

Cada certificado de usuario de solución debe tener un `Subject` diferente. Por ejemplo, considere incluir el nombre de usuario de solución (como `vpzd`) u otro identificador único.

## Procedimiento

- 1 Haga una copia de `certtool.cfg`, quite los campos Nombre, Dirección IP, Correo electrónico y Nombre DNS, y cambie el nombre del archivo: por ejemplo, a `sol_usr.cfg`.

Se pueden nombrar los certificados desde la línea de comandos como parte de la generación. La otra información no es necesaria para los usuarios de solución. Si se deja la información predeterminada, los certificados generados podrían resultar confusos.

- 2 Genere un par de archivos de clave pública/privada y un certificado para cada usuario de solución y pase el archivo de configuración que recién personalizó.

Por ejemplo:

```
certtool --genkey --privkey=vpzd.priv --pubkey=vpzd.pub
certtool --gencert --privkey=vpzd.priv --cert vpzd.crt --Name=VPXD_1 --config sol_usr.cfg
```

- 3 Busque el nombre de cada usuario de solución.

```
dir-cli service list
```

Puede usar el identificador único que se devuelve al reemplazar los certificados. La entrada y la salida deben verse de la siguiente manera.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpzd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpzd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Cuando enumera certificados de usuario de solución en implementaciones de varios nodos, el resultado de la lista de `dir-cli` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

- 4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

### Windows

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

### vCenter Server Appliance

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

- 5 Reemplace el certificado que ya existe primero en vmdir y después en VECS.

Debe agregar los certificados en ese orden para los usuarios de solución. Por ejemplo:

```
dir-cli service update --name <vpzd-xxxx-xxx-7c7b769cd9f4> --cert ./vpzd.crt
vecs-cli entry delete --store vpzd --alias vpzd
vecs-cli entry create --store vpzd --alias vpzd --cert vpzd.crt --key vpzd.priv
```

---

**Nota** Los usuarios de solución no pueden iniciar sesión en vCenter Single Sign-On si no reemplaza el certificado en vmdir.

---

- 6 Reinicie todos los servicios.

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

### Ejemplo: Reemplazo de certificados de usuarios de solución (entidad de certificación intermedia)

- 1 Genere un par de claves pública/privada para cada usuario de solución. Esto incluye un par para el usuario de solución de la máquina en cada instancia de Platform Services Controller y en cada nodo de administración, y un par para cada usuario de solución adicional (vpzd, vpzd-extension, vsphere-webclient) en cada nodo de administración.
  - a Genere un par de claves para el usuario de solución de la máquina de una implementación integrada o para el usuario de solución de la máquina de Platform Services Controller.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- b (Opcional) Para implementaciones con una instancia de Platform Services Controller externa, genere un par de claves para el usuario de solución de la máquina en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- c Genere un par de claves para el usuario de solución vpxd en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

- d Genere un par de claves para el usuario de solución vpxd-extension en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

- e Genere un par de claves para el usuario de solución vsphere-webclient en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

- 2 Genere certificados de usuarios de solución que estén firmados con el nuevo certificado raíz de VMCA para el usuario de solución de la máquina en cada instancia de Platform Services Controller y en cada nodo de administración, así como para cada usuario de solución adicional (vpxd, vpxd-extension, vsphere-webclient) en cada nodo de administración.

---

**Nota** El parámetro `--Name` tiene que ser único. Al incluir el nombre del almacén del usuario de solución (por ejemplo, vpxd o vpxd-extension) resulta más fácil ver qué certificado se asigna a cada usuario de solución.

---

- a Ejecute el siguiente comando en el nodo de Platform Services Controller a fin de generar un certificado de usuario de solución de la máquina en ese nodo.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

- b Genere un certificado para el usuario de solución de la máquina en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

- c Genere un certificado para el usuario de solución vpxd en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

- d Genere un certificado para el usuario de solución vpxd-extensions en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\VCServer\vmcad\certtool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

- e Ejecute el siguiente comando para generar un certificado para el usuario de solución vsphere-webclient en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\VCServer\vmcad\certtool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

- 3 Reemplace los certificados de usuario de solución en VECS por los nuevos certificados de usuario de solución.

---

**Nota** Los parámetros `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados de los servicios.

---

- a En el nodo de Platform Services Controller, ejecute el siguiente comando para reemplazar el certificado de usuario de solución de la máquina.

```
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b Reemplace el certificado de usuario de solución de la máquina en cada nodo de administración:

```
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c Reemplace el certificado de usuario de solución vpxd en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

- d Reemplace el certificado de usuario de solución vpxd-extension en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

- e Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key
vsphere-webclient-key.priv
```

- 4 Actualice VMware Directory Service (vmdir) con los nuevos certificados de usuarios de solución. Se solicita una contraseña de administrador de vCenter Single Sign-On.
  - a Ejecute `dir-cli service list` para obtener el sufijo de identificador único de servicio para cada usuario de solución. Puede ejecutar este comando en un sistema Platform Services Controller o vCenter Server.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

**Nota** Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

- b Reemplace el certificado de máquina en vmdir de Platform Services Controller. Por ejemplo, si `machine-29a45d00-60a7-11e4-96ff-00505689639a` es el usuario de solución de la máquina en Platform Services Controller, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

- c Reemplace el certificado de la máquina en vmdir en cada nodo de administración. Por ejemplo, si `machine-6fd7f140-60a9-11e4-9e28-005056895a69` es el usuario de solución de la máquina en vCenter Server, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

- d Reemplace el certificado de usuario de solución vpxd en vmdir en cada nodo de administración. Por ejemplo, si vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vpxd, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

- e Reemplace el certificado de usuario de solución vpxd-extension en vmdir en cada nodo de administración. Por ejemplo, si vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vpxd-extension, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

- f Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo de administración. Por ejemplo, si vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vsphere-webclient, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

## Reemplazar certificado para VMware Directory Service

Si decide usar un nuevo certificado raíz de VMCA, y anula la publicación del certificado raíz de VMCA que se utilizó al aprovisionar el entorno, deberá reemplazar los certificados SSL de máquina, los certificados de usuario de solución y los certificados de algunos servicios internos.

Si anula la publicación del certificado raíz de VMCA, deberá reemplazar el certificado con firma de SSL que utiliza vCenter Single Sign-On. Consulte [Actualizar el certificado del servicio de token de seguridad](#). También deberá reemplazar el certificado para VMware Directory Service (vmdir).

### Requisitos previos

Solicite un certificado para vmdir a la entidad de certificación empresarial o externa.

### Procedimiento

- 1 Detenga vmdir.

#### Linux

```
service-control --stop vmdird
```

#### Windows

```
service-control --stop VMWareDirectoryService
```

- 2 Copie el certificado y la clave que acaba de generar en la ubicación de vmdir.

#### Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

#### Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 Reinicie vmdir desde vSphere Web Client o use el comando `service-control`.

#### Linux

```
service-control --start vmdird
```

#### Windows

```
service-control --start VMWareDirectoryService
```

## Reemplazar el certificado de VMware Directory Service en entornos de modo mixto

Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

El vmdir utiliza el certificado SSL de VMware Directory Service para realizar negociaciones entre los nodos de Platform Services Controller que realizan la replicación de vCenter Single Sign-On.

Estos pasos no son necesarios para un entorno de modo mixto que incluya los nodos de vSphere 6.0 y vSphere 6.5. Estos pasos son necesarios solo si:

- El entorno incluye servicios tanto de vCenter Single Sign-On 5.5 como de vCenter Single Sign-On 6.x.
- Los servicios de vCenter Single Sign-On se configuran para replicar datos de vmdir.
- Planea reemplazar los certificados firmados por VMCA predeterminados por certificados personalizados del nodo en el que se ejecuta el servicio de vCenter Single Sign-On 6.x.

---

**Nota** Actualizar el entorno al completo antes de reiniciar los servicios es una práctica recomendada. Generalmente, el reemplazo del certificado de VMware Directory Service no se recomienda.

---

**Procedimiento**

- 1 En el nodo en el que se ejecuta el servicio de vCenter Single Sign-On 6.x, reemplace el certificado SSL de vmdird y la clave.  
 Consulte [Reemplazar certificado para VMware Directory Service](#).
- 2 En el nodo en el que se ejecuta el servicio de vCenter Single Sign-On 5.5, configure el entorno para que se reconozca el servicio de vCenter Single Sign-On 6.x.
  - a Haga una copia de seguridad de todos los archivos  
`C:\ProgramData\VMware\CIS\cfg\vmdird`.
  - b Haga una copia del archivo `vmdircert.pem` en el nodo 6.x y cámbiele el nombre por `<sso_node2.domain.com>.pem`, donde `<sso_node2.domain.com>` es el FQDN del nodo 6.x.
  - c Copie el certificado con nombre nuevo en `C:\ProgramData\VMware\CIS\cfg\vmdird` para reemplazar el certificado de replicación existente.
- 3 Reinicie VMware Directory Service en todas las máquinas en las que reemplazó certificados.  
 Puede reiniciar el servicio desde vSphere Web Client o utilizar el comando `service-control`.

**Usar certificados de terceros con vSphere**

Si la directiva de la empresa lo requiere, puede reemplazar todos los certificados que se utilizan en vSphere por certificados firmados por CA de terceros. Si lo hace, VMCA no estará en su cadena de certificados, pero todos los certificados de vCenter deberán almacenarse en VECS.

Puede reemplazar todos los certificados o utilizar una solución híbrida. Por ejemplo, considere reemplazar todos los certificados que se utilizan para el tráfico de red y dejar los certificados de usuarios de solución firmados por VMCA. Los certificados de usuarios de solución se utilizan solo para la autenticación en vCenter Single Sign-On.

---

**Nota** Si no desea utilizar VMCA, es su responsabilidad reemplazar todos los certificados, aprovisionar componentes nuevos con certificados y hacer un seguimiento de la caducidad de los certificados.

---

**Procedimiento**

- 1 [Solicitar certificados e importar un certificado raíz personalizado](#)  
 Si la directiva de la empresa no permite una CA intermedia, VMCA no puede generar los certificados. Debe utilizar certificados personalizados de una CA de la empresa o externa.
- 2 [Reemplazar certificados SSL de máquina por certificados personalizados](#)  
 Después de recibir los certificados personalizados, puede reemplazar los certificados de cada máquina.



**3 Reemplazar los certificados de usuarios de soluciones con certificados personalizados**

Después de reemplazar los certificados SSL de máquina, puede reemplazar los certificados de usuarios de solución firmados por VMCA con certificados externos o empresariales.

**4 Reemplazar certificado para VMware Directory Service**

Si decide usar un nuevo certificado raíz de VMCA, y anula la publicación del certificado raíz de VMCA que se utilizó al aprovisionar el entorno, deberá reemplazar los certificados SSL de máquina, los certificados de usuario de solución y los certificados de algunos servicios internos.

**5 Reemplazar el certificado de VMware Directory Service en entornos de modo mixto**

Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

**Solicitar certificados e importar un certificado raíz personalizado**

Si la directiva de la empresa no permite una CA intermedia, VMCA no puede generar los certificados. Debe utilizar certificados personalizados de una CA de la empresa o externa.

**Requisitos previos**

El certificado debe cumplir con los siguientes requisitos:

- Tamaño de clave: 2.048 bits o más (formato codificado PEM)
- Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8
- x509 versión 3
- Para los certificados raíz, la extensión CA se debe establecer en true y el signo cert debe estar en la lista de requisitos.
- SubjectAltName debe contener DNS Name=<machine\_FQDN>
- Formato CRT
- Contiene los siguientes usos de claves: firma digital, no repudio, cifrado de clave
- Hora de inicio de un día anterior a la hora actual
- CN (y SubjectAltName) establecidos con el nombre de host (o dirección IP) que el host ESXi tiene en el inventario de vCenter Server.

**Procedimiento**

- 1 Envíe CSR para los siguientes certificados al proveedor de certificados de la empresa o externo.
  - Un certificado SSL de máquina para cada máquina. Para el certificado SSL de máquina, el campo SubjectAltName debe contener el nombre de dominio completo (DNS NAME= *machine\_FQDN*)
  - De forma opcional, cuatro certificados de usuario de solución para cada sistema o nodo de administración integrados. Los certificados de usuario de solución no deben incluir dirección IP, nombre de host ni dirección de correo electrónico. Cada certificado debe tener un asunto de certificado diferente.

Generalmente, el resultado es un archivo PEM para la cadena de confianza, junto con los certificados SSL firmados para cada sistema Platform Services Controller o nodo de administración.

- 2 Enumere los almacenes TRUSTED\_ROOTS y SSL de máquina.

```
vecs-cli store list
```

- a Asegúrese de que el certificado raíz actual y todos los certificados SSL de máquina estén firmados por VMCA.
  - b Anote el contenido de los campos Número de serie, Emisor y Nombre común de asunto.
  - c (opcional) Con un explorador web, abra una conexión HTTPS al nodo en el que se reubicará el certificado, compruebe la información del certificado y asegúrese de que esta coincida con la del certificado SSL de máquina.
- 3 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

**Windows**

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

**vCenter Server Appliance**

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

- 4 Publique el certificado raíz personalizado, que es el certificado de firma de la CA externa.

```
dir-cli trustedcert publish --cert <my_custom_root>
```

Si no especifica un nombre de usuario y una contraseña en la línea de comandos, el sistema se lo solicitará.

- 5 Reinicie todos los servicios.

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

### Pasos siguientes

Se puede quitar el certificado raíz original de VMCA del almacén de certificados si así lo establece la directiva de la empresa. En caso de hacerlo, deberá actualizar estos certificados internos:

- Reemplace el certificado de firma de vCenter Single Sign-On. Consulte [Actualizar el certificado del servicio de token de seguridad](#).
- Reemplace el certificado de VMware Directory Service. Consulte [Reemplazar certificado para VMware Directory Service](#).

## Reemplazar certificados SSL de máquina por certificados personalizados

Después de recibir los certificados personalizados, puede reemplazar los certificados de cada máquina.

Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. En una implementación de varios nodos, debe ejecutar los comandos de generación de certificados SSL de máquina en cada nodo. Use el parámetro `--server` para apuntar a Platform Services Controller desde vCenter Server con Platform Services Controller externo.

Para poder empezar a reemplazar los certificados, debe tener la siguiente información:

- Contraseña de administrator@vsphere.local.
- Un certificado SSL de máquina personalizado y válido (archivo `.crt`).
- Una clave SSL de máquina personalizada y válida (archivo `.key`).
- Un certificado personalizado válido para la raíz (archivo `.crt`).
- Si ejecuta el comando en vCenter Server con Platform Services Controller externo en una implementación de varios nodos, la dirección IP de Platform Services Controller.

### Requisitos previos

Seguramente recibió un certificado para cada máquina de la entidad de certificación de la empresa o externa.

- Tamaño de clave: 2.048 bits o más (formato codificado PEM)

- Formato CRT
- x509 versión 3
- SubjectAltName debe contener DNS Name=<machine\_FQDN>
- Contiene los siguientes usos de claves: firma digital, no repudio, cifrado de clave

### Procedimiento

- 1 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

### Windows

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

### vCenter Server Appliance

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

- 2 Inicie sesión en cada nodo y agregue a VECS los certificados de máquina nuevos obtenidos de la CA.

Todas las máquinas necesitan el certificado nuevo en el almacén de certificados local para comunicarse mediante SSL.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-path>
--key <key-file-path>
```

- 3 Reinicie todos los servicios.

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

### Ejemplo: Reemplazar certificados SSL de máquina por certificados personalizados

Puede reemplazar el certificado SSL de máquina en cada nodo del mismo modo.

- 1 Primero, elimine el certificado existente en VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafd"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
```

## 2 A continuación, agregue el certificado de reemplazo.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-wl-
vim-cat-dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-
cat-dhcp-1128.vmware.com.priv
```

### Pasos siguientes

También puede reemplazar los certificados de sus hosts ESXi. Consulte la publicación *Seguridad de vSphere*.

Después de reemplazar el certificado raíz en una implementación de varios nodos, debe reiniciar los servicios en todas las instancias de vCenter Server con nodos de Platform Services Controller externo.

## Reemplazar los certificados de usuarios de soluciones con certificados personalizados

Después de reemplazar los certificados SSL de máquina, puede reemplazar los certificados de usuarios de solución firmados por VMCA con certificados externos o empresariales.

Los usuarios de soluciones usan los certificados únicamente para autenticarse en vCenter Single Sign-On. Si el certificado es válido, vCenter Single Sign-On asigna un token SAML al usuario de solución. Este usa el token SAML para autenticarse en otros componentes de vCenter.

Considere si en su entorno es necesario reemplazar los certificados de usuarios de soluciones. Dado que los usuarios de soluciones se encuentran detrás de un servidor proxy y que se usa el certificado SSL de máquina para proteger el tráfico de SSL, los certificados de usuarios de soluciones quizás no sean un factor de seguridad tan importante.

Debe reemplazar el certificado de usuario de solución de la máquina en cada nodo de administración y en cada nodo de Platform Services Controller. Debe reemplazar los certificados de usuarios de solución solo en cada nodo de administración. Utilice el parámetro `--server` para apuntar a Platform Services Controller cuando ejecute comandos en un nodo de administración con una instancia externa de Platform Services Controller.

---

**Nota** Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

---

### Requisitos previos

- Tamaño de clave: 2.048 bits o más (formato codificado PEM)
- Formato CRT
- x509 versión 3

- SubjectAltName debe contener DNS Name=<machine\_FQDN>
- Cada certificado de usuario de solución debe tener un `Subject` diferente. Por ejemplo, considere incluir el nombre de usuario de solución (como `vpzd`) u otro identificador único.
- Contiene los siguientes usos de claves: firma digital, no repudio, cifrado de clave

### Procedimiento

- 1 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdir
service-control --start vmca
```

- 2 Busque el nombre de cada usuario de solución.

```
dir-cli service list
```

Puede usar el identificador único que se devuelve al reemplazar los certificados. La entrada y la salida deben verse de la siguiente manera.

```
C:\Program Files\VMware\vCenter Server\vmafd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpzd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpzd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Cuando enumera certificados de usuario de solución en implementaciones de varios nodos, el resultado de la lista de `dir-cli` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

- 3 En cada usuario de solución, reemplace el certificado actual en VECS y, a continuación, en `vmdir`.

Debe agregar los certificados en ese orden.

```
vecs-cli entry delete --store vpzd --alias vpzd
vecs-cli entry create --store vpzd --alias vpzd --cert vpzd.crt --key vpzd.priv
dir-cli service update --name <vpzd-xxxx-xxx-xxxxxx> --cert vpzd.crt
```

---

**Nota** Los usuarios de solución no podrán autenticarse en vCenter Single Sign-On si no se reemplaza el certificado en `vmdir`.

---

#### 4 Reinicie todos los servicios.

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

### Reemplazar certificado para VMware Directory Service

Si decide usar un nuevo certificado raíz de VMCA, y anula la publicación del certificado raíz de VMCA que se utilizó al aprovisionar el entorno, deberá reemplazar los certificados SSL de máquina, los certificados de usuario de solución y los certificados de algunos servicios internos.

Si anula la publicación del certificado raíz de VMCA, deberá reemplazar el certificado con firma de SSL que utiliza vCenter Single Sign-On. Consulte [Actualizar el certificado del servicio de token de seguridad](#). También deberá reemplazar el certificado para VMware Directory Service (vmdir).

#### Requisitos previos

Solicite un certificado para vmdir a la entidad de certificación empresarial o externa.

#### Procedimiento

##### 1 Detenga vmdir.

###### Linux

```
service-control --stop vmdird
```

###### Windows

```
service-control --stop VMWareDirectoryService
```

##### 2 Copie el certificado y la clave que acaba de generar en la ubicación de vmdir.

###### Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem  
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

###### Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem  
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 Reinicie vmdir desde vSphere Web Client o use el comando `service-control`.

#### Linux

```
service-control --start vmdird
```

#### Windows

```
service-control --start VMWareDirectoryService
```

## Reemplazar el certificado de VMware Directory Service en entornos de modo mixto

Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

El vmdir utiliza el certificado SSL de VMware Directory Service para realizar negociaciones entre los nodos de Platform Services Controller que realizan la replicación de vCenter Single Sign-On.

Estos pasos no son necesarios para un entorno de modo mixto que incluya los nodos de vSphere 6.0 y vSphere 6.5. Estos pasos son necesarios solo si:

- El entorno incluye servicios tanto de vCenter Single Sign-On 5.5 como de vCenter Single Sign-On 6.x.
- Los servicios de vCenter Single Sign-On se configuran para replicar datos de vmdir.
- Planea reemplazar los certificados firmados por VMCA predeterminados por certificados personalizados del nodo en el que se ejecuta el servicio de vCenter Single Sign-On 6.x.

---

**Nota** Actualizar el entorno al completo antes de reiniciar los servicios es una práctica recomendada. Generalmente, el reemplazo del certificado de VMware Directory Service no se recomienda.

---

#### Procedimiento

- 1 En el nodo en el que se ejecuta el servicio de vCenter Single Sign-On 6.x, reemplace el certificado SSL de vmdir y la clave.

Consulte [Reemplazar certificado para VMware Directory Service](#).



- 2 En el nodo en el que se ejecuta el servicio de vCenter Single Sign-On 5.5, configure el entorno para que se reconozca el servicio de vCenter Single Sign-On 6.x.
  - a Haga una copia de seguridad de todos los archivos  
`C:\ProgramData\VMware\CIS\cfg\vmldird.`
  - b Haga una copia del archivo `vmldircert.pem` en el nodo 6.x y cámbiele el nombre por `<sso_node2.domain.com>.pem`, donde `<sso_node2.domain.com>` es el FQDN del nodo 6.x.
  - c Copie el certificado con nombre nuevo en `C:\ProgramData\VMware\CIS\cfg\vmldird` para reemplazar el certificado de replicación existente.
- 3 Reinicie VMware Directory Service en todas las máquinas en las que reemplazó certificados.  
 Puede reiniciar el servicio desde vSphere Web Client o utilizar el comando `service-control`.

## Administrar certificados y servicios con comandos de CLI

Un conjunto de CLI permite administrar VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store) y VMware Directory Service (vmdir). La utilidad vSphere Certificate Manager también admite muchas tareas relacionadas, pero las CLI son necesarias para la administración manual de certificados.

**Tabla 3-5. Herramientas de CLI para administrar certificados y servicios asociados**

CLI	Descripción	Consulte
<code>certool</code>	Genere y administre certificados y claves. Parte de VMCA.	<a href="#">Referencia de comandos de inicialización de certool</a>
<code>vecs-cli</code>	Administre el contenido de las instancias de VMware Certificate Store. Parte de VMAFD.	<a href="#">Referencia de comandos vecs-cli</a>
<code>dir-cli</code>	Cree y actualice los certificados en VMware Directory Service. Parte de VMAFD.	<a href="#">Referencia de comando dir-cli</a>
<code>service-control</code>	Iniciar o detener los servicios, por ejemplo, como parte de un flujo de trabajo de reemplazo de certificados	

## Ubicaciones de las herramientas de administración de certificados

De forma predeterminada, las herramientas se encuentran en las siguientes ubicaciones de cada nodo.

### Windows

`C:\Archivos de programa\VMware\vCenter Server\vmafdd\vecs-cli.exe`

`C:\Archivos de programa\VMware\vCenter Server\vmafdd\dir-cli.exe`

`C:\Archivos de programa\VMware\vCenter Server\vmcad\certool.exe`

`RUTA_DE_INSTALACIÓN_DE_VCENTER\bin\service-control`

## Linux

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

`/usr/lib/vmware-vmafd/bin/dir-cli`

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

En Linux, el comando `service-control` no requiere que especifique la ruta de acceso.

Si ejecuta comandos desde un nodo de administración con una instancia de Platform Services Controller externa, puede especificar Platform Services Controller con el parámetro `--server`.

## Privilegios necesarios para operaciones de administración de certificados

Para la mayoría de las operaciones de administración de certificados de vCenter, el usuario debe estar en el grupo Administradores de CA del dominio `vsphere.local`. El usuario `administrator@vsphere.local` se encuentra en el grupo Administradores de CA. Algunas operaciones están permitidas para todos los usuarios.

Si se ejecuta la utilidad vCenter Certificate Manager, se solicita la contraseña de `administrator@vsphere.local`. Si se reemplazan los certificados de forma manual, las diferentes opciones de las distintas CLI requieren privilegios diferentes.

### dir-cli

Es necesario ser miembro del grupo Administradores de CA del dominio `vsphere.local`. Cada vez que se ejecuta un comando `dir-cli`, se solicita un nombre de usuario y una contraseña.

### vecs-cli

Al principio, solo el propietario del almacén tiene acceso al almacén. El propietario del almacén es el usuario administrador en los sistemas Windows y el usuario raíz en los sistemas Linux. El propietario del almacén puede brindar acceso a otros usuarios.

Los almacenes `MACHINE_SSL_CERT` y `TRUSTED_ROOTS` son almacenes especiales. Solo el usuario raíz o el usuario administrador (según el tipo de instalación), tienen acceso total.

### certool

La mayoría de los comandos `certool` requieren que el usuario esté en el grupo Administradores de CA. El usuario `administrator@vsphere.local` se encuentra en el grupo Administradores de CA. Todos los usuarios pueden ejecutar los siguientes comandos:

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`

- waitVMCA
- genkey
- viewcert

Para administrar certificados de los hosts ESXi, se debe tener el privilegio **Certificados**.

**Administrar certificados.** Este privilegio se puede establecer desde vSphere Web Client.

## Cambiar la configuración de certtool

Al ejecutar `certtool --gencert` y otros comandos específicos de inicialización o administración de certificados, la CLI lee todos los valores de un archivo de configuración. Puede editar el archivo existente, anular el archivo de configuración predeterminado (`certtool.cfg`) con la opción `--config=<file name>` o anular los diferentes valores en la línea de comandos.

El archivo de configuración tiene varios campos con los siguientes valores predeterminados:

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

Puede cambiar los valores en la configuración de la siguiente manera:

- Cree una copia de seguridad del archivo de configuración y, a continuación, edite el archivo. Si utiliza el archivo de configuración predeterminado, no es necesario que lo especifique. O bien si cambió, por ejemplo, el nombre del archivo de configuración, utilice la opción de línea de comandos `--config`.
- Anule el valor del archivo de configuración en la línea de comandos. Por ejemplo, para anular la localidad, ejecute este comando:

```
certtool --gencert --privkey=private.key --Locality="Mountain View"
```

Especifique `--Name` para reemplazar el campo Nombre común del nombre de asunto del certificado.

- Para los certificados de usuarios de solución, el nombre es `<sol_user name>@<domain>` por convención, pero puede cambiarlo si se utiliza una convención diferente en el entorno.

- Para los certificados SSL de máquina, se utiliza el FQDN de la máquina porque el cliente SSL revisa el campo Nombre común del nombre de asunto del certificado cuando comprueba el nombre de host de la máquina. Ya que una máquina puede tener más de un alias, los certificados tienen la extensión de campo Nombre alternativo de asunto, en la que se pueden especificar otros nombres (nombres DNS, direcciones IP, etc.). Sin embargo, VMCA permite solo un `DNSName` (en el campo `Hostname`) y ninguna otra opción de alias. Si es el usuario quien especifica la dirección IP, esta también se almacena en `SubAltName`.

El parámetro `--Hostname` se utiliza para especificar el `DNSName` de `SubAltName` del certificado.

## Referencia de comandos de inicialización de certool

Los comandos de inicialización de `certool` permiten generar solicitudes de firma de certificados, ver y generar certificados y claves firmadas por VMCA, importar certificados raíz y realizar otras operaciones de administración de certificados.

En muchos casos, se puede pasar un archivo de configuración a un comando `certool`. Consulte [Cambiar la configuración de certool](#). Consulte [Reemplazar certificados firmados por VMCA existentes por certificados firmados por VMCA nuevos](#) para ver algunos ejemplos de uso.

### certool --initcsr

Genera una solicitud de firma de certificados (CSR). El comando genera un archivo PKCS10 y una clave privada.

Opción	Descripción
<code>--initcsr</code>	Se necesita para generar las CSR.
<code>--privkey &lt;key_file&gt;</code>	Nombre del archivo de clave privada.
<code>--pubkey &lt;key_file&gt;</code>	Nombre del archivo de clave pública.
<code>--csrfile &lt;csr_file&gt;</code>	Nombre del archivo de CSR que se enviará al proveedor de la entidad de certificación.
<code>--config &lt;config_file&gt;</code>	Nombre opcional del archivo de configuración. El valor predeterminado es <code>certool.cfg</code> .

Ejemplo:

```
certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

### certool --selfca

Crea un certificado autofirmado y aprovisiona el servidor de VMCA con una entidad de certificación raíz autofirmada. Esta opción es una de las formas más simples de aprovisionar el servidor de VMCA. Otra opción es aprovisionar el servidor VMCA con un certificado raíz externo de modo que VMCA sea una entidad de certificación intermedia. Consulte [Utilizar VMCA como entidad de certificación intermedia](#).

Este comando genera un certificado con la fecha establecida tres días antes para evitar conflictos entre las zonas horarias.

Opción	Descripción
<code>--selfca</code>	Se necesita para generar un certificado autofirmado.
<code>--predate &lt;number_of_minutes&gt;</code>	Permite establecer el campo No válido hasta del certificado raíz en la cantidad de minutos determinada antes de la hora actual. Esta opción puede resultar útil para dar cuenta de posibles problemas con las zonas horarias. El valor máximo es tres días.
<code>--config &lt;config_file&gt;</code>	Nombre opcional del archivo de configuración. El valor predeterminado es <code>certool.cfg</code> .
<code>--server &lt;server&gt;</code>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280 --selfca --server=
192.0.2.24 --srp-upn=administrator@vsphere.local
```

## certool --rootca

Importa un certificado raíz. Agrega el certificado especificado y la clave privada a VMCA. VMCA usa siempre el certificado raíz más reciente para la firma, pero puede haber otros certificados raíz disponibles. Esto significa que el usuario puede actualizar la infraestructura un paso a la vez y, por último, eliminar los certificados que ya no use.

Opción	Descripción
<code>--rootca</code>	Se necesita para importar una entidad de certificación raíz.
<code>--cert &lt;certfile&gt;</code>	Nombre opcional del archivo de configuración. El valor predeterminado es <code>certool.cfg</code> .
<code>--privkey &lt;key_file&gt;</code>	Nombre del archivo de clave privada. Este archivo debe estar en el formato codificado PEM.
<code>--server &lt;server&gt;</code>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

## certool --getdc

Devuelve el nombre de dominio predeterminado que usa vmdir.

Opción	Descripción
<code>--server &lt;server&gt;</code>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.
<code>--port &lt;port_num&gt;</code>	Número de puerto opcional. El valor predeterminado es el puerto 389.

Ejemplo:

```
certool --getdc
```

## certool --waitVMDIR

Espere a que VMware Directory Service se ejecute o a que se cumpla el tiempo de espera especificado por `--wait`. Use esta opción, junto con otras opciones, para programar determinadas tareas, como obtener el nombre de dominio predeterminado.

Opción	Descripción
<code>--wait</code>	Cantidad opcional de minutos para esperar. El valor predeterminado es 3.
<code>--server &lt;server&gt;</code>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.
<code>--port &lt;port_num&gt;</code>	Número de puerto opcional. El valor predeterminado es el puerto 389.

Ejemplo:

```
certool --waitVMDIR --wait 5
```

## certool --waitVMCA

Espere a que el servicio VMCA se ejecute o a que se cumpla el tiempo de espera especificado. Use esta opción, junto con otras opciones, para programar determinadas tareas, como generar un certificado.

Opción	Descripción
<code>--wait</code>	Cantidad opcional de minutos para esperar. El valor predeterminado es 3.
<code>--server &lt;server&gt;</code>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.
<code>--port &lt;port_num&gt;</code>	Número de puerto opcional. El valor predeterminado es el puerto 389.

Ejemplo:

```
certool --waitVMCA --selfca
```

## certool --publish-roots

Fuerza la actualización de certificados raíz. Este comando requiere privilegios administrativos.

Opción	Descripción
<code>--server &lt;server&gt;</code>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --publish-roots
```

## Referencia de comandos de administración certool

Los comandos de administración `certool` permiten ver, generar y revocar certificados, y ver información sobre ellos.

### certool --genkey

Genera un par de claves privada y pública. Estos archivos se pueden utilizar para generar un certificado firmado por VMCA. Se puede utilizar el certificado para aprovisionar máquinas o usuarios de solución.

Opción	Descripción
<code>--genkey</code>	Se requiere para generar una clave privada y pública.
<code>--privkey &lt;keyfile&gt;</code>	Nombre del archivo de clave privada.
<code>--pubkey &lt;keyfile&gt;</code>	Nombre del archivo de clave pública.
<code>--server &lt;server&gt;</code>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

### certool --gencert

Genera un certificado desde el servidor de VMCA. Este comando utiliza la información de `certool.cfg` o del archivo de configuración especificado.

Opción	Descripción
<code>--gencert</code>	Se requiere para generar un certificado.
<code>--cert &lt;certfile&gt;</code>	Nombre del archivo de certificado. Este archivo debe estar en el formato codificado PEM.
<code>--privkey &lt;keyfile&gt;</code>	Nombre del archivo de clave privada. Este archivo debe estar en el formato codificado PEM.

Opción	Descripción
<code>--config &lt;config_file&gt;</code>	Nombre opcional del archivo de configuración. El valor predeterminado es <code>certool.cfg</code> .
<code>--server &lt;server&gt;</code>	Nombre opcional del servidor de VMCA. El comando usa el nombre <code>localhost</code> como valor predeterminado.

Ejemplo:

```
certool --gencert --privkey=<filename> --cert=<filename>
```

## certool --getrootca

Imprime un certificado actual de la entidad de certificación raíz en formato de lenguaje natural. Si ejecuta este comando desde un nodo de administración, utilice el nombre de máquina del nodo de Platform Services Controller para recuperar la entidad de certificación raíz. Esta salida no se puede utilizar como certificado porque está cambiada a lenguaje natural.

Opción	Descripción
<code>--getrootca</code>	Se requiere para imprimir el certificado raíz.
<code>--server &lt;server&gt;</code>	Nombre opcional del servidor de VMCA. El comando usa el nombre <code>localhost</code> como valor predeterminado.

Ejemplo:

```
certool --getrootca --server=remoteserver
```

## certool --viewcert

Imprime todos los campos de un certificado en formato de lenguaje natural.

Opción	Descripción
<code>--viewcert</code>	Se requiere para ver un certificado.
<code>--cert &lt;certfile&gt;</code>	Nombre opcional del archivo de configuración. El valor predeterminado es <code>certool.cfg</code> .

Ejemplo:

```
certool --viewcert --cert=<filename>
```

## certool --enumcert

Enumera todos los certificados que conoce el servidor de VMCA. La opción `filter` (filtrar) permite enumerar todos los certificados o solo los certificados revocados, activos o caducados.



Opción	Descripción
<code>--enumcert</code>	Se requiere para enumerar todos los certificados.
<code>--filter [all   active]</code>	Filtro requerido. Especifique todos o los que están activos. Las opciones revocadas o caducadas no se admiten en este momento.

Ejemplo:

```
certool --enumcert --filter=active
```

## certool --status

Envía un certificado especificado al servidor de VMCA para comprobar si está revocado.

Certificado de impresión: REVOCADO si el certificado es revocado; de lo contrario, Certificado: ACTIVO.

Opción	Descripción
<code>--status</code>	Se requiere para comprobar el estado de un certificado.
<code>--cert &lt;certfile&gt;</code>	Nombre opcional del archivo de configuración. El valor predeterminado es <code>certool.cfg</code> .
<code>--server &lt;server&gt;</code>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --status --cert=<filename>
```

## certool --genselfcert

Genera un certificado autofirmado a partir de los valores del archivo de configuración. Este comando genera un certificado con la fecha establecida tres días antes para evitar conflictos entre las zonas horarias.

Opción	Descripción
<code>--genselfcert</code>	Se necesita para generar un certificado autofirmado.
<code>--outcert &lt;cert_file&gt;</code>	Nombre del archivo de certificado. Este archivo debe estar en el formato codificado PEM.
<code>--outprivkey &lt;key_file&gt;</code>	Nombre del archivo de clave privada. Este archivo debe estar en el formato codificado PEM.
<code>--config &lt;config_file&gt;</code>	Nombre opcional del archivo de configuración. El valor predeterminado es <code>certool.cfg</code> .

Ejemplo:

```
certool --genselfcert --privkey=<filename> --cert=<filename>
```

## Referencia de comandos vecs-cli

El conjunto de comandos `vecs-cli` permite administrar las instancias de VMware Certificate Store (VECS). Utilice estos comandos junto con `dir-cli` y `certool` para administrar la infraestructura de certificados.

### vecs-cli store create

Crea un almacén de certificados.

Opción	Descripción
<code>--name &lt;name&gt;</code>	Nombre del almacén de certificados.

Ejemplo:

```
vecs-cli store create --name <store>
```

### vecs-cli store delete

Elimina un almacén de certificados. No se pueden eliminar los almacenes de certificados predefinidos por el sistema.

Opción	Descripción
<code>--name &lt;name&gt;</code>	Nombre del almacén de certificados que se va a eliminar.

Ejemplo:

```
vecs-cli store delete --name <store>
```

### vecs-cli store list

Enumera los almacenes de certificados.

VECS incluye los siguientes almacenes.

Tabla 3-6. Almacenes en VECS

Almacén	Descripción
Almacén SSL de máquina (MACHINE_SSL_CERT)	<ul style="list-style-type: none"> <li>■ El servicio de proxy inverso lo utiliza en cada nodo de vSphere.</li> <li>■ VMware Directory Service (vmdir) lo utiliza en implementaciones integradas y en cada nodo de Platform Services Controller.</li> </ul> <p>Todos los servicios de vSphere 6.0 se comunican mediante un proxy inverso que utiliza el certificado SSL de máquina. Por razones de compatibilidad con versiones anteriores, los servicios de la versión 5.x todavía utilizan puertos específicos. Como resultado, algunos servicios como vpxd todavía tienen su propio puerto abierto.</p>
Almacén raíz de confianza (TRUSTED_ROOTS)	Contiene todos los certificados raíz de confianza.
Almacenes de usuarios de solución <ul style="list-style-type: none"> <li>■ virtual</li> <li>■ vpxd</li> <li>■ vpxd-extensions</li> <li>■ vsphere-webclient</li> </ul>	<p>VECS incluye un almacén para cada usuario de solución. El asunto de cada certificado de usuario de solución debe ser único, por ejemplo, el certificado de máquina no puede tener el mismo asunto que el certificado de vpxd.</p> <p>Los certificados de usuarios de solución se utilizan para la autenticación con vCenter Single Sign-On. vCenter Single Sign-On comprueba que el certificado sea válido, pero no comprueba otros atributos del certificado. En una implementación integrada, todos los certificados de usuarios de solución están en el mismo sistema.</p> <p>Los siguientes almacenes de certificados de usuarios de solución se incluyen en VECS en cada nodo de administración y en cada implementación integrada:</p> <ul style="list-style-type: none"> <li>■ <code>machine</code>: lo utilizan el administrador de componentes, el servidor de licencias y el servicio de registro.</li> </ul> <hr/> <p><b>Nota</b> El certificado de usuario de solución de la máquina no tiene relación alguna con el certificado SSL de máquina. El certificado de usuario de solución de la máquina se utiliza para el intercambio de tokens SAML, mientras que el certificado SSL de máquina se utiliza para las conexiones SSL seguras de una máquina.</p> <hr/> <ul style="list-style-type: none"> <li>■ <code>vpxd</code>: almacén de daemon del servicio vCenter (vpxd) de los nodos de administración y las implementaciones integradas. vpxd utiliza el certificado de usuario de solución que está en este almacén para autenticarse en vCenter Single Sign-On.</li> <li>■ <code>vpxd-extensions</code>: almacén de extensiones de vCenter. Incluye el servicio de Auto Deploy, el servicio de inventario u otros servicios que no forman parte de otros usuarios de solución.</li> <li>■ <code>vsphere-webclient</code>: almacén de vSphere Web Client. También incluye algunos servicios adicionales como el servicio de gráficos de rendimiento.</li> </ul> <p>El almacén <code>machine</code> también se incluye en cada nodo de Platform Services Controller.</p>

Tabla 3-6. Almacenes en VECS (continuación)

Almacén	Descripción
Almacén de copias de seguridad de la utilidad vSphere Certificate Manager (BACKUP_STORE)	VMCA (VMware Certificate Manager) lo utiliza para admitir la reversión de certificados. Solo el estado más reciente se almacena como copia de seguridad; no se puede volver más de un paso.
Otros almacenes	<p>Las soluciones pueden agregar otros almacenes. Por ejemplo, la solución Virtual Volumes agrega un almacén SMS. No modifique los certificados de estos almacenes a menos que lo indique la documentación de VMware o un artículo de la base de conocimientos de VMware.</p> <p><b>Nota</b> Las CRL no son compatibles con vSphere 6.0. Sin embargo, si se elimina el almacén TRUSTED_ROOTS_CRLS, se puede dañar la infraestructura de certificados. No elimine ni modifique el almacén TRUSTED_ROOTS_CRLS.</p>

Ejemplo:

```
vecs-cli store list
```

## vecs-cli store permissions

Otorga o revoca permisos en el almacén. Utilice la opción `--grant` o `--revoke`.

El propietario del almacén tiene el control de su almacén, incluida la capacidad para otorgar y revocar permisos. El administrador tiene todos los privilegios en todos los almacenes, incluida la capacidad para otorgar y revocar permisos.

Se puede utilizar `vecs-cli get-permissions --name <store-name>` para recuperar la configuración actual del almacén.

Opción	Descripción
<code>--name &lt;name&gt;</code>	Nombre del almacén de certificados.
<code>--user &lt;username&gt;</code>	Nombre único del usuario al que se otorgan permisos.
<code>--grant [read write]</code>	Permiso que se va a otorgar, ya sea de lectura o de escritura.
<code>--revoke [read write]</code>	Permiso que se va a revocar, ya sea de lectura o de escritura. No es compatible en este momento.

## vecs-cli entry create

Cree una entrada en VECS. Utilice este comando para agregar una clave privada o un certificado a un almacén.

Opción	Descripción
<code>--store &lt;NameOfStore&gt;</code>	Nombre del almacén de certificados.
<code>--alias &lt;Alias&gt;</code>	Alias opcional del certificado. Esta opción se ignora para el almacén raíz de confianza.
<code>--cert &lt;certificate_file_path&gt;</code>	Ruta de acceso completa del archivo de certificado.
<code>--key &lt;key-file-path&gt;</code>	Ruta de acceso completa de la clave que corresponde al certificado. Opcional.

## vecs-cli entry list

Enumera todas las entradas en un almacén especificado.

Opción	Descripción
<code>--store &lt;NameOfStore&gt;</code>	Nombre del almacén de certificados.
<code>--text</code>	Muestra una versión del certificado en lenguaje natural.

## vecs-cli entry getcert

Recupera un certificado de VECS. Es posible enviar el certificado en un archivo de salida o mostrarlo como texto en lenguaje natural.

Opción	Descripción
<code>--store &lt;NameOfStore&gt;</code>	Nombre del almacén de certificados.
<code>--alias &lt;Alias&gt;</code>	Alias del certificado.
<code>--output &lt;output_file_path&gt;</code>	Archivo donde se escribe el certificado.
<code>--text</code>	Muestra una versión del certificado en lenguaje natural.

## vecs-cli entry getkey

Recupera una clave almacenada en VECS. Es posible enviar el certificado en un archivo de salida o mostrarlo como texto en lenguaje natural.

Opción	Descripción
<code>--store &lt;NameOfStore&gt;</code>	Nombre del almacén de certificados.
<code>--alias &lt;Alias&gt;</code>	Alias de la clave.
<code>--output &lt;output_file_path&gt;</code>	Archivo de salida donde se escribe la clave.
<code>--text</code>	Muestra una versión de la clave en lenguaje natural.

## vecs-cli entry delete

Elimina una entrada de un almacén de certificados. Si se elimina una entrada en VECS, esta se quita de forma permanente de VECS. La única excepción es el certificado raíz actual. VECS sondea vmdir en busca de un certificado raíz.

Opción	Descripción
<code>--store &lt;NameOfStore&gt;</code>	Nombre del almacén de certificados.
<code>--alias &lt;Alias&gt;</code>	Alias de la entrada que se desea eliminar.

## vecs-cli force-refresh

Fuerza una actualización de `vecs-cli`. Cuando esto ocurre, `vecs-cli` se actualiza para utilizar la información más reciente de vmdir. De forma predeterminada, VECS sondea vmdir cada 5 minutos en busca de archivos de certificado raíz nuevos. Utilice este comando para realizar una actualización inmediata de VECS desde vmdir.

## Referencia de comando dir-cli

La utilidad `dir-cli` permite crear y actualizar usuarios de solución, crear otras cuentas de usuario y administrar certificados y contraseñas en vmdir. Puede usar esta utilidad junto con `vecs-cli` y `certool` para administrar la infraestructura de certificados.

## dir-cli service create

Crea un usuario de solución. Se usa sobre todo en soluciones externas.

Opción	Descripción
<code>--name &lt;name&gt;</code>	Nombre del usuario de solución que se va a crear
<code>--cert &lt;cert file&gt;</code>	Ruta de acceso al archivo de certificado. Puede ser un certificado firmado por VMCA o un certificado externo.
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli service list

Enumera a los usuarios de solución que conoce `dir-cli`.

Opción	Descripción
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli service delete

Elimina un usuario de solución en `vmdir`. Cuando se elimina el usuario de solución, todos los servicios asociados dejan de estar disponibles en los nodos de administración que usan esta instancia de `vmdir`.

Opción	Descripción
<code>--name</code>	Nombre del usuario de solución que se va a eliminar.
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli service update

Actualiza el certificado de un usuario de solución especificado, es decir, de una recopilación de servicios. Después de ejecutar este comando, VECS aplica el cambio transcurridos 5 minutos; o bien también se puede usar `vecs-cli force-refresh` para forzar la actualización.

Opción	Descripción
<code>--name &lt;name&gt;</code>	Nombre del usuario de solución que se va a actualizar.
<code>--cert &lt;cert_file&gt;</code>	Nombre del certificado que se va a asignar al servicio.
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli user create

Crea un usuario regular en vmdir. Este comando puede usarse para usuarios humanos que se autentican en vCenter Single Sign-On con un nombre de usuario y una contraseña. Use este comando únicamente durante la creación de prototipos.

Opción	Descripción
<code>--account &lt;name&gt;</code>	Nombre del usuario de vCenter Single Sign-On que se va a crear.
<code>--user-password &lt;password&gt;</code>	Contraseña inicial del usuario.
<code>--first-name &lt;name&gt;</code>	Nombre de pila del usuario.
<code>--last-name &lt;name&gt;</code>	Apellido del usuario.
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli user delete

Elimina el usuario especificado en vmdir.

Opción	Descripción
<code>--account &lt;name&gt;</code>	Nombre del usuario de vCenter Single Sign-On que se va a eliminar.
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli group modify

Agrega un usuario o un grupo a un grupo que ya existe.

Opción	Descripción
<code>--name &lt;name&gt;</code>	Nombre del grupo en vmdir.
<code>--add &lt;user_or_group_name&gt;</code>	Nombre del usuario o el grupo que se va a agregar.



Opción	Descripción
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli group list

Enumera un grupo de vmdir específico.

Opción	Descripción
<code>--name &lt;name&gt;</code>	Nombre opcional del grupo en vmdir. Esta opción permite comprobar si un grupo existe.
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli trustedcert publish

Publica un certificado raíz de confianza en vmdir.

Opción	Descripción
<code>--cert &lt;file&gt;</code>	Ruta de acceso al archivo de certificado.
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli trustedcert unpublsh

Anula la publicación de un certificado raíz de confianza que actualmente está en vmdir. Utilice este comando, por ejemplo, si agregó un certificado raíz diferente a vmdir que es ahora el certificado raíz de todos los otros certificados del entorno. La anulación de la publicación de los certificados que ya no se utilizan forma parte del fortalecimiento del entorno.

Opción	Descripción
<code>--cert-file &lt;file&gt;</code>	Ruta de acceso al archivo de certificado cuya publicación se va a anular.
<code>--crl &lt;file&gt;</code>	Ruta de acceso al archivo CRL asociado con este certificado. No se encuentra en uso.
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli trustedcert list

Enumera todos los certificados raíz de confianza y sus correspondientes identificadores. Los identificadores de los certificados son necesarios para recuperar un certificado con `dir-cli trustedcert get`.

Opción	Descripción
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli trustedcert get

Recupera un certificado raíz de confianza desde vmdir y lo escribe en un archivo especificado.

Opción	Descripción
<code>--id &lt;cert_ID&gt;</code>	Identificador del certificado que se va a recuperar. El identificador se muestra en el comando <code>dir-cli trustedcert list</code> .
<code>--outcert &lt;path&gt;</code>	Ruta de acceso donde se escribe el archivo de certificado.
<code>--outcrl &lt;path&gt;</code>	Ruta de acceso donde se escribe el archivo CRL. No se encuentra en uso.
<code>--login &lt;admin_user_id&gt;</code>	De forma predeterminada, es <code>administrator@vsphere.local</code> . Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
<code>--password &lt;admin_password&gt;</code>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli password create

Crea una contraseña aleatoria que cumple con los requisitos de contraseñas. Este comando puede ser utilizado por usuarios de solución externa.

Opción	Descripción
--login <admin_user_id>	De forma predeterminada, es administrator@vsphere.local. Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli password reset

Permite que un administrador restablezca la contraseña de un usuario. Si usted es un usuario sin permisos de administrador y desea restablecer una contraseña, utilice el comando `dir-cli password change`.

Opción	Descripción
--account	Nombre de la cuenta a la que se le asignará una nueva contraseña.
--new	Nueva contraseña del usuario especificado.
--login <admin_user_id>	De forma predeterminada, es administrator@vsphere.local. Este administrador puede agregar otros usuarios al grupo Administradores de CA de vCenter Single Sign-On para otorgarles privilegios de administrador.
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

## dir-cli password change

Le permite a un usuario cambiar su contraseña. Es necesario ser el usuario propietario de la cuenta para poder hacer este cambio. Los administradores pueden utilizar el comando `dir-cli password reset` para restablecer cualquier contraseña.

Opción	Descripción
--account	Nombre de la cuenta.
--current	Contraseña actual del usuario propietario de la cuenta.
--new	Nueva contraseña del usuario propietario de la cuenta.

## Ver certificados de vCenter con vSphere Web Client

Es posible ver los certificados que conoce vCenter Certificate Authority (VMCA) para determinar si los certificados activos están por caducar, comprobar los certificados caducados y ver el estado del certificado raíz. Todas las tareas de administración de certificados se realizan con las CLI de administración de certificados.

Los certificados asociados se ven con la instancia de VMCA que se incluye con la implementación integrada o con Platform Services Controller. La información de certificados se replica en todas las instancias de VMware Directory Service (vmdir).

Cuando se intentan ver certificados en vSphere Web Client, se solicitan un nombre de usuario y una contraseña. Especifique el nombre de usuario y la contraseña de un usuario con privilegios para VMware Certificate Authority, es decir, un usuario que esté en el grupo Administradores de CA de vCenter Single Sign-On.

### Procedimiento

- 1 Inicie sesión en vCenter Server como `administrator@vsphere.local` u otro usuario del grupo Administradores de CA de vCenter Single Sign-On.
- 2 Seleccione **Administración**, haga clic en **Implementación** y, a continuación, en **Configuración del sistema**.
- 3 Haga clic en **Nodos** y seleccione el nodo para el cual desea ver o administrar certificados.
- 4 Haga clic en la pestaña **Administrar** y en **Entidad de certificación**.
- 5 Haga clic en el tipo de certificado para el que desea ver información.

Opción	Descripción
<b>Certificados activos</b>	Muestra los certificados activos, incluida su información de validación. El icono verde Válido hasta cambia cuando el certificado está por caducar.
<b>Certificados revocados</b>	Muestra la lista de certificados revocados. No se admite en esta versión.
<b>Certificados caducados</b>	Enumera los certificados caducados.
<b>Certificados raíz</b>	Muestra los certificados raíz disponibles para esta instancia de vCenter Certificate Authority.

- 6 Seleccione un certificado y haga clic en el botón **Mostrar detalles de certificado** para ver los detalles del certificado.

Los detalles incluyen Nombre de asunto, Emisor, Validez y Algoritmo.

## Establecer el umbral para las advertencias de caducidad de certificados de vCenter

A partir de vSphere 6.0, vCenter Server supervisa todos los certificados de VMware Endpoint Certificate Store (VECS) y emite una alarma cuando un certificado está a 30 días o menos de

caducar. Puede cambiar el tiempo de anticipación con el que desea recibir el alerta con la opción avanzada `vpxd.cert.threshold`.

#### Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Seleccione el objeto de vCenter Server y, a continuación, seleccione la pestaña **Administrar** y la subpestaña **Configuración**.
- 3 Haga clic en **Configuración avanzada**, seleccione **Editar** y filtre el umbral.
- 4 Cambie la configuración de `vpxd.cert.threshold` por el valor deseado y haga clic en **Aceptar**.

# Tareas de administración de permisos y usuarios de vSphere

## 4

vCenter Single Sign-On admite la autenticación, lo cual implica que determina si un usuario puede acceder o no a los componentes de vSphere. Asimismo, cada usuario debe recibir autorización para ver o manipular los objetos de vSphere.

vSphere admite varios mecanismos de autorización diferentes, que se analizan en [Descripción de la autorización en vSphere](#). El eje de la información en esta sección es el modelo de permisos de vCenter Server y cómo realizar tareas de administración de usuarios.

vCenter Server permite un control detallado de la autorización con permisos y funciones. Cuando se asigna un permiso a un objeto en la jerarquía de objetos de vCenter Server, se especifica qué usuario o grupo tiene cuál privilegio sobre ese objeto. Para especificar los privilegios se usan funciones, que son conjuntos de privilegios.

En principio, solo el usuario de `administrator@vsphere.local` está autorizado a iniciar sesión en el sistema vCenter Server. Este usuario puede proceder de las siguientes formas:

- 1 Agregar un origen de identidad en el cual los usuarios y grupos adicionales estén definidos en vCenter Single Sign-On. Consulte [Agregar un origen de identidad de vCenter Single Sign-On](#).
- 2 Otorgar privilegios a un usuario o grupo mediante la selección de un objeto, como una máquina virtual o un sistema vCenter Server, y asignándole una función sobre ese objeto al usuario o grupo.



Funciones, privilegios y permisos

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_8vla7txu/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8vla7txu/uiConfId/49694343/))

Este capítulo incluye los siguientes temas:

- [Descripción de la autorización en vSphere](#)
- [Descripción general del modelo de permisos de vCenter Server](#)
- [Herencia jerárquica de permisos](#)
- [Configuración de varios permisos](#)
- [Administrar permisos para componentes de vCenter](#)
- [Permisos globales](#)
- [Usar funciones para asignar privilegios](#)

- [Prácticas recomendadas para funciones y permisos](#)
- [Privilegios necesarios para la realización de tareas comunes](#)

## Descripción de la autorización en vSphere

El método principal para autorizar a un usuario o grupo en vSphere es con los permisos de vCenter Server. El tipo de autorización depende del tipo de tarea que se desea realizar.

vSphere 6.0 y versiones posteriores permiten a los usuarios con privilegios otorgar a otros usuarios permisos para realizar tareas de la siguiente manera. Estos métodos son, en la gran mayoría, mutuamente exclusivos. Sin embargo, se pueden asignar permisos globales de uso para autorizar a ciertos usuarios en todas las soluciones, y permisos locales de vCenter Server para autorizar a otros usuarios en sistemas vCenter Server individuales.

### Permisos de vCenter Server

El modelo de permisos de los sistemas vCenter Server se basa en la asignación de permisos a los objetos de la jerarquía de objetos de esas instancias de vCenter Server. Cada permiso otorga un conjunto de privilegios a un usuario o grupo; es decir, asigna una función para un objeto seleccionado. Por ejemplo, se puede seleccionar un host ESXi y asignar una función a un grupo de usuarios para otorgarles los privilegios correspondientes sobre ese host.

### Permisos globales

Los permisos globales se aplican a un objeto raíz global que expande soluciones. Por ejemplo, si vCenter Server y vCenter Orchestrator están instalados, se pueden otorgar permisos a todos los objetos de ambas jerarquías de objetos mediante los permisos globales.

Los permisos globales se replican en todo el dominio vsphere.local. Los permisos globales no proporcionan autorización para los servicios administrados mediante grupos de vsphere.local. Consulte [Permisos globales](#).

### Pertenencia a los grupos de vsphere.local

El usuario administrator@vsphere.local puede realizar tareas asociadas con los servicios incluidos con Platform Services Controller. Además, los miembros de un grupo de vsphere.local pueden realizar la tarea correspondiente. Por ejemplo, se puede llevar a cabo la administración de licencias si se es miembro del grupo LicenseService.Administrators. Consulte [Grupos del dominio vsphere.local](#).

### Permisos de hosts locales de ESXi

Si administra un host ESXi independiente que no está administrado por un sistema vCenter Server, puede asignar uno de las funciones predefinidas a los usuarios. Consulte la documentación de *Administración de vSphere con vSphere Client*.

## Descripción general del modelo de permisos de vCenter Server

El modelo de permisos de los sistemas vCenter Server se basa en la asignación de permisos a los objetos de la jerarquía de objetos de vSphere. Cada permiso otorga un conjunto de privilegios a un usuario o grupo; es decir, asigna una función para el objeto seleccionado.

Es necesario comprender los siguientes conceptos:

### Permisos

Cada objeto en la jerarquía de objetos de vCenter Server tiene permisos asociados. Cada permiso especifica en un solo grupo o usuario qué privilegios tiene ese grupo o usuario sobre el objeto.

### Usuarios y grupos

En los sistemas vCenter Server se pueden asignar privilegios solo a usuarios autenticados o a grupos de usuarios autenticados. Los usuarios se autentican mediante vCenter Single Sign-On. Los usuarios y los grupos deben definirse en el origen de identidad que vCenter Single Sign-On utiliza para autenticar. Defina usuarios y grupos utilizando las herramientas en su origen de identidad, por ejemplo, Active Directory.

### Funciones

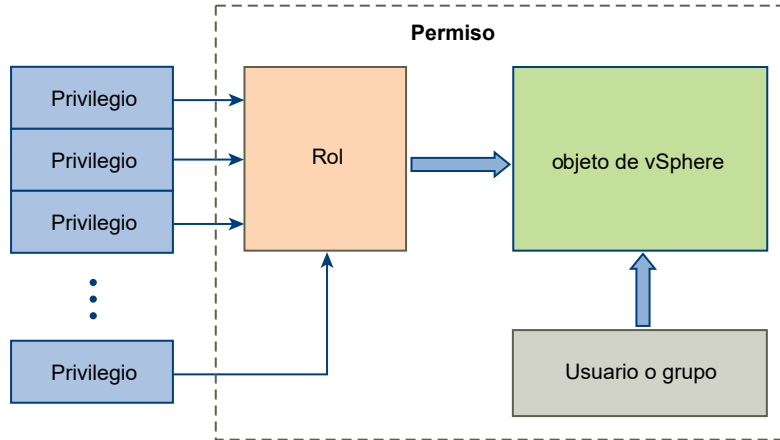
Las funciones permiten asignar permisos en un objeto en función de un conjunto típico de tareas que realizan los usuarios. En vCenter Server, las funciones predeterminados —tales como Administrador— están predefinidos y no se pueden cambiar. Otras funciones, como Administrador de grupo de recursos, son funciones de muestra predefinidos. Se pueden crear funciones personalizadas, ya sea desde cero o mediante la clonación y la modificación de las funciones de muestra.

### Privilegios

Los privilegios son controles de acceso detallados. Esos privilegios se pueden agrupar en funciones que, a continuación, se pueden asignar a los usuarios o a los grupos.



Figura 4-1. Permisos de vSphere



Para asignar permisos sobre un objeto, siga estos pasos:

- 1 Seleccione el objeto en la jerarquía de objetos de vCenter sobre el cual desea aplicar el permiso.
- 2 Seleccione el grupo o el usuario que tendrá los privilegios sobre el objeto.
- 3 Seleccione la función, o el conjunto de privilegios, que el grupo o el usuario cumplirá sobre el objeto. De forma predeterminada, los permisos se propagan; esto significa que el grupo o el usuario cumple la función determinada sobre el objeto seleccionado y sus objetos secundarios.

El modelo de permisos ofrece funciones predefinidas y así, facilita y acelera la ejecución de tareas. También es posible combinar privilegios para crear funciones personalizadas. Consulte [Capítulo 11 Privilegios definidos](#) como referencia para todos los privilegios y los objetos sobre los que puede aplicar privilegios. Consulte [Privilegios necesarios para la realización de tareas comunes](#) para ver algunos ejemplos de los conjuntos de privilegios que necesita para realizar estas tareas.

En muchos casos, los permisos deben definirse tanto en un objeto de origen como en un objeto de destino. Por ejemplo, al mover una máquina virtual, se necesitan algunos privilegios en esa máquina, pero también otros privilegios en el centro de datos de destino.

El modelo de permisos de los hosts ESXi independientes es más simple. Consulte [Asignar permisos para ESXi](#)

## Validar usuarios de vCenter Server

Los sistemas vCenter Server que usan un servicio de directorio suelen validar usuarios y grupos en función del dominio del directorio de usuarios. La validación se produce en intervalos regulares especificados en la configuración de vCenter Server. Por ejemplo, si se asigna una función sobre varios objetos al usuario Smith y, posteriormente, se cambia el nombre del usuario en el dominio a Smith2, el host interpreta que Smith ya no existe y elimina los permisos asociados con ese usuario de los objetos de vSphere en la siguiente validación.

De modo similar, si se elimina el usuario Smith del dominio, todos los permisos asociados con ese usuario se eliminan en la siguiente validación. Si se agrega un nuevo usuario Smith al dominio antes de la siguiente validación, el nuevo usuario Smith reemplaza al antiguo usuario Smith en los permisos sobre cualquier objeto.

## Herencia jerárquica de permisos

Al asignar un permiso a un objeto, se puede elegir si el permiso se propagará en la jerarquía de objetos. La propagación se establece para cada permiso. Es decir, no se aplica universalmente. Los permisos definidos para un objeto secundario siempre anulan los permisos propagados desde los objetos primarios.

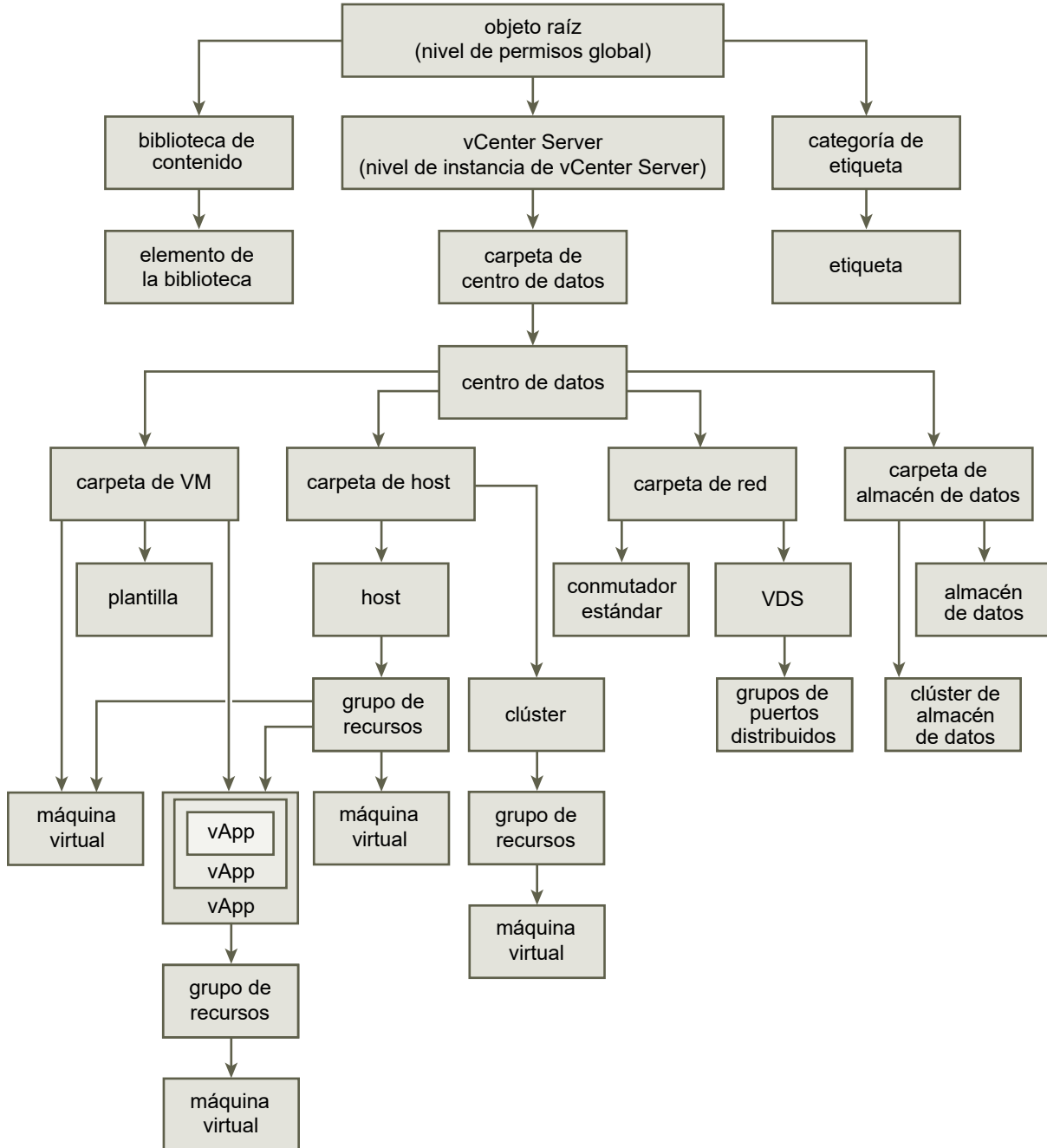
La figura ilustra la jerarquía de inventario y las rutas mediante las cuales pueden propagarse los permisos.

---

**Nota** Los permisos globales son compatibles con la asignación de privilegios en soluciones de un objeto raíz global. Consulte [Permisos globales](#).

---

Figura 4-2. Jerarquía de inventario de vSphere



La mayoría de los objetos del inventario heredan permisos de un único objeto primario de la jerarquía. Por ejemplo, el almacén de datos hereda permisos de la carpeta primaria del almacén o del centro de datos primario. Las máquinas virtuales heredan permisos de la carpeta primaria de máquinas virtuales y del host, clúster o grupo de recursos primario simultáneamente.

Por ejemplo, se pueden establecer permisos para un conmutador distribuido y sus grupos de puertos distribuidos asociados si se configuran permisos para un objeto primario, como una carpeta o un centro de datos. También se debe seleccionar la opción para propagar estos permisos a los objetos secundarios.

Los permisos tienen distintas formas en la jerarquía:

### Entidades administradas

Los usuarios que tienen privilegios pueden definir permisos en las entidades administradas.

- Clústeres
- Centros de datos
- Almacenes de datos
- Clústeres de almacenes de datos
- Carpetas
- Hosts
- Redes (excepto vSphere Distributed Switch)
- Grupos de puertos distribuidos
- Grupos de recursos
- Plantillas
- Máquinas virtuales
- vSphere vApps

### Entidades globales

No se pueden modificar los permisos en entidades que derivan sus permisos del sistema vCenter Server raíz.

- Campos personalizados
- Licencias
- Funciones
- Intervalos de estadísticas
- Sesiones

## Configuración de varios permisos

Los objetos pueden tener varios permisos, pero solo es posible tener un permiso por cada usuario o grupo. Por ejemplo, un permiso podría especificar que el grupo A tiene privilegios de administrador en un objeto. Otro permiso podría especificar que el grupo B puede tener privilegios de administrador de máquina virtual en el mismo objeto.

Si un objeto hereda permisos de dos objetos primarios, los permisos de un objeto se agregan a los permisos del otro objeto. Por ejemplo, si una máquina virtual figura en una carpeta de máquinas virtuales y, a su vez, pertenece a un grupo de recursos, esa máquina virtual hereda la configuración de todos los permisos, tanto de la carpeta de máquinas virtuales como del grupo de recursos.

Los permisos aplicados en un objeto secundario siempre anulan los permisos aplicados en un objeto primario. Consulte [Ejemplo 2: permisos secundarios que anulan permisos primarios](#).

Si se establecen varios permisos grupales en el mismo objeto y un usuario pertenece a dos o más de esos grupos, pueden ocurrir dos situaciones:

- Si no hay ningún permiso establecido para el usuario en ese objeto, se asigna al usuario al conjunto de privilegios asignados a los grupos de dicho objeto.
- Si hay un permiso establecido para el usuario en ese objeto, el permiso del usuario tiene prioridad sobre todos los permisos grupales.

## Ejemplo 1: herencia de varios permisos

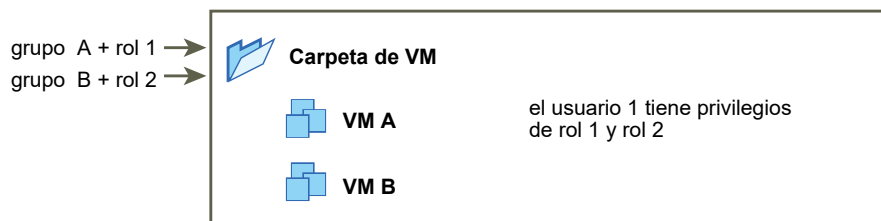
En este ejemplo se muestra cómo un objeto puede heredar varios permisos de los grupos que tienen permisos sobre un objeto primario.

En este ejemplo, se asignan dos permisos sobre el mismo objeto a dos grupos diferentes.

- La Función 1 permite encender las máquinas virtuales.
- La Función 2 puede crear instantáneas de las máquinas virtuales.
- Se asigna la Función 1 al Grupo A en la carpeta de máquina virtual; se otorga el permiso para la propagación a objetos secundarios.
- Se asigna la Función 2 al Grupo B en la carpeta de máquina virtual; se otorga el permiso para la propagación a objetos secundarios.
- No se asignan privilegios específicos al Usuario 1.

El Usuario 1, que pertenece a los grupos A y B, inicia sesión. El Usuario 1 puede encender y crear instantáneas de las máquinas virtuales A y B.

Figura 4-3. Ejemplo 1: herencia de varios permisos



## Ejemplo 2: permisos secundarios que anulan permisos primarios

En este ejemplo, se muestra cómo los permisos que se asignan a un objeto secundario pueden anular los permisos que se asignan a un objeto primario. Este comportamiento de anulación se puede utilizar para restringir el acceso de los usuarios a áreas específicas del inventario.

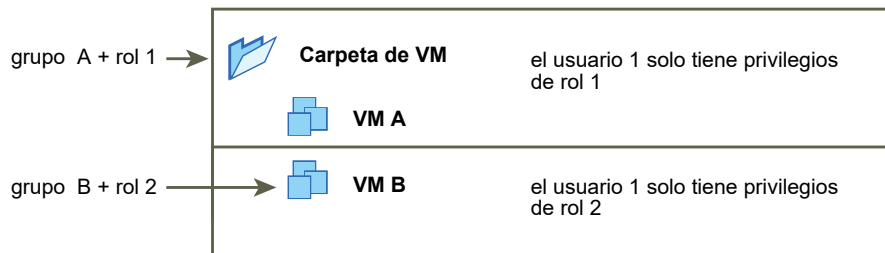
En este ejemplo, los permisos están definidos en dos objetos diferentes de dos grupos distintos.

- La Función 1 permite encender las máquinas virtuales.

- La Función 2 puede crear instantáneas de las máquinas virtuales.
- Se asigna la Función 1 al Grupo A en la carpeta de máquina virtual; se otorga el permiso para la propagación a objetos secundarios.
- Se asigna la Función 2 al Grupo B en la máquina virtual B.

El Usuario 1, que pertenece a los grupos A y B, inicia sesión. Ya que la Función 2 se asigna en un nivel inferior de la jerarquía que la Función 1, la Función 1 se anula en la máquina virtual B. De esta forma, el Usuario 1 puede encender la máquina virtual A, pero no puede crear instantáneas. El Usuario 1 puede crear instantáneas de la máquina virtual B, pero no puede encenderla.

**Figura 4-4. Ejemplo 2: permisos secundarios que anulan permisos primarios**



### Ejemplo 3: función de usuario que anula la función de grupo

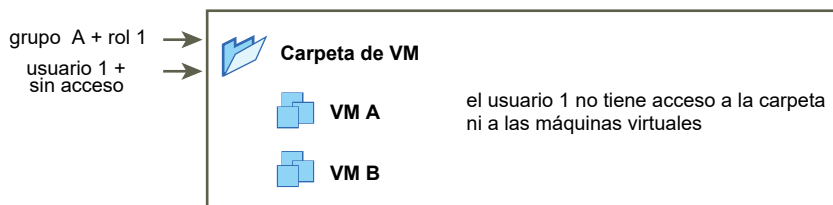
Este ejemplo ilustra cómo la función asignada directamente a un usuario individual anula los privilegios asociados con una función asignada a un grupo.

En este ejemplo, los permisos se definen sobre el mismo objeto. Un permiso asocia un grupo con una función; el otro permiso asocia un usuario individual con una función. El usuario es un miembro del grupo.

- La Función 1 permite encender las máquinas virtuales.
- Se asigna la Función 1 al Grupo A en la carpeta de máquina virtual.
- Se asigna la función Sin acceso al Usuario 1 en la carpeta de máquina virtual.

El Usuario 1, que pertenece al grupo A, inicia sesión. La función Sin acceso otorgada al Usuario 1 en la carpeta de máquina virtual anula la función asignada al grupo. El Usuario 1 no tiene acceso a la carpeta de máquina virtual ni a las máquinas virtuales A y B.

**Figura 4-5. Ejemplo 3: permisos de usuario que anulan permisos de grupo**



# Administrar permisos para componentes de vCenter

Se establece un permiso sobre un objeto en la jerarquía de objetos de vCenter. Cada permiso asocia el objeto con un grupo o un usuario y con las funciones de acceso de ese grupo o usuario. Por ejemplo, se puede seleccionar un objeto de la máquina virtual, agregar un permiso que asigne la función de solo lectura al Grupo 1 y, a continuación, agregar un segundo permiso que asigne la función de administrador al Usuario 2.

Al asignar una función diferente a un grupo de usuarios en diferentes objetos, se controlan las tareas que esos usuarios pueden realizar en el entorno de vSphere. Por ejemplo, para permitir que un grupo configure memoria del host, seleccione el host y agregue un permiso que otorgue una función a ese grupo, donde se incluya el privilegio **Host. Configuración.Configuración de memoria**.

Para administrar permisos desde vSphere Web Client, debe entender los siguientes conceptos:

## Permisos

Cada objeto en la jerarquía de objetos de vCenter Server tiene permisos asociados. Cada permiso especifica en un solo grupo o usuario qué privilegios tiene ese grupo o usuario sobre el objeto.

## Usuarios y grupos

En los sistemas vCenter Server se pueden asignar privilegios solo a usuarios autenticados o a grupos de usuarios autenticados. Los usuarios se autentican mediante vCenter Single Sign-On. Los usuarios y los grupos deben definirse en el origen de identidad que vCenter Single Sign-On utiliza para autenticar. Defina usuarios y grupos utilizando las herramientas en su origen de identidad, por ejemplo, Active Directory.

## Funciones

Las funciones permiten asignar permisos en un objeto en función de un conjunto típico de tareas que realizan los usuarios. En vCenter Server, las funciones predeterminados —tales como Administrador— están predefinidos y no se pueden cambiar. Otras funciones, como Administrador de grupo de recursos, son funciones de muestra predefinidos. Se pueden crear funciones personalizadas, ya sea desde cero o mediante la clonación y la modificación de las funciones de muestra.

## Privilegios

Los privilegios son controles de acceso detallados. Esos privilegios se pueden agrupar en funciones que, a continuación, se pueden asignar a los usuarios o a los grupos.

Puede asignar permisos sobre objetos de diferentes niveles de la jerarquía; por ejemplo, puede asignar permisos a un objeto del host o una carpeta que incluyan todos los objetos del host. Consulte [Herencia jerárquica de permisos](#). Asimismo, puede asignar permisos a un objeto raíz global donde se apliquen los permisos en todos los objetos de todas las soluciones. Consulte [Permisos globales](#).

## Agregar un permiso a un objeto de inventario

Después de crear usuarios y grupos, y definir sus funciones, debe asignarlos a los objetos de inventario correspondientes. Para asignar los mismos permisos a varios objetos al mismo tiempo, mueva los objetos a una carpeta y configure los permisos allí mismo.

Al asignar permisos desde vSphere Web Client, los nombres de usuarios y grupos deben coincidir exactamente con los de Active Directory, con distinción de mayúsculas y minúsculas. Si realizó una actualización de versiones anteriores de vSphere y tiene problemas con los grupos, compruebe que no haya inconsistencias de mayúsculas y minúsculas.

### Requisitos previos

En el objeto cuyos permisos desea modificar, debe tener una función que incluya el privilegio **Permisos.Modificar permiso**.

### Procedimiento

- 1 Desplácese hasta el objeto para el que desea asignar permisos en el navegador de objetos de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y seleccione **Permisos**.
- 3 Haga clic en el icono Agregar y, a continuación, en **Agregar**.
- 4 Identifique al usuario o al grupo que tendrá los privilegios definidos por la función seleccionada.
  - a En el menú desplegable **Dominio**, seleccione el dominio en el que se encuentra el usuario o el grupo.
  - b Escriba un nombre en el cuadro Búsqueda o seleccione un nombre de la lista.  
El sistema busca nombres de usuario, nombres de grupo y descripciones.
  - c Seleccione el usuario o el grupo, y haga clic en **Agregar**.  
El nombre se agrega ya sea a la lista **Usuarios** o a la lista **Grupos**.
  - d (opcional) Haga clic en **Comprobar nombres** para comprobar que el usuario o el grupo existen en el origen de identidad.
  - e Haga clic en **Aceptar**.
- 5 Seleccione una función en el menú desplegable **Función asignada**.  
En el menú aparecen las funciones que se asignarán al objeto. Los privilegios contenidos en la función se enumeran en la sección debajo del título de la función.
- 6 (opcional) Para limitar la propagación, desactive la casilla **Propagar a los objetos secundarios**.  
La función se aplica únicamente al objeto seleccionado y no se propaga a los objetos secundarios.
- 7 Haga clic en **Aceptar** para agregar el permiso.



## Cambiar permisos

Después de que se establece un par usuario/grupo-función para un objeto de inventario, se puede cambiar la función emparejada con el usuario o grupo, o cambiar la configuración de la casilla **Propagar**. También se puede quitar la configuración de permisos.

### Procedimiento

- 1 Desplácese hasta el objeto en el navegador de objetos de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y seleccione **Permisos**.
- 3 Para seleccionar el par usuario/grupo-función, haga clic en el elemento de línea.
- 4 Haga clic en **Cambiar función en el permiso**.
- 5 En el menú desplegable **Función asignada**, seleccione una función para el usuario o grupo.
- 6 Para propagar los privilegios a los objetos secundarios del objeto de inventario asignado, active la casilla **Propagar** y haga clic en **Aceptar**.

## Quitar permisos

Puede quitar permisos de un objeto de la jerarquía de objetos correspondientes a usuarios individuales o grupos. Al hacerlo, el usuario deja de tener privilegios asociados con la función que está en el objeto.

### Procedimiento

- 1 Desplácese hasta el objeto en el navegador de objetos de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y seleccione **Permisos**.
- 3 Haga clic en el elemento de línea adecuado para seleccionar el par usuario/grupo-función.
- 4 Haga clic en **Quitar permiso**.

### Resultados

vCenter Server quita la configuración del permiso.

## Cambiar la configuración de validación de permisos

vCenter Server valida de forma periódica la lista de usuarios y grupos con los usuarios y grupos del directorio de usuarios. A continuación, quita los usuarios y los grupos que ya no existen en el dominio. Se puede deshabilitar la validación o cambiar el intervalo entre las validaciones. Si tiene dominios con miles de usuarios o grupos, o bien si las búsquedas tardan mucho en completarse, considere ajustar la configuración de la búsqueda.

Para las versiones de vCenter Server anteriores a vCenter Server 5.0, esta configuración se aplica en un Active Directory asociado con vCenter Server. Para las versiones vCenter Server 5.0 y posteriores, esta configuración se aplica a los orígenes de identidad de vCenter Single Sign-On.

**Nota** Este procedimiento se aplica únicamente a las listas de usuarios de vCenter Server. No se pueden realizar búsquedas en las listas de usuarios de ESXi de la misma manera.

#### Procedimiento

- 1 Desplácese hasta el sistema vCenter Server en el navegador de objetos de vSphere Web Client.
- 2 Seleccione la pestaña **Administrar** y haga clic en **Configuración**.
- 3 Haga clic en **General** y en **Editar**.
- 4 Seleccione **Directorio de usuarios**.
- 5 Cambie los valores según sea necesario.

Opción	Descripción
Tiempo de espera del directorio de usuarios	Intervalo de tiempo de espera en segundos para la conexión al servidor de Active Directory. Este valor especifica la cantidad máxima de tiempo que vCenter Server permite para la ejecución de una búsqueda en el dominio seleccionado. La búsqueda en dominios grandes puede tardar mucho.
Límite de consulta	Active la casilla para establecer la cantidad máxima de usuarios y grupos que vCenter Server puede mostrar.
Tamaño del límite de consulta	Especifica la cantidad máxima de usuarios y grupos que vCenter Server muestra en el dominio seleccionado en el cuadro de diálogo <b>Seleccionar usuarios o grupos</b> . Si escribe 0 (cero), aparecen todos los usuarios y grupos.
Validación	Anule la selección de la casilla para deshabilitar la validación.
Período de validación	Especifica la frecuencia con que vCenter Server valida permisos (en minutos).

- 6 Haga clic en **Aceptar**.

## Permisos globales

Los permisos globales se aplican a un objeto raíz global que expande soluciones, por ejemplo, vCenter Server y vCenter Orchestrator. Utilice los permisos globales para otorgar a un usuario o grupo privilegios sobre todos los objetos de todas las jerarquías de objetos.

Cada solución tiene un objeto raíz en su propia jerarquía de objetos. El objeto raíz global actúa como objeto primario para cada objeto de la solución. Puede asignar permisos globales a usuarios o grupos, y decidir qué función asignar a cada usuario o grupo. La función determina el conjunto de privilegios. Puede asignar una función predefinida o crear funciones personalizadas. Consulte [Usar funciones para asignar privilegios](#). Es importante distinguir entre los permisos de vCenter Server y los permisos globales.

#### Permisos de vCenter Server

En la mayoría de los casos, se aplica un permiso a un objeto de inventario de vCenter Server, como un host ESXi o una máquina virtual. Cuando se realiza esta acción, se especifica que el usuario o grupo tenga un conjunto de privilegios, también llamada función, sobre el objeto.

### Permisos globales

Los permisos globales otorgan al usuario o grupo privilegios para ver o administrar todos los objetos en cada una de las jerarquías de inventario de la implementación.

Si asigna un permiso global y no selecciona Propagar, los usuarios o grupos asociados con este permiso no tendrán acceso a los objetos de la jerarquía. Solo podrán acceder a algunas funcionalidades globales, como la creación de funciones.

---

**Importante** Utilice los permisos globales con atención. Compruebe si realmente desea asignar permisos para todos los objetos en todas las jerarquías del inventario.

---

## Agregar permisos globales

Se pueden utilizar permisos globales para otorgar a un usuario o un grupo privilegios sobre todos los objetos de todas las jerarquías del inventario de la implementación.

Utilice los permisos globales con atención. Compruebe si realmente desea asignar permisos para todos los objetos en todas las jerarquías del inventario.

### Requisitos previos

Para realizar esta tarea, se deben tener los privilegios **.Permisos.Modificar permisos** en el objeto raíz de todas las jerarquías del inventario.

### Procedimiento

- 1 Haga clic en **Administración** y seleccione **Permisos globales** en el área de control de acceso.
- 2 Haga clic en **Administrar** y en el icono Agregar permisos.
- 3 Identifique al usuario o al grupo que tendrá los privilegios definidos por la función seleccionada.
  - a En el menú desplegable **Dominio**, seleccione el dominio en el que se encuentra el usuario o el grupo.
  - b Escriba un nombre en el cuadro Búsqueda o seleccione un nombre de la lista.  
El sistema busca nombres de usuario, nombres de grupo y descripciones.
  - c Seleccione el usuario o el grupo, y haga clic en **Agregar**.  
El nombre se agrega ya sea a la lista **Usuarios** o a la lista **Grupos**.
  - d (opcional) Haga clic en **Comprobar nombres** para comprobar que el usuario o el grupo existen en el origen de identidad.
  - e Haga clic en **Aceptar**.

#### 4 Seleccione una función en el menú desplegable **Función asignada**.

En el menú aparecen las funciones que se asignarán al objeto. Los privilegios contenidos en la función se enumeran en la sección debajo del título de la función.

#### 5 Deje activada la casilla Propagar a objetos secundarios en la mayoría de los casos.

Si asigna un permiso global y no selecciona Propagar, los usuarios o grupos asociados con este permiso no tendrán acceso a los objetos de la jerarquía. Solo podrán acceder a algunas funcionalidades globales, como la creación de funciones.

#### 6 Haga clic en **Aceptar**.

## Permisos en objetos de etiqueta

En la jerarquía de objetos de vCenter Server, los objetos de etiqueta no son objetos secundarios de vCenter Server, sino que se crean al nivel de raíz de vCenter Server. En los entornos que tienen varias instancias de vCenter Server, los objetos de etiqueta se comparten en las instancias de vCenter Server. El funcionamiento de los permisos para los objetos de etiqueta es distinto al de los permisos para otros objetos de la jerarquía de objetos de vCenter Server.

### Solo se aplican los permisos globales o los permisos asignados al objeto de etiqueta

Si otorga permisos a un usuario en un objeto de inventario de vCenter Server, como un host ESXi o una máquina virtual, ese usuario no puede realizar operaciones de etiquetado en ese objeto.

Por ejemplo, si otorga el privilegio **Asignar etiqueta de vSphere** al usuario Dana en el host TPA, ese permiso no afecta la posibilidad de Dana de asignar etiquetas en el host TPA. Dana debe tener el privilegio **Asignar etiqueta de vSphere** en el nivel de raíz, es decir, un permiso global, o debe tener el privilegio para el objeto de etiqueta.

**Tabla 4-1. Cómo influyen los permisos globales y los permisos de objeto de etiqueta en lo que pueden hacer los usuarios**

Permiso global	Permiso de nivel de etiqueta	Permiso de nivel de objeto de vCenter Server	Permiso efectivo
No hay privilegios de etiquetado asignados.	Dana tiene los privilegios <b>Asignar o desasignar etiqueta de vSphere</b> para la etiqueta.	Dana tiene los privilegios <b>Eliminar etiqueta de vSphere</b> en el host ESXi TPA.	Dana tiene los privilegios <b>Asignar o desasignar etiqueta de vSphere</b> para la etiqueta.
Dana tiene los privilegios <b>Asignar o desasignar etiqueta de vSphere</b> .	No hay privilegios asignados para la etiqueta.	Dana tiene los privilegios <b>Eliminar etiqueta de vSphere</b> en el host ESXi TPA.	Dana tiene los privilegios globales <b>Asignar o desasignar etiqueta de vSphere</b> . Eso incluye privilegios en el nivel de etiqueta.
No hay privilegios de etiquetado asignados.	No hay privilegios asignados para la etiqueta.	Dana tiene los privilegios <b>Asignar o desasignar etiqueta de vSphere</b> en el host ESXi TPA.	Dana no tiene privilegios de etiquetado en ningún objeto, incluido el host TPA.

## Los permisos globales complementan los permisos de objeto de etiqueta

Los permisos globales, es decir, los permisos que están asignados en el objeto de raíz, complementan los permisos en los objetos de etiqueta cuando los permisos de los objetos de etiqueta tienen más restricciones. Los permisos de vCenter Server no influyen en los objetos de etiqueta.

Por ejemplo, suponga que asigna el privilegio **Eliminar etiqueta de vSphere** al usuario Robin en el nivel de raíz, es decir, mediante el uso de permisos globales. Para la producción de la etiqueta, no asigna el privilegio **Eliminar etiqueta de vSphere** a Robin. En ese caso, Robin tiene el privilegio, incluso para la producción de etiqueta porque tiene el permiso global. No se pueden restringir los privilegios a menos que se modifique el permiso global.

**Tabla 4-2. Los permisos globales complementan los permisos de nivel de etiqueta**

Permiso global	Permiso de nivel de etiqueta	Permiso efectivo
Robin tiene los privilegios <b>Eliminar etiqueta de vSphere</b> .	Robin no tiene los privilegios <b>Eliminar etiqueta de vSphere</b> para la etiqueta.	Robin tiene los privilegios <b>Eliminar etiqueta de vSphere</b> .
No hay privilegios de etiquetado asignados.	Robin no tiene los privilegios <b>Eliminar etiqueta de vSphere</b> asignados para la etiqueta.	Robin no tiene los privilegios <b>Eliminar etiqueta de vSphere</b> .

## Los permisos de nivel de etiqueta pueden extender los permisos globales

Se pueden utilizar permisos de nivel de etiqueta para extender los permisos globales. Eso significa que los usuarios pueden tener un permiso global y un permiso de nivel de etiqueta en una etiqueta.

**Tabla 4-3. Los permisos globales extienden los permisos de nivel de etiqueta**

Permiso global	Permiso de nivel de etiqueta	Permiso efectivo
Lee tiene el privilegio <b>Asignar o desasignar etiqueta de vSphere</b> .	Lee tiene el privilegio <b>Eliminar etiqueta de vSphere</b> .	Lee tiene los privilegios <b>Asignar etiqueta de vSphere</b> y <b>Eliminar etiqueta de vSphere</b> para la etiqueta.
No hay privilegios de etiquetado asignados.	Lee tiene el privilegio <b>Eliminar etiqueta de vSphere</b> asignado para la etiqueta.	Lee tiene el privilegio <b>Eliminar etiqueta de vSphere</b> para la etiqueta.

## Usar funciones para asignar privilegios

Una función es un conjunto predefinido de privilegios. Los privilegios definen derechos para realizar acciones y propiedades de lectura. Por ejemplo, la función de administrador de máquinas virtuales consiste en propiedades de lectura y un conjunto de derechos para realizar acciones. La función permite que un usuario lea y cambie los atributos de una máquina virtual.

Al asignar permisos, se establece un par entre un usuario o grupo y una función, y se asocia ese par a un objeto del inventario. Un mismo usuario o grupo puede tener diferentes funciones para distintos objetos del inventario.

Por ejemplo, si hay dos grupos de recursos en el inventario, el Grupo A y el Grupo B, se puede asignar a un usuario específico la función de usuario de la máquina virtual para el Grupo A y la función de solo lectura para el Grupo B. Estas asignaciones permiten que el usuario encienda las máquinas virtuales del Grupo A, y que solo vea las del Grupo B.

vCenter Server proporciona funciones del sistema y funciones de muestra de forma predeterminada:

### Funciones del sistema

Las funciones del sistema son permanentes. No se pueden editar los privilegios asociados con estas funciones.

### Funciones de muestra

VMware proporciona funciones de muestra para ciertas combinaciones de tareas frecuentes. Se pueden clonar, modificar o quitar estas funciones.

---

**Nota** Para evitar perder la configuración predefinida en una función de muestra, primero clone la función y, a continuación, realice las modificaciones en el clon. No se puede restablecer la muestra a su configuración predeterminada.

---

Los usuarios pueden programar tareas únicamente si tienen una función que incluya privilegios para realizar esa tarea en el momento de crearla.

---

**Nota** Los cambios en las funciones y en los privilegios se aplican de inmediato, incluso si los usuarios involucrados iniciaron sesión. La excepción son las búsquedas, para las cuales los cambios se aplican una vez que el usuario cierra la sesión y vuelve a iniciarla.

---

## Funciones personalizadas en vCenter Server y ESXi

Puede crear funciones personalizadas para vCenter Server y todos los objetos que administra, o bien para hosts individuales.

### Funciones personalizadas de vCenter Server (recomendado)

Si se desean crear funciones personalizadas, se pueden utilizar las opciones de edición de funciones en vSphere Web Client para crear conjuntos de privilegios que se adapten a los requisitos.

### Funciones personalizadas de ESXi

Puede crear funciones personalizadas para hosts individuales mediante la utilización de una CLI o de vSphere Client. Consulte la documentación de *Administración de vSphere con vSphere Client*. No se puede acceder a las funciones de host personalizadas desde vCenter Server.

Si administra los hosts ESXi a través de vCenter Server, mantener funciones personalizadas tanto en el host como en vCenter Server puede provocar confusión y una utilización incorrecta. En la mayoría de los casos, se recomienda definir las funciones en vCenter Server.

Cuando se administra un host por medio de vCenter Server, los permisos asociados con ese host se crean desde vCenter Server y se almacenan en vCenter Server. Si se conecta directamente a un host, solo están disponibles las funciones que se crearon de forma directa en el host.

---

**Nota** Cuando se agrega una función personalizada y no se le asignan privilegios, la función creada es de solo lectura con tres privilegios definidos por el sistema: **System.Anonymous**, **System.View** y **System.Read**.

---



Creación de funciones en vSphere Web Client

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_egsyxkp4/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_egsyxkp4/uiConfId/49694343/))

## Funciones del sistema vCenter Server

Una función es un conjunto predefinido de privilegios. Al agregar permisos a un objeto, se empareja un usuario o un grupo con una función. vCenter Server incluye varias funciones de sistema que no se pueden cambiar.

### Funciones del sistema vCenter Server

vCenter Server proporciona una pequeña cantidad de funciones predeterminadas. Los privilegios asociados con las funciones predeterminadas no se pueden cambiar. Las funciones predeterminadas se organizan en una jerarquía. Cada función hereda los privilegios de la función anterior. Por ejemplo, la función de administrador hereda los privilegios de la función de solo lectura. Las funciones que se crean no heredan los privilegios de otras funciones del sistema.

#### Función de administrador

Los usuarios a los que se asigna la función de administrador para un objeto tienen permiso para ver el objeto y realizar todas las acciones posibles en él. Esta función también incluye todos los privilegios inherentes a la función de solo lectura. Si actúa con función de administrador en un objeto, puede asignar privilegios a usuarios y grupos individuales. Si actúa con función de administrador en vCenter Server, puede asignar privilegios a los usuarios y grupos del origen de identidad predeterminado de vCenter Single Sign-On. Los servicios de identidad admitidos incluyen Windows Active Directory y OpenLDAP 2.4.

De forma predeterminada, el usuario `administrator@vsphere.local` tiene la función de administrador tanto en vCenter Single Sign-On como en vCenter Server después de la instalación. Ese usuario puede asociar otros usuarios con la función de administrador en vCenter Server.

#### Función Sin acceso

Los usuarios a los que se asigna la función Sin acceso a un objeto no pueden ver ni cambiar ese objeto de ninguna manera. Los usuarios y grupos nuevos tienen asignada esta función de forma predeterminada. Es posible cambiar la función de un solo objeto a la vez.

El usuario `administrator@vsphere.local`, el usuario raíz y `vpxuser` son los únicos usuarios que no tienen asignada la función Sin acceso de forma predeterminada. En su lugar, tienen

asignada la función de administrador. Es posible quitar al usuario raíz cualquier permiso o cambiar su función a Sin acceso siempre y cuando se cree primero un permiso de reemplazo en el nivel de raíz con la función de administrador, y se asocie este permiso a otro usuario.

### Función de solo lectura

Los usuarios que tienen asignado la función de solo lectura para un objeto tienen permiso para ver el estado y los detalles de este. Con esta función, un usuario puede ver la máquina virtual, el host y los atributos de un grupo de recursos. El usuario no puede ver la consola remota de un host. Las acciones desde los menús y las barras de herramientas no están permitidas.

## Crear una función personalizada

Puede crear funciones personalizadas de vCenter Server que se adapten a las necesidades de control de acceso del entorno.

Si crea o edita una función en un sistema vCenter Server que forma parte del mismo dominio de vCenter Single Sign-On que los otros sistemas vCenter Server, VMware Directory Service (vmdir) propaga los cambios que se hacen en todos los demás sistemas vCenter Server del grupo. Las asignaciones de funciones a usuarios y objetos específicos no se comparten en los sistemas vCenter Server.

### Requisitos previos

Compruebe haber iniciado sesión como un usuario con privilegios de administrador.

### Procedimiento

- 1 Inicie sesión en vCenter Server con vSphere Web Client.
- 2 Seleccione Inicio, haga clic en **Administración** y, a continuación, en **Funciones**.
- 3 Haga clic en el botón (+) **Crear acción de función**.
- 4 Escriba un nombre para la nueva función.
- 5 Seleccione los privilegios de la función y haga clic en **Aceptar**.

## Clonar una función

Se puede realizar una copia de una función ya creada, cambiarle el nombre y editarla. Al realizar una copia, la función nueva no se aplica a ningún usuario, grupo u objeto. Debe asignar la función a usuarios o grupos y objetos.

Si crea o edita una función en un sistema vCenter Server que forma parte del mismo dominio de vCenter Single Sign-On que los otros sistemas vCenter Server, VMware Directory Service (vmdir) propaga los cambios que se hacen en todos los demás sistemas vCenter Server del grupo. Las asignaciones de funciones a usuarios y objetos específicos no se comparten en los sistemas vCenter Server.

### Requisitos previos

Compruebe haber iniciado sesión como un usuario con privilegios de administrador.



**Procedimiento**

- 1 Inicie sesión en vCenter Server con vSphere Web Client.
- 2 Seleccione Inicio, haga clic en **Administración** y, a continuación, en **Funciones**.
- 3 Seleccione una función y haga clic en el icono **Clonar acción de función**.
- 4 Escriba un nombre para la función clonada.
- 5 Seleccione o anule la selección de privilegios para la función y haga clic en **Aceptar**.

**Editar una función**

Cuando se edita una función, se pueden cambiar los privilegios seleccionados para esa función. Una vez completado este paso, los privilegios se aplican a todos los usuarios o grupos a los que se haya asignado la función editada.

Si crea o edita una función en un sistema vCenter Server que forma parte del mismo dominio de vCenter Single Sign-On que los otros sistemas vCenter Server, VMware Directory Service (vmdir) propaga los cambios que se hacen en todos los demás sistemas vCenter Server del grupo. Las asignaciones de funciones a usuarios y objetos específicos no se comparten en los sistemas vCenter Server.

**Requisitos previos**

Compruebe haber iniciado sesión como un usuario con privilegios de administrador.

**Procedimiento**

- 1 Inicie sesión en vCenter Server con vSphere Web Client.
- 2 Seleccione Inicio, haga clic en **Administración** y, a continuación, en **Funciones**.
- 3 Seleccione una función y haga clic en el botón **Editar acción de función**.
- 4 Seleccione o anule la selección de privilegios para la función y haga clic en **Aceptar**.

**Prácticas recomendadas para funciones y permisos**

Utilice las prácticas recomendadas para funciones y permisos con el fin de maximizar la seguridad y la capacidad de administración del entorno de vCenter Server.

VMware recomienda las siguientes prácticas recomendadas para configurar funciones y permisos en un entorno de vCenter Server:

- Cuando sea posible, en lugar de que los usuarios individuales otorguen privilegios a un grupo, asigne una función a este último.
- Otorgue permisos solo en los objetos en los que esto sea necesario y asigne privilegios solo a los usuarios o grupos que deban tenerlos. El uso de una cantidad mínima de permisos facilita la comprensión y la administración de la estructura de permisos.

- Si asigna una función restrictiva a un grupo, compruebe que el grupo no contenga el usuario administrador u otros usuarios con privilegios administrativos. De lo contrario, es posible que restrinja privilegios de administradores de forma accidental en partes de la jerarquía de inventario en las que asignó la función restrictiva al grupo.
- Use carpetas para agrupar objetos. Por ejemplo, si desea otorgar un permiso de modificación para un grupo de hosts y ver dicho permiso en otro conjunto de hosts, coloque cada conjunto de hosts en una carpeta.
- Tenga cuidado al agregar un permiso a los objetos raíz de vCenter Server. Los usuarios con privilegios en nivel de raíz tienen acceso a los datos globales en vCenter Server, como funciones, atributos personalizados y configuración de vCenter Server.
- En la mayoría de los casos, habilite la propagación al asignar permisos para un objeto. Esto garantiza que los objetos nuevos que se inserten en la jerarquía de inventario hereden los permisos y sean accesibles para los usuarios.
- Utilice la función Sin acceso para enmascarar áreas específicas de la jerarquía si no desea que determinados usuarios o grupos tengan acceso a los objetos de esa parte de la jerarquía de objetos.
- Los cambios en las licencias se propagan a todos los sistemas de vCenter Server vinculados a la misma instancia de Platform Services Controller o a Platform Services Controller del mismo dominio de vCenter Single Sign-On, incluso si el usuario no tiene privilegios en todos los sistemas vCenter Server.

## Privilegios necesarios para la realización de tareas comunes

Muchas tareas necesitan permisos sobre más de un objeto del inventario. Puede revisar los privilegios necesarios para realizar las tareas y, cuando corresponda, las funciones de muestra adecuadas.

En la siguiente tabla se enumeran las tareas comunes que necesitan más de un privilegio. Puede agregar permisos a los objetos del inventario; para ello, asigne uno de las funciones predefinidas al usuario. También puede crear funciones personalizadas con el conjunto de privilegios que espera usar varias veces.

Si la tarea que desea realizar no figura en la tabla, las siguientes reglas pueden ayudarlo a determinar dónde debe asignar permisos para permitir determinadas operaciones:

- Cualquier operación que consuma espacio de almacenamiento, como la creación de un disco virtual o la captura de una snapshot, necesita el privilegio **Almacén de datos.Asignar espacio** en el almacén de datos de destino, así como el privilegio para realizar la operación en sí.
- Mover un objeto en la jerarquía del inventario requiere los privilegios apropiados en el objeto mismo, el objeto primario de origen (como una carpeta o un clúster) y el objeto primario de destino.

- Cada host o clúster tiene su propio grupo de recursos implícito, que contiene todos los recursos de ese host o clúster. Para implementar una máquina virtual directamente en un host o un clúster, se necesita el privilegio **Recurso.Asignar máquina virtual a un grupo de recursos**.

Tabla 4-4. Privilegios necesarios para la realización de tareas comunes

Tarea	Privilegios necesarios	Función aplicable
Crear una máquina virtual	En la carpeta de destino o el centro de datos: <ul style="list-style-type: none"> <li>■ <b>Virtual machine.Inventory.Create new</b></li> <li>■ <b>Virtual machine.Configuration.Add new disk</b> (si se está creando un nuevo disco virtual)</li> <li>■ <b>Virtual machine.Configuration.Add existing disk</b> (si se está usando un disco virtual existente)</li> <li>■ <b>Virtual machine.Configuration.Raw device</b> (si se está usando un dispositivo de acceso directo RDM o SCSI)</li> </ul>	Administrador
	En el host, clúster o grupo de recursos de destino: <b>Resource.Assign virtual machine to resource pool</b>	Administrador del grupo de recursos o Administrador
	En el almacén de datos de destino o en la carpeta que contiene un almacén de datos: <b>Datastore.Allocate space</b>	Administrador o Consumidor del almacén de datos
	En la red a la cual se asignará la máquina virtual: <b>Network.Assign network</b>	Administrador o Consumidor de la red
Implementación de una máquina virtual desde una plantilla	En la carpeta de destino o el centro de datos: <ul style="list-style-type: none"> <li>■ <b>Virtual machine .Inventory.Create from existing</b></li> <li>■ <b>Virtual machine.Configuration.Add new disk</b></li> </ul>	Administrador
	En una plantilla o una carpeta de plantillas: <b>Virtual machine.Provisioning.Deploy template</b>	Administrador
	En el host, clúster o grupo de recursos de destino: <b>Resource.Assign virtual machine to resource pool</b>	Administrador
	En el almacén de datos de destino o en la carpeta de almacenes de datos: <b>Datastore.Allocate space</b>	Administrador o Consumidor del almacén de datos
	En la red a la cual se asignará la máquina virtual: <b>Network.Assign network</b>	Administrador o Consumidor de la red
Creación de una instantánea de una máquina virtual	En la máquina virtual o en una carpeta de máquinas virtuales: <b>Virtual machine.Snapshot management. Create snapshot</b>	Administrador o Usuario avanzado de la máquina virtual

Tabla 4-4. Privilegios necesarios para la realización de tareas comunes (continuación)

Tarea	Privilegios necesarios	Función aplicable
Transferencia de una máquina virtual a un grupo de recursos	En la máquina virtual o en una carpeta de máquinas virtuales: <ul style="list-style-type: none"> <li>■ <b>Resource.Assign virtual machine to resource pool</b></li> <li>■ <b>Virtual machine.Inventory.Move</b></li> </ul>	Administrador
	En el grupo de recursos de destino: <ul style="list-style-type: none"> <li>■ <b>Resource.Assign virtual machine to resource pool</b></li> </ul>	Administrador
Instalar un sistema operativo invitado en una máquina virtual	En la máquina virtual o en una carpeta de máquinas virtuales: <ul style="list-style-type: none"> <li>■ <b>Virtual machine.Interaction.Answer question</b></li> <li>■ <b>Virtual machine.Interaction.Console interaction</b></li> <li>■ <b>Virtual machine.Interaction.Device connection</b></li> <li>■ <b>Virtual machine.Interaction.Power Off</b></li> <li>■ <b>Virtual machine.Interaction.Power On</b></li> <li>■ <b>Virtual machine.Interaction.Reset</b></li> <li>■ <b>Virtual machine.Interaction.Configure CD media</b> (si se está instalando desde un CD)</li> <li>■ <b>Virtual machine.Interaction.Configure floppy media</b> (si se está instalando desde un disquete)</li> <li>■ <b>Virtual machine.Interaction.VMware Tools install</b></li> </ul>	Administrador o Usuario avanzado de la máquina virtual
	En un almacén de datos que contiene la imagen ISO de los medios de instalación: <ul style="list-style-type: none"> <li>■ <b>Datastore.Browse datastore</b> (si se está instalando desde una imagen ISO en un almacén de datos)</li> </ul>	Administrador o Usuario avanzado de la máquina virtual
	En el almacén de datos en el que se cargue la imagen ISO de los medios de instalación: <ul style="list-style-type: none"> <li>■ <b>Datastore.Browse datastore</b></li> <li>■ <b>Datastore.Low level file operations</b></li> </ul>	
Migración de una máquina virtual con vMotion	En la máquina virtual o en una carpeta de máquinas virtuales: <ul style="list-style-type: none"> <li>■ <b>Resource.Migrate powered on virtual machine</b></li> <li>■ <b>Recurso.Asignar máquina virtual a un grupo de recursos</b> (si el destino es un grupo de recursos distinto al de origen)</li> </ul>	Administrador del grupo de recursos o Administrador
	En el host, clúster o grupo de recursos de destino (si es distinto al de origen): <ul style="list-style-type: none"> <li>■ <b>Resource.Assign virtual machine to resource pool</b></li> </ul>	Administrador del grupo de recursos o Administrador
Migración en frío (reubicación) de una máquina virtual	En la máquina virtual o en una carpeta de máquinas virtuales: <ul style="list-style-type: none"> <li>■ <b>Resource.Migrate powered off virtual machine</b></li> <li>■ <b>Resource.Assign virtual machine to resource pool</b> (si el destino es un grupo de recursos distinto al de origen)</li> </ul>	Administrador del grupo de recursos o Administrador
	En el host, clúster o grupo de recursos de destino (si es distinto al de origen): <ul style="list-style-type: none"> <li>■ <b>Resource.Assign virtual machine to resource pool</b></li> </ul>	Administrador del grupo de recursos o Administrador

Tabla 4-4. Privilegios necesarios para la realización de tareas comunes (continuación)

Tarea	Privilegios necesarios	Función aplicable
	En el almacén de datos de destino (si es distinto al de origen): <b>Datastore.Allocate space</b>	Administrador o Consumidor del almacén de datos
Migración de una máquina virtual con Storage vMotion	En la máquina virtual o en una carpeta de máquinas virtuales: <b>Resource.Migrate powered on virtual machine</b>	Administrador del grupo de recursos o Administrador
	En el almacén de datos de destino: <b>Datastore.Allocate space</b>	Administrador o Consumidor del almacén de datos
Transferencia de un host a un clúster	En el host: <b>Host.Inventory.Add host to cluster</b>	Administrador
	En el clúster de destino: <b>Host.Inventory.Add host to cluster</b>	Administrador

# Proteger hosts ESXi

# 5

La arquitectura del hipervisor de ESXi tiene muchas características de seguridad incorporadas, como aislamiento de la CPU, aislamiento de la memoria y aislamiento del dispositivo. Es posible configurar características adicionales, como el modo de bloqueo, el reemplazo de certificados y la autenticación de tarjeta inteligente para una seguridad mejorada.

Un host ESXi también está protegido con un firewall. Puede abrir los puertos para el tráfico entrante y saliente según sea necesario, pero debe restringir el acceso a los servicios y los puertos. El modo de bloqueo de ESXi y la limitación de acceso a ESXi Shell puede contribuir aún más a un entorno más seguro. Comenzando con vSphere 6.0, los hosts ESXi participan en la infraestructura de certificados. Los hosts están aprovisionados con certificados firmados por VMware Certificate Authority (VMCA) de forma predeterminada.

Consulte el informe técnico VMware *Seguridad de VMware vSphere Hypervisor* para obtener información adicional sobre la seguridad de ESXi.

Este capítulo incluye los siguientes temas:

- Usar de scripts para administrar las opciones de configuración de hosts
- Configurar hosts ESXi con Host Profiles
- Recomendaciones generales sobre seguridad de ESXi
- Administrar certificados para hosts ESXi
- Personalizar hosts con el perfil de seguridad
- Asignar permisos para ESXi
- Usar Active Directory para administrar usuarios de ESXi
- Usar vSphere Authentication Proxy
- Prácticas recomendadas de seguridad de ESXi
- Configurar la autenticación de tarjeta inteligente de ESXi
- Claves SSH de ESXi
- Usar ESXi Shell
- Modificar la configuración del proxy web de ESXi
- Consideraciones de seguridad de vSphere Auto Deploy

## ■ Administrar archivos de registro de ESXi

# Usar de scripts para administrar las opciones de configuración de hosts

En los entornos con muchos hosts, la administración de hosts con scripts resulta más rápida y es menos proclive a errores que la administración de hosts desde vSphere Web Client.

vSphere incluye varios lenguajes de scripting para la administración de hosts. Consulte la *documentación de vSphere Command-Line* y la *documentación de vSphere API/SDK* para obtener información de referencia y consejos de programación. Consulte las comunidades de VMware para ver otros consejos sobre la administración generada por script. La documentación sobre el administrador de vSphere se centra en el uso de vSphere Web Client para realizar la administración.

### vSphere PowerCLI

VMware vSphere PowerCLI es una interfaz Windows PowerShell para vSphere API. vSphere PowerCLI incluye cmdlets PowerShell para administrar componentes de vSphere.

vSphere PowerCLI incluye más de 200 cmdlets, un conjunto de scripts de muestra y una biblioteca de funciones para las tareas de administración y automatización. Consulte la *documentación de vSphere PowerCLI*.

### vSphere Command-Line Interface (vCLI)

vCLI incluye un conjunto de comandos para administrar las máquinas virtuales y los hosts ESXi. El instalador, que también instala vSphere SDK for Perl, ejecuta sistemas Windows o Linux e instala comandos ESXCLI, comandos vicfg- y un conjunto de otros comandos de vCLI. Consulte la *documentación de vSphere Command-Line Interface*.

A partir de vSphere 6.0, también es posible usar una de las interfaces de scripting en vCloud Suite SDK, como vCloud Suite SDK for Python.

### Procedimiento

- 1 Cree una función personalizada con privilegios limitados.

Por ejemplo, considere crear una función que contenga un conjunto de privilegios para administrar hosts, pero que no incluya privilegios para administrar máquinas virtuales, almacenamiento o redes. Si el script que desea usar solamente extrae información, puede crear una función con privilegios de solo lectura para el host.

- 2 En vSphere Web Client, cree una cuenta de servicio y asigne la función personalizada a esa cuenta.

Puede crear varias funciones personalizadas con diferentes niveles de acceso si desea que el acceso a determinados hosts sea bastante limitado.

### 3 Escriba scripts para comprobar o modificar parámetros, y ejecute esos scripts.

Por ejemplo, puede comprobar o establecer el tiempo de espera interactivo del shell de un host de la siguiente manera:

Lenguaje	Comandos
<b>vCLI (ESXCLI)</b>	<pre>esxcli &lt;conn_options&gt; system settings advanced get / UserVars/ESXiShellTimeout</pre> <pre>esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list   grep /UserVars/ ESXiShellTimeout</pre>
<b>PowerCLI</b>	<pre>#List UserVars.ESXiShellInteractiveTimeout for each host Get-VMHost   Select Name, @{N="UserVars.ESXiShellInteractiveTimeout";E={\$_   Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeout   Select -ExpandProperty Value}}</pre> <pre># Set UserVars.ESXiShellTimeout to 900 on all hosts Get-VMHost   Foreach { Get-AdvancedSetting -Entity \$_ -Name UserVars.ESXiShellInteractiveTimeout   Set- AdvancedSetting -Value 900 }</pre>

- 4 En entornos grandes, cree funciones con diferentes privilegios de acceso y hosts de grupos en carpetas según las tareas que desee realizar. Posteriormente, puede ejecutar scripts en diferentes carpetas desde diferentes cuentas de servicio.
- 5 Verifique que se hayan producido cambios después de ejecutar el comando.

## Configurar hosts ESXi con Host Profiles

Los perfiles de host permiten establecer configuraciones estándar para los hosts ESXi y automatizar el cumplimiento de estas opciones de configuración. Los perfiles de host permiten controlar varios aspectos de la configuración de hosts, como la memoria, el almacenamiento, las redes, etc.

Se pueden configurar perfiles de host para un host de referencia desde vSphere Web Client y aplicar el perfil de host a todos los hosts que comparten las características del host de referencia. También se pueden usar perfiles de host para detectar cambios de configuración en los hosts. Consulte la documentación de *Perfiles de host de vSphere*.

Es posible asociar el perfil de host a un clúster para aplicarlo a todos los hosts de este.

### Procedimiento

- 1 Configure el host de referencia de acuerdo con las especificaciones y cree un perfil de host.
- 2 Asocie el perfil a un host o un clúster.



- 3 Aplique el perfil de host del host de referencia a otros hosts o clústeres.

## Recomendaciones generales sobre seguridad de ESXi

Para proteger un host ESXi contra la intromisión no autorizada o el uso incorrecto, VMware impone restricciones sobre varios parámetros, opciones de configuración y actividades. Es posible reducir las restricciones para cumplir con las necesidades de configuración del usuario. Si lo hace, asegúrese de trabajar en un entorno confiable y de tomar todas las medidas de seguridad necesarias para proteger la red en su totalidad y los dispositivos conectados al host.

### Características de seguridad integradas

Los riesgos para los hosts se mitigan desde el comienzo de la siguiente manera:

- ESXi Shell y SSH están deshabilitados de forma predeterminada.
- Solo una cantidad limitada de puertos de firewall está abierta de forma predeterminada. Puede abrir de forma explícita puertos de firewall adicionales asociados con dispositivos específicos.
- ESXi ejecuta solo los servicios que son fundamentales para administrar sus funciones. La distribución está limitada a las características necesarias para ejecutar ESXi.
- De forma predeterminada, todos los puertos que no son estrictamente necesarios para el acceso de administración al host están cerrados. Si necesita servicios adicionales, debe abrir los puertos en cada situación en particular.
- De forma predeterminada, los cifrados débiles están deshabilitados y las comunicaciones de los clientes están protegidas con SSL. Los algoritmos exactos utilizados para proteger el canal dependen del protocolo de enlace de SSL. Los certificados predeterminados creados en ESXi utilizan el cifrado PKCS#1 SHA-256 con RSA como algoritmo de firmas.
- El servicio web Tomcat, que ESXi utiliza de forma interna para admitir el acceso de Web client, se modificó para ejecutar solo las funciones necesarias para la administración y la supervisión que realiza Web client. Como resultado, ESXi no es vulnerable a los problemas de seguridad de Tomcat que se experimentan durante el uso general.
- VMware supervisa todas las alertas de seguridad que pueden afectar la seguridad de ESXi y emite una revisión de seguridad según sea necesario.
- No se instalan servicios no seguros, como FTP y Telnet, y sus puertos están cerrados de forma predeterminada. Dado que hay servicios más seguros que son fáciles de obtener, como SSH y SFTP, evite el uso de los servicios no seguros y opte por alternativas más seguras. Por ejemplo, utilice Telnet con SSL para acceder a los puertos serie virtuales si SSH no está disponible y se debe utilizar Telnet.

Si debe utilizar servicios no seguros, pero implementó las medidas de seguridad correspondientes para el host, puede abrir puertos de forma explícita para admitir estos servicios.

## Medidas de seguridad adicionales

Tenga en cuenta las siguientes recomendaciones al evaluar la seguridad y la administración de los hosts.

### Restricción del acceso

Si decide habilitar el acceso a la interfaz de usuario de la consola directa (DCUI), a ESXi Shell o a SSH, aplique directivas de seguridad de acceso estrictas.

ESXi Shell tiene acceso privilegiado a ciertas partes del host. Proporcione acceso de inicio de sesión a ESXi Shell solo a usuarios de confianza.

### Acceso no directo a los hosts administrados

Utilice vSphere Web Client para administrar los hosts ESXi que administra un sistema vCenter Server. No acceda a los hosts administrados directamente con vSphere Client y no haga cambios en los hosts administrados desde la DCUI del host.

Si administra hosts con una interfaz o API de scripting, no apunte directamente al host. En su lugar, apunte al sistema vCenter Server que administra el host y especifique el nombre de host.

### Usar vSphere Client, o de las CLI o las API de VMware para administrar hosts ESXi individuales

Utilice vSphere Client o una de las CLI o API de VMware para administrar los hosts ESXi. Acceda al host desde la DCUI o ESXi Shell como usuario raíz solo para solucionar problemas. Si decide utilizar ESXi Shell, limite las cuentas con acceso y establezca los tiempos de espera.

### Usar orígenes de VMware solamente para actualizar los componentes de ESXi

El host ejecuta una variedad de paquetes externos para admitir las interfaces de administración o las tareas que se deben realizar. VMware no admite la actualización de estos paquetes desde cualquier otro elemento que no sea un origen de VMware. Si utiliza una descarga o una revisión de otro origen, puede comprometer la seguridad o las funciones de la interfaz de administración. Compruebe los sitios de proveedores externos y la base de conocimientos de VMware con regularidad para consultar las alertas de seguridad.

---

**Nota** Siga los avisos de seguridad de VMware en <http://www.vmware.com/security/>.

---

## Bloqueo de cuenta y contraseñas ESXi

Para los hosts ESXi, debe utilizar una contraseña con requisitos predefinidos. Puede cambiar el requisito de longitud requerida y clases de caracteres o permitir frases de contraseña si utiliza la opción avanzada `Security.PasswordQualityControl`.

ESXi utiliza el módulo Linux PAM `pam_passwdqc` para la administración y el control de contraseñas. Consulte la página del manual de `pam_passwdqc` para obtener información detallada.

---

**Nota** Los requisitos predeterminados para las contraseñas de ESXi pueden cambiar de una versión a otra. Puede comprobar las restricciones predeterminadas para la contraseña y modificarlas con la opción avanzada `Security.PasswordQualityControl`.

---

## Contraseñas de ESXi

ESXi aplica requisitos de contraseña para el acceso desde la interfaz de usuario de la consola directa, ESXi Shell, SSH o vSphere Client. De manera predeterminada, cuando cree la contraseña deberá incluir una combinación de cuatro clases de caracteres: letras en minúscula, letras en mayúscula, números y caracteres especiales, como el guion bajo o el guion.

---

**Nota** Un carácter en mayúscula al inicio de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan. Un número al final de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan.

---

Las contraseñas no pueden contener una palabra de diccionario o parte de una palabra de diccionario.

## Ejemplos de contraseñas de ESXi

A continuación se indican posibles contraseñas en caso de configurar la opción de la siguiente manera.

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

Con esta configuración, no se permiten las contraseñas que tienen una o dos clases de caracteres y frases de contraseña porque los primeros tres elementos están deshabilitados. Las contraseñas de tres y cuatro clases de caracteres requieren siete caracteres. Consulte la página del manual de `pam_passwdqc` para obtener detalles.

Con esta configuración, se permiten las siguientes contraseñas.

- `xQaTEhb!`: contiene ocho caracteres de tres clases.
- `xQaT3#A`: contiene siete caracteres de cuatro clases.

Las siguientes contraseñas posibles no cumplen con los requisitos.

- `Xqat3hi`: comienza con un carácter en mayúscula, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.
- `xQaTEh2`: termina con un número, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.

## Frase de contraseña de ESXi

En lugar de una contraseña, también puede utilizar una frase de contraseña. Sin embargo, las frases de contraseña están deshabilitadas de forma predeterminada. Puede cambiar este valor predeterminado u otros valores de configuración mediante la opción avanzada `Security.PasswordQualityControl` de vSphere Web Client.

Por ejemplo, puede cambiar la opción por la siguiente.

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

Este ejemplo permite frases de contraseña de al menos 16 caracteres y un mínimo de 3 palabras separadas por espacios.

En el caso de los hosts heredados, todavía se puede cambiar el archivo `/etc/pamd/passwd`, pero no se podrá hacer en las próximas versiones. En su lugar, utilice la opción avanzada `Security.PasswordQualityControl`.

## Modificar las restricciones predeterminadas de contraseña

Puede cambiar la restricción predeterminada de contraseñas y frases de contraseña con la opción avanzada `Security.PasswordQualityControl` (Control de calidad de contraseña de seguridad) del host ESXi. Consulte la documentación de *Administración de vCenter Server y hosts* para obtener información sobre la configuración de las opciones avanzadas de ESXi.

Puede cambiar el valor predeterminado, por ejemplo, a fin de que se requiera un mínimo de 15 caracteres y una cantidad mínima de cuatro palabras, de la siguiente manera:

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

Consulte la página del manual de `pam_passwdqc` para obtener información detallada.

---

**Nota** Aún no se probaron todas las combinaciones posibles de las opciones de `pam_passwdqc`. Después de cambiar la configuración de contraseña predeterminada, realice una prueba adicional.

---

## Comportamiento del bloqueo de cuentas de ESXi

A partir de vSphere 6.0, se admite el bloqueo de cuentas para el acceso a través de SSH y vSphere Web Services SDK. La interfaz de la consola directa (DCUI) y ESXi Shell no admiten el bloqueo de cuentas. De forma predeterminada, se permite un máximo de diez intentos con errores antes de que la cuenta se bloquee. De forma predeterminada, la cuenta se desbloquea después de dos minutos.

## Configurar el comportamiento de inicio de sesión

Puede configurar el comportamiento de inicio de sesión del host ESXi con las siguientes opciones avanzadas:

- `Security.AccountLockFailures`. Cantidad máxima de intentos de inicio de sesión con errores antes de que la cuenta de un usuario se bloquee. Cero deshabilita el bloqueo de cuentas.

- `Security.AccountUnlockTime`. Cantidad de segundos en los que el usuario queda bloqueado.

Consulte la documentación de *Administración de vCenter Server y hosts* para obtener información sobre la configuración de las opciones avanzadas de ESXi.

## Recomendaciones de seguridad para redes de ESXi

El aislamiento del tráfico de red es fundamental para proteger el entorno de ESXi. Las distintas redes requieren distintos niveles de aislamiento y acceso.

El host ESXi usa varias redes. Emplee las medidas de seguridad que correspondan para cada red y aisle el tráfico de aplicaciones y funciones específicas. Por ejemplo, asegúrese de que el tráfico de vSphere vMotion no pase por las redes en las que haya máquinas virtuales. El aislamiento impide las intromisiones. Además, por motivos de rendimiento, también se recomienda usar redes separadas.

- Las redes de infraestructura de vSphere se usan para las características como VMware vSphere vMotion®, VMware vSphere Fault Tolerance y almacenamiento. Estas redes se consideran aisladas por sus funciones específicas y a menudo no se enrutan fuera de un mismo conjunto físico de bastidores de servidores.
- La red de administración aísla los distintos tráficos (tráfico de clientes, de la interfaz de la línea de comandos (CLI) o de la API y del software de terceros) del tráfico normal. Esta red debe estar accesible únicamente para los administradores de sistemas, redes y seguridad. Use jump box o Virtual Private Network (VPN) para proteger el acceso a la red de administración. Controle el acceso dentro de esta red de potenciales orígenes de malware de manera estricta.
- El tráfico de las máquinas virtuales puede transmitirse por medio de una red o de muchas. Puede optimizar el aislamiento de las máquinas virtuales mediante soluciones de firewall virtuales que establezcan reglas de firewall en la controladora de red virtual. Esta configuración se envía junto con una máquina virtual cuando esta se migra de un host a otro dentro del entorno de vSphere.

## Deshabilitar el explorador de objetos administrados (MOB)

El explorador de objetos administrados es una forma de explorar el modelo de objetos VMkernel. Sin embargo, los atacantes pueden utilizar esta interfaz para realizar acciones o cambios maliciosos en la configuración porque se puede cambiar la configuración del host desde el explorador de objetos administrados. Utilice este tipo de explorador únicamente para depurar y asegúrese de que esté deshabilitado en los sistemas de producción.

A partir de vSphere 6.0, el MOB se encuentra deshabilitado de forma predeterminada. Sin embargo, es necesario utilizar el MOB para ciertas tareas, por ejemplo, para extraer un certificado antiguo de un sistema.

### Procedimiento

- 1 Seleccione el host en vSphere Web Client y vaya a **Configuración avanzada del sistema**.

- 2 Compruebe el valor de **Config.HostAgent.plugins.solo.enableMob** y cámbielo según corresponda.

Ya no se recomienda utilizar `vim-cmd` desde ESXi Shell.

## Deshabilitar claves autorizadas (SSH)

Las claves autorizadas permiten habilitar el acceso a un host ESXi a través de SSH sin necesitar autenticación del usuario. Para aumentar la seguridad del host, no permite que los usuarios accedan a este con claves autorizadas.

Un usuario se considera confiable si su clave pública está en el archivo `/etc/ssh/keys-root/authorized_keys` de un host. Los usuarios remotos confiables tienen permiso de acceder al host sin proporcionar una contraseña.

### Procedimiento

- ◆ Para realizar las operaciones diarias, deshabilite SSH en los hosts ESXi.
- ◆ Si SSH está deshabilitado, incluso temporalmente, supervise el contenido del archivo `/etc/ssh/keys-root/authorized_keys` para asegurarse de que ningún usuario tenga permiso de acceder al host sin la autenticación correspondiente.
- ◆ Supervise el archivo `/etc/ssh/keys-root/authorized_keys` para verificar que esté vacío y que no se hayan agregado claves de SSH en él.
- ◆ Si ve que el archivo `/etc/ssh/keys-root/authorized_keys` no está vacío, elimine las claves que contenga.

### Resultados

Al deshabilitar el acceso remoto con claves autorizadas, es posible que se limite la capacidad de ejecutar comandos de forma remota en un host sin proporcionar los datos de inicio de sesión correspondientes. Por ejemplo, esto puede impedir la ejecución de un script remoto desatendido.

## Administrar certificados para hosts ESXi

En vSphere 6.0 y versiones posteriores, VMware Certificate Authority (VMCA) aprovisiona a cada host nuevo de ESXi con un certificado firmado cuya entidad de certificación raíz de forma predeterminada es VMCA. El aprovisionamiento ocurre cuando se agrega el host a vCenter Server explícitamente, o bien como parte de la instalación o la actualización a ESXi 6.0 o una versión posterior.

Puede ver y administrar estos certificados desde vSphere Web Client y por medio de la API `vim.CertificateManager` de vSphere Web Services SDK. No puede ver ni administrar los certificados de ESXi por medio de las CLI de administración de certificados que están disponibles para administrar certificados de vCenter Server.

## Certificados en vSphere 5.5 y en vSphere 6.0

Cuando ESXi y vCenter Server se comunican, estas utilizan SSL para casi todo el tráfico de administración.

En vSphere 5.5 y versiones anteriores, los extremos de SSL están protegidos únicamente por una combinación de nombre de usuario, contraseña y huella digital. Los usuarios pueden reemplazar los correspondientes certificados autofirmados por sus propios certificados. Consulte el centro de documentación de vSphere 5.5.

En vSphere 6.0 y versiones posteriores, vCenter Server admite los siguientes modos de certificación para los hosts ESXi.

**Tabla 5-1. Modos de certificación para hosts ESXi**

Modo de certificación	Descripción
VMware Certificate Authority (predeterminada)	<p>Utilice este modo si VMCA aprovisiona a todos los hosts ESXi, ya sea como entidad de certificación intermedia o de nivel superior.</p> <p>VMCA aprovisiona de forma predeterminada a los hosts ESXi con certificados.</p> <p>En este modo, es posible actualizar y renovar los certificados desde vSphere Web Client.</p>
Entidad de certificación personalizada	<p>Utilice este modo si desea utilizar solamente certificados personalizados que estén firmados por una entidad de certificación externa.</p> <p>En este modo, usted es responsable de administrar los certificados. No puede actualizar ni renovar los certificados desde vSphere Web Client.</p> <p><b>Nota</b> A menos que cambie el modo de certificación al modo Entidad de certificación personalizada, VMCA podrá reemplazar los certificados personalizados, por ejemplo, al seleccionar <b>Renovar</b> en vSphere Web Client.</p>
Modo de huella digital	<p>vSphere 5.5 usaba el modo de huella digital, el cual todavía está disponible como opción de reserva para vSphere 6.0. En este modo, vCenter Server verifica que el certificado tenga el formato correcto, pero no verifica la validez del certificado. Se aceptan incluso los certificados que caducaron.</p> <p>No utilice este modo a menos que detecte problemas con uno de los otros dos modos y no pueda solucionarlos. Algunos servicios de vCenter 6.0 y de versiones posteriores pueden funcionar de forma incorrecta en el modo de huella digital.</p>

## Caducidad de los certificados

A partir de vSphere 6.0, puede ver información sobre la caducidad de los certificados firmados por VMCA o por una entidad de certificación externa en vSphere Web Client. Puede ver la información de todos los hosts administrados por vCenter Server o de hosts individuales. Una alarma de color amarillo se enciende si el certificado se encuentra en estado **Por caducar en breve** (dentro de menos de 8 meses). Una alarma de color rojo se enciende si el certificado se encuentra en estado **Caducidad inminente** (dentro de menos de 2 meses).

## Aprovisionar ESXi y VMCA

Cuando inicia un host ESXi desde los medios de instalación, el host en principio tiene un certificado autogenerated. Cuando se agrega el host al sistema vCenter Server, se le aprovisiona un certificado firmado por VMCA como entidad de certificación raíz.

El proceso es similar para los hosts aprovisionados con Auto Deploy. No obstante, dado que estos hosts no almacenan ningún estado, el servidor Auto Deploy almacena el certificado firmado en su almacén local de certificados. El certificado se vuelve a utilizar en los arranques subsiguientes de los hosts ESXi. Un servidor Auto Deploy forma parte de cualquier nodo de administración o implementación integrado.

Si VMCA no está disponible cuando arranca un host de Auto Deploy por primera vez, el host en principio intentará conectarse y, a continuación, se apagará y reiniciará hasta que VMCA esté disponible y el host pueda ser aprovisionado con un certificado firmado.

## Cambios en el nombre de host y la dirección IP

En vSphere 6.0 y versiones posteriores, un cambio en el nombre de host o la dirección IP podría afectar si vCenter Server considera que un certificado de host es válido o no. El modo en que se agregó el host a vCenter Server puede hacer que sea necesario una intervención manual. Por intervención manual se entiende que se debe volver a conectar el host, o bien se lo debe quitar de vCenter Server y volver a agregar.

Tabla 5-2. Cuando el nombre de host o la dirección IP se deben cambiar de forma manual

Se agregó un host a vCenter Server mediante...	Cambios en el nombre de host	Cambios en la dirección IP
Nombre de host	Problema de conectividad de vCenter Server. Se necesita una intervención manual.	No se debe realizar ninguna acción.
Dirección IP	No se debe realizar ninguna acción.	Problema de conectividad de vCenter Server. Se necesita una intervención manual.



Administración de certificados de ESXi

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_vkuyp3rf/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vkuyp3rf/uiConfId/49694343/))



## Certificados y actualizaciones de hosts

Si actualiza un host ESXi a ESXi 6.0 o una versión posterior, el proceso de actualización reemplaza los certificados autofirmados por certificados firmados por VMCA. El proceso conserva los certificados personalizados incluso si ya caducaron o no son válidos.

El flujo de trabajo recomendado para actualizar depende de los certificados actuales.

### Host aprovisionado con certificados de huellas digitales

Si el host actualmente usa certificados de huellas digitales, se le asignan certificados de VMCA de manera automática como parte del proceso de actualización.

---

**Nota** No se pueden aprovisionar hosts heredados con certificados de VMCA. Es necesario actualizar a ESXi 6.0 o una versión posterior.

---

### Host aprovisionado con certificados personalizados

Si el host se aprovisiona con certificados personalizados (por lo general, certificados externos firmados por entidades de certificación), esos certificados permanecen en su lugar. Cambie el modo de certificación a Personalizado para garantizar que los certificados no se reemplacen por accidente.

---

**Nota** Si el entorno se encuentra en modo VMCA y se actualizan los certificados desde vSphere Web Client, todos los certificados existentes se reemplazan por certificados firmados por VMCA.

---

Posteriormente, vCenter Server supervisa los certificados y muestra información, como la caducidad del certificado, en vSphere Web Client.

Si decide no actualizar los hosts a vSphere 6.0 o una versión posterior, los hosts conservan los certificados que usan actualmente incluso si el host es administrado por un sistema vCenter Server que usa certificados de VMCA.

Siempre se asignan nuevos certificados a los hosts que aprovisiona Auto Deploy cuando se arrancan por primera vez con el software ESXi 6.0. Al actualizar un host aprovisionado por Auto Deploy, el servidor Auto Deploy genera una solicitud de firma de certificados (CSR) para el host y la envía a VMCA. VMCA almacena el certificado firmado para el host. Cuando el servidor Auto Deploy aprovisiona el host, este recupera el certificado de VMCA y lo incluye en el proceso de aprovisionamiento.

Puede utilizar Auto Deploy con certificados personalizados.

## Configuración predeterminada de certificados de ESXi

Cuando vCenter Server pide una solicitud de firma de certificado (CSR) a un host ESXi, usa la configuración predeterminada. Muchos de los valores predeterminados son adecuados para diversas situaciones, pero la información específica de la empresa puede cambiarse.

Considere cambiar la información de la organización y ubicación. Puede cambiar varios de los valores predeterminados mediante vSphere Web Client. Consulte [Cambiar configuración predeterminada de certificados](#).

**Tabla 5-3. Configuración de CSR**

Parámetro	Valor predeterminado	Opción avanzada
Tamaño de clave	2048	N.A.
Algoritmo de clave	RSA	N.A.
Algoritmo de firma de certificado	sha256WithRSAEncryption	N.A.
Nombre común	Nombre del host si este se agregó a vCenter Server por nombre de host. Dirección IP del host si este se agregó a vCenter Server por dirección IP.	N.A.
País	EE. UU.	vpxd.certmgmt.certs.cn.country
Dirección de correo electrónico	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
Localidad (Ciudad)	Palo Alto	vpxd.certmgmt.certs.cn.localityName
Nombre de unidad de organización	Ingeniería de VMware	vpxd.certmgmt.certs.cn.organizationalUnitName
Nombre de organización	VMware	vpxd.certmgmt.certs.cn.organizationName
Estado o provincia	California	vpxd.certmgmt.certs.cn.state
Cantidad de días en que el certificado es válido.	1825	vpxd.certmgmt.certs.cn.daysValid
Umbral duro para la fecha de caducidad del certificado. vCenter Server activa una alarma roja cuando se alcanza el umbral.	30 días	vpxd.certmgmt.certs.cn.hardThreshold
Intervalo de medición de las comprobaciones de validez de certificados de vCenter Server.	5 días	vpxd.certmgmt.certs.cn.pollIntervalDays

Tabla 5-3. Configuración de CSR (continuación)

Parámetro	Valor predeterminado	Opción avanzada
Umbral flexible de la fecha de caducidad del certificado. vCenter Server activa un evento cuando se alcanza el umbral.	240 días	vpxd.certmgmt.certs.cn.softThreshold
Modo en que los usuarios de vCenter Server determinan si los certificados existentes deben reemplazarse. Cambie este modo para conservar los certificados durante la actualización. Consulte <a href="#">Certificados y actualizaciones de hosts</a> .	El valor predeterminado es vmca  También puede especificar el modo de huella digital o personalizado. Consulte <a href="#">Cambiar el modo de certificado</a> .	modo de vpxd.certmgmt.

## Ver la información de caducidad de certificados de varios hosts ESXi

Si utiliza ESXi 6.0 o versiones posteriores, puede ver el estado de los certificados de todos los hosts que administra el sistema vCenter Server. Esta visualización permite determinar si alguno de los certificados está por caducar.

Es posible ver la información del estado de los certificados de los hosts que usan el modo VMCA y los hosts que usan el modo personalizado en vSphere Web Client. No se puede ver la información del estado de los certificados de los hosts que están en modo de huella digital.

### Procedimiento

- Desplácese hasta el host en la jerarquía de inventario de vSphere Web Client.  
De forma predeterminada, la pantalla Hosts no incluye el estado de los certificados.
- Haga clic con el botón derecho en el campo Nombre y seleccione **Mostrar/Ocultar columnas**.
- Seleccione **Certificado válido hasta**, haga clic en **Aceptar**, y desplácese hacia la derecha de ser necesario.  
  
La información del certificado muestra la fecha de caducidad del certificado.  
  
Si un host se agrega a vCenter Server o se vuelve a conectar después de una desconexión, vCenter Server renueva el certificado siempre y cuando el estado sea Caducado, En caducidad, Por caducar o Caducidad inminente. El estado es Expiring si el certificado es válido durante menos de ocho meses, Expiring shortly si el certificado es válido durante menos de dos meses y Expiration imminent si el certificado es válido durante menos de un mes.
- (opcional) Anule la selección de las demás columnas para que le sea más fácil ver lo que le interesa.

### Pasos siguientes

Renueve los certificados que estén por caducar. Consulte [Renovar o actualizar de certificados de ESXi](#).

## Ver los detalles de certificado para un host único de ESXi

En los hosts ESXi 6.0 y las versiones posteriores en modo VMCA o modo personalizado, se pueden ver los detalles de los certificados desde vSphere Web Client. La información de los certificados puede resultar útil para las tareas de depuración.

### Procedimiento

- 1 Desplácese hasta el host en el inventario de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 Seleccione **Sistema** y haga clic en **Certificado**.

Puede examinar la siguiente información. Esta información está disponible únicamente en la vista de host único.

Campo	Descripción
<b>Asunto</b>	El asunto usado durante la generación del certificado.
<b>Emisor</b>	El emisor del certificado.
<b>Válido desde</b>	La fecha en la que se generó el certificado.
<b>Válido hasta</b>	La fecha en la que caduca el certificado.
<b>Estado</b>	El estado del certificado, que puede ser: <div> <p><b>Bueno</b></p> <p>Funcionamiento normal.</p> <p><b>Por caducar</b></p> <p>El certificado caducará pronto.</p> <p><b>Por caducar en breve</b></p> <p>El certificado caducará en ocho meses o menos (valor predeterminado).</p> <p><b>Caducidad inminente</b></p> <p>El certificado caducará en dos meses o menos (valor predeterminado).</p> <p><b>Caducó</b></p> <p>El certificado no es válido porque ya caducó.</p> </div>

## Renovar o actualizar de certificados de ESXi

Si VMCA firma certificados en sus hosts ESXi (6.0 y versiones posteriores), puede renovar dichos certificados desde vSphere Web Client. También puede actualizar todos los certificados del almacén TRUSTED\_ROOTS asociado con vCenter Server.

Puede renovar los certificados cuando estos estén por caducar o si desea aprovisionar el host con un certificado nuevo por otros motivos. Si el certificado ya caducó, debe desconectar el host y volverlo a conectar.

De forma predeterminada, vCenter Server renueva los certificados de un host con estado Caducada, En caducidad inmediata o En caducidad cada vez que el host se agrega al inventario o se vuelve a conectar.

#### Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Web Client.

2 Haga clic en la pestaña **Administrar** y en **Configuración**.

3 Seleccione **Sistema** y haga clic en **Certificado**.

Puede ver información detallada sobre el certificado del host seleccionado.

4 Haga clic en **Renovar** o **Actualizar certificados de CA**.

Opción	Descripción
<b>Renew</b>	Recupera un certificado recién firmado desde VMCA para el host.
<b>Actualiza los certificados de CA</b>	Envía todos los certificados del almacén TRUSTED_ROOTS del almacén vCenter Server VECS al host.

5 Haga clic en **Sí** para confirmar.

## Cambiar configuración predeterminada de certificados

Cuando se agrega un host al sistema vCenter Server, vCenter Server envía una solicitud de firma de certificado (CSR) para el host en VMCA. Se puede cambiar parte de la configuración predeterminada en la CSR a través de la configuración avanzada de vCenter Server en vSphere Web Client.

Cambie la configuración predeterminada de los certificados específica de la empresa. Consulte [Configuración predeterminada de certificados de ESXi](#) para obtener la lista completa de la configuración predeterminada. Algunos de los valores predeterminados no se pueden cambiar.

#### Procedimiento

1 En vSphere Web Client, seleccione el sistema vCenter Server que administra los hosts.

2 Haga clic en la pestaña **Administrar** y en **Configuración**.

3 Haga clic en **Configuración avanzada** y en **Editar**.

4 En la casilla Filtro, introduzca **certmgmt** para mostrar únicamente los parámetros de administración de certificados.

5 Cambie el valor de los parámetros actuales para cumplir con la directiva de la empresa y haga clic en **Aceptar**.

La próxima vez que se agregue un host a vCenter Server, la nueva configuración se utilizará en la CSR que vCenter Server envía a VMCA y en el certificado que se asigna al host.

## Pasos siguientes

Los cambios en los metadatos de los certificados solo afectan a los nuevos certificados. Si desea cambiar los certificados de los hosts que ya son administrados por el sistema vCenter Server, desconecte los hosts y vuelva a conectarlos.

## Descripción general de los cambios de modo de certificación

A partir de vSphere 6.0, los hosts ESXi están aprovisionados de forma predeterminada con certificados de VMCA. En lugar de eso, es posible usar el modo de certificación personalizada o, con fines de depuración, el modo de huella digital. En la mayoría de los casos, los cambios de modo son disruptivos e innecesarios. Si el cambio de modo es necesario, revise el posible impacto que puede provocar antes de realizarlo.

En vSphere 6.0 y versiones posteriores, vCenter Server admite los siguientes modos de certificación para los hosts ESXi.

**Tabla 5-4. Modos de certificación para hosts ESXi**

Modo de certificación	Descripción
VMware Certificate Authority (predeterminada)	De forma predeterminada, se usa VMware Certificate Authority para los certificados de hosts ESXi. VMCA es la entidad de certificación raíz predeterminada, pero se puede configurar como la entidad de certificación intermedia de otra entidad. En este modo, los usuarios pueden administrar los certificados desde vSphere Web Client. También se usa si VMCA es un certificado subordinado.
Entidad de certificación personalizada	Algunos clientes pueden preferir administrar su propia entidad de certificación externa. En este modo, los clientes son responsables de administrar los certificados y no pueden hacerlo desde vSphere Web Client.
Modo de huella digital	vSphere 5.5 usaba el modo de huella digital, el cual todavía está disponible como opción de reserva para vSphere 6.0. No utilice este modo a menos que encuentre problemas que no puede resolver con uno de los otros dos modos. Algunos servicios de vCenter 6.0 y de versiones posteriores pueden funcionar de forma incorrecta en el modo de huella digital.

## Usar certificados ESXi personalizados

Si la directiva de la empresa exige que se use una entidad de certificación raíz distinta de VMCA, puede cambiar el modo de certificación en el entorno después de una minuciosa planificación. El siguiente es el flujo de trabajo recomendado.

- 1 Obtenga los certificados que desea utilizar.
- 2 Coloque el host o los hosts en modo de mantenimiento y desconéctelos de vCenter Server.
- 3 Agregue el certificado raíz de la entidad de certificación personalizada a VECS.

- 4 Implemente los certificados de la entidad de certificación personalizada en cada host y reinicie los servicios de dicho host.
- 5 Cambie al modo de entidad de certificación personalizada. Consulte [Cambiar el modo de certificado](#).
- 6 Conecte el host o los hosts al sistema de vCenter Server.

## Cambiar del modo de entidad de certificación personalizada al modo VMCA

Si está usando el modo de entidad de certificación personalizada y cree que el modo VMCA puede funcionar mejor en su entorno, puede realizar el cambio de modo después de una minuciosa planificación. El siguiente es el flujo de trabajo recomendado.

- 1 Quite todos los hosts del sistema vCenter Server.
- 2 En el sistema vCenter Server, elimine de VECS el certificado raíz de la entidad de certificación externa.
- 3 Cambie al modo VMCA. Consulte [Cambiar el modo de certificado](#).
- 4 Agregue los hosts al sistema vCenter Server.

---

**Nota** Si sigue otro flujo de trabajo para este cambio de modo, se puede generar un comportamiento impredecible.

---

## Conservar los certificados del modo de huella digital durante la actualización

El cambio del modo VMCA al modo de huella digital puede resultar necesario si se producen problemas con los certificados de VMCA. En el modo de huella digital, el sistema vCenter Server comprueba que exista un solo certificado y que su formato sea el correcto, pero no comprueba si el certificado es válido. Consulte [Cambiar el modo de certificado](#) para obtener instrucciones.

## Cambiar del modo de huella digital al modo VMCA

Si usa el modo de huella digital y desea comenzar a usar certificados firmados por VMCA, debe planificar un poco el cambio. El siguiente es el flujo de trabajo recomendado.

- 1 Quite todos los hosts del sistema vCenter Server.
- 2 Cambie al modo de certificación de VMCA. Consulte [Cambiar el modo de certificado](#).
- 3 Agregue los hosts al sistema vCenter Server.

---

**Nota** Si sigue otro flujo de trabajo para este cambio de modo, se puede generar un comportamiento impredecible.

---

## Cambiar del modo de entidad de certificación personalizada al modo de huella digital

Si experimenta problemas con la entidad de certificación personalizada, considere cambiar temporalmente al modo de huella digital. El cambio se ejecutará sin problemas si sigue las instrucciones detalladas en [Cambiar el modo de certificado](#). Después de cambiar el modo, el sistema vCenter Server comprueba solamente el formato del certificado y ya no comprueba la validez del certificado.

## Cambiar del modo de huella digital al modo de entidad de certificación personalizada

Si establece el entorno en el modo de huella digital durante la solución de problemas y desea comenzar a usar el modo de entidad de certificación personalizada, primero debe generar los certificados necesarios. El siguiente es el flujo de trabajo recomendado.

- 1 Quite todos los hosts del sistema vCenter Server.
- 2 Agregue el certificado raíz de la entidad de certificación personalizada al almacén TRUSTED\_ROOTS de VECS en el sistema vCenter Server. Consulte [Actualizar el almacén TRUSTED\\_ROOTS de vCenter Server \(certificados personalizados\)](#).
- 3 En cada host ESXi:
  - a Implemente la clave y el certificado de la entidad de certificación personalizada.
  - b Reinicie los servicios del host.
- 4 Cambie al modo personalizado. Consulte [Cambiar el modo de certificado](#).
- 5 Agregue los hosts al sistema vCenter Server.

## Cambiar el modo de certificado

En la mayoría de los casos, la utilización de VMCA para aprovisionar a los hosts ESXi del entorno es la mejor solución. Si la directiva de la empresa establece la utilización de certificados personalizados con una entidad de certificación raíz diferente, se pueden editar las opciones avanzadas de vCenter Server de modo que los hosts no se aprovisionen automáticamente con certificados VMCA al actualizar los certificados. En este caso, usted será responsable de administrar los certificados del entorno.

Puede utilizar la configuración avanzada de vCenter Server para cambiar al modo de huella digital o al modo de entidad de certificación personalizada. Utilice el modo de huella digital únicamente como opción de reserva.

### Procedimiento

- 1 Seleccione la instancia de vCenter Server que administra los hosts y haga clic en **Configuración**.
- 2 Haga clic en **Configuración avanzada** y en **Editar**.



- 3 En el cuadro Filtro, introduzca **certmgmt** para visualizar únicamente las claves de administración de certificados.
- 4 Cambie el modo vpxd.certmgmt. al valor **personalizado** si desea administrar sus propios certificados o al valor **huella digital** si desea utilizar el modo de huella digital temporalmente; a continuación, haga clic en **Aceptar**.
- 5 Reinicie el servicio de vCenter Server.

## Reemplazo de certificados y claves SSL de ESXi

La directiva de seguridad de su empresa puede requerir que reemplace el certificado SSL predeterminado de ESXi por un certificado firmado por una CA externa en cada host.

De forma predeterminada, los componentes de vSphere utilizan el certificado firmado por VMCA y la clave que se crean durante la instalación. Si elimina el certificado firmado por VMCA de forma accidental, quite el host de su sistema vCenter Server y vuelva a agregarlo. Al agregar el host, vCenter Server solicita un certificado nuevo de VMCA y aprovisiona el host con este certificado.

Reemplace los certificados firmados por VMCA por certificados de una CA de confianza, ya sea una CA comercial o una CA organizacional, si la directiva de la empresa lo requiere.

Los certificados predeterminados están en la misma ubicación que los certificados de vSphere 5.5. Puede reemplazar los certificados predeterminados por certificados de confianza de varias maneras.

---

**Nota** También puede utilizar los objetos administrados `vim.CertificateManager` y `vim.host.CertificateManager` en vSphere Web Services SDK. Consulte la documentación de vSphere Web Services SDK.

---

Después de reemplazar el certificado, debe actualizar el almacén TRUSTED\_ROOTS de VECS en el sistema vCenter Server que administra el host, para que vCenter Server y el host ESXi tengan una relación de confianza.

- **Requisitos de las solicitudes de firma de certificados de ESXi**

Si se desea utilizar un certificado de terceros firmado por una entidad de certificación, ya sea con VMCA como entidad subordinada o con una entidad de certificación personalizada, se debe enviar una solicitud de firma de certificado (CSR) a la entidad de certificación.

- **Reemplazar el certificado y de la clave predeterminados de ESXi Shell**

Puede reemplazar los certificados firmados por VMCA predeterminados de ESXi en ESXi Shell.

- **Reemplazar la clave y el certificado predeterminados con el comando `vifs`**

Puede reemplazar los certificados de ESXi firmados por VMCA predeterminados con el comando `vifs`.

- [Reemplazar un certificado predeterminado mediante el método PUT de HTTPS](#)

Puede usar aplicaciones de terceros para cargar certificados y claves. Las aplicaciones que admiten las operaciones del método PUT de HTTPS funcionan con la interfaz de HTTPS incluida en ESXi.

- [Actualizar el almacén TRUSTED\\_ROOTS de vCenter Server \(certificados personalizados\)](#)

Si configura los hosts ESXi para usar certificados personalizados, debe actualizar el almacén `TRUSTED_ROOTS` en el sistema vCenter Server que administra los hosts.

## Requisitos de las solicitudes de firma de certificados de ESXi

Si se desea utilizar un certificado de terceros firmado por una entidad de certificación, ya sea con VMCA como entidad subordinada o con una entidad de certificación personalizada, se debe enviar una solicitud de firma de certificado (CSR) a la entidad de certificación.

Utilice una CSR con estas características:

- 2048 bits
- PKCS1
- Sin comodines
- Hora de inicio de un día anterior a la hora actual
- CN (y SubjectAltName) establecidos con el nombre de host (o dirección IP) que el host ESXi tiene en el inventario de vCenter Server.

## Reemplazar el certificado y de la clave predeterminados de ESXi Shell

Puede reemplazar los certificados firmados por VMCA predeterminados de ESXi en ESXi Shell.

### Requisitos previos

- Si desea usar certificados firmados por una entidad de certificación (CA) externa, genere la solicitud de certificación, envíela a la entidad de certificación y almacene los certificados en cada host ESXi.
- De ser necesario, habilite ESXi Shell o el tráfico SSH desde vSphere Web Client. Consulte la publicación *Seguridad de vSphere* para obtener información sobre cómo habilitar el acceso a ESXi Shell.
- Todas las transferencias de archivos y demás comunicaciones se realizan en una sesión de HTTPS segura. El usuario que se usa para autenticar la sesión debe tener el privilegio **Host.Configuración.Configuración avanzada** en el host. Consulte la publicación *Seguridad de vSphere* para obtener información sobre cómo asignar privilegios a través de funciones.

### Procedimiento

- 1 Inicie sesión en ESXi Shell, ya sea directamente desde la DCUI o desde un cliente de SSH, como un usuario con privilegios de administrador.

- 2 En el directorio `/etc/vmware/ssl`, cambie el nombre de los certificados existentes con los siguientes comandos.

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

- 3 Copie los certificados que desea utilizar en `/etc/vmware/ssl`.
- 4 Cambie el nombre del certificado nuevo y de la clave por `rui.crt` y `rui.key`.
- 5 Después de instalar el certificado nuevo, reinicie el host.

Como alternativa, puede colocar el host en modo de mantenimiento, instalar el certificado nuevo, utilizar la interfaz de usuario de la consola directa (DCUI) para reiniciar los agentes de administración y, a continuación, establecer el host para que salga del modo de mantenimiento.

#### Pasos siguientes

Actualice el almacén vCenter Server TRUSTED\_ROOTS. Consulte [Actualizar el almacén TRUSTED\\_ROOTS de vCenter Server \(certificados personalizados\)](#).

### Reemplazar la clave y el certificado predeterminados con el comando `vifs`

Puede reemplazar los certificados de ESXi firmados por VMCA predeterminados con el comando `vifs`.

#### Requisitos previos

- Si desea usar certificados firmados por una entidad de certificación (CA) externa, genere la solicitud de certificación, envíela a la entidad de certificación y almacene los certificados en cada host ESXi.
- De ser necesario, habilite ESXi Shell o el tráfico SSH desde vSphere Web Client. Consulte la publicación *Seguridad de vSphere* para obtener información sobre cómo habilitar el acceso a ESXi Shell.
- Todas las transferencias de archivos y demás comunicaciones se realizan en una sesión de HTTPS segura. El usuario que se usa para autenticar la sesión debe tener el privilegio **Host.Configuración.Configuración avanzada** en el host. Consulte la publicación *Seguridad de vSphere* para obtener información sobre cómo asignar privilegios a través de funciones.

#### Procedimiento

- 1 Realice una copia de seguridad de los certificados actuales.
- 2 Genere la solicitud de certificación con las instrucciones de la entidad de certificación.
- 3 Cuando tenga el certificado, use el comando `vifs` para cargar el certificado en la ubicación adecuada del host a través de una conexión SSH.

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

#### 4 Reinicie el host.

##### Pasos siguientes

Actualice el almacén vCenter Server TRUSTED\_ROOTS. Consulte [Actualizar el almacén TRUSTED\\_ROOTS de vCenter Server \(certificados personalizados\)](#).

## Reemplazar un certificado predeterminado mediante el método PUT de HTTPS

Puede usar aplicaciones de terceros para cargar certificados y claves. Las aplicaciones que admiten las operaciones del método PUT de HTTPS funcionan con la interfaz de HTTPS incluida en ESXi.

##### Requisitos previos

- Si desea usar certificados firmados por una entidad de certificación (CA) externa, genere la solicitud de certificación, envíela a la entidad de certificación y almacene los certificados en cada host ESXi.
- De ser necesario, habilite ESXi Shell o el tráfico SSH desde vSphere Web Client. Consulte la publicación *Seguridad de vSphere* para obtener información sobre cómo habilitar el acceso a ESXi Shell.
- Todas las transferencias de archivos y demás comunicaciones se realizan en una sesión de HTTPS segura. El usuario que se usa para autenticar la sesión debe tener el privilegio **Host.Configuración.Configuración avanzada** en el host. Consulte la publicación *Seguridad de vSphere* para obtener información sobre cómo asignar privilegios a través de funciones.

##### Procedimiento

- 1 Realice una copia de seguridad de los certificados actuales.
- 2 En la aplicación de carga, procese cada archivo de la siguiente manera:
  - a Abra el archivo.
  - b Publique el archivo en una de estas ubicaciones.

Opción	Descripción
<b>Certificados</b>	<code>https://hostname/host/ssl_cert</code>
<b>Claves</b>	<code>https://hostname/host/ssl_key</code>

Las ubicaciones `/host/ssl_cert` y `host/ssl_key` conducen a los archivos de certificado en `/etc/vmware/ssl`.

#### 3 Reinicie el host.

##### Pasos siguientes

Actualice el almacén vCenter Server TRUSTED\_ROOTS. Consulte [Actualizar el almacén TRUSTED\\_ROOTS de vCenter Server \(certificados personalizados\)](#).

## Actualizar el almacén TRUSTED\_ROOTS de vCenter Server (certificados personalizados)

Si configura los hosts ESXi para usar certificados personalizados, debe actualizar el almacén TRUSTED\_ROOTS en el sistema vCenter Server que administra los hosts.

### Requisitos previos

Reemplace los certificados de cada host por los certificados personalizados.

### Procedimiento

- 1 Inicie sesión en el sistema vCenter Server que administra los hosts ESXi.  
Inicie sesión en el sistema Windows en el que instaló el software, o en el shell de vCenter Server Appliance.
- 2 Ejecute `vecs-cli` para agregar los nuevos los certificados al almacén TRUSTED\_ROOTS, por ejemplo:

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt
--cert /etc/vmware/ssl/custom1.crt
```

Opción	Descripción
Linux	<pre>/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert /etc/vmware/ssl/ custom1.crt</pre>
Windows	<pre>C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt -- cert c:\ssl\custom1.crt</pre>

### Pasos siguientes

Establezca el modo de certificación en Personalizado. Si el modo de certificación es VCMA (valor predeterminado) y ejecuta una actualización de certificados, los certificados personalizados se reemplazan por los certificados firmados por VMCA. Consulte [Cambiar el modo de certificado](#).

## Usar certificados personalizados con Auto Deploy

De manera predeterminada, el servidor Auto Deploy aprovisiona cada host con certificados firmados por VMCA. Es posible configurar el servidor Auto Deploy para que aprovisiona todos los hosts con certificados personalizados que no estén firmados por VMCA. En ese caso, el servidor Auto Deploy se transforma en una entidad de certificación subordinada a la entidad de certificación externa.

## Requisitos previos

- Solicite un certificado que cumpla con los requisitos de la entidad de certificación correspondiente.
  - Tamaño de clave: 2.048 bits o más (formato codificado PEM)
  - Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8
  - x509 versión 3
  - Para los certificados raíz, la extensión CA se debe establecer en true y el signo cert debe estar en la lista de requisitos.
  - SubjectAltName debe contener DNS Name=<machine\_FQDN>
  - Formato CRT
  - Contiene los siguientes usos de claves: firma digital, no repudio, cifrado de clave
  - Hora de inicio de un día anterior a la hora actual
  - CN (y SubjectAltName) establecidos con el nombre de host (o dirección IP) que el host ESXi tiene en el inventario de vCenter Server.
- Asigne un nombre para el certificado y los archivos de claves `rbd-ca.crt` y `rbd-ca.key`.

## Procedimiento

- 1 Realice una copia de seguridad de los certificados de ESXi predeterminados.  
Los certificados están ubicados en `/etc/vmware-rbd/ssl/`.
- 2 Desde vSphere Web Client, detenga el servicio de Auto Deploy.
  - a Seleccione **Administración** y haga clic en **Configuración del sistema** en **Implementación**.
  - b Haga clic en **Servicios**.
  - c Haga clic con el botón derecho en el servicio que desee detener y seleccione **Detener**.
- 3 En el sistema donde se ejecuta el servicio de Auto Deploy, reemplace `rbd-ca.crt` y `rbd-ca.key` en `/etc/vmware-rbd/ssl/` por el certificado personalizado y el archivo de claves.
- 4 En el sistema donde se ejecuta el servicio de Auto Deploy, actualice el almacén TRUSTED\_ROOTS de VECS para utilizar los nuevos certificados.

```
vecs-cli entry delete --store TRUSTED_ROOTS --alias
    rbd_cert
vecs-cli entry create --store TRUSTED_ROOTS --alias
    rbd_cert --cert /etc/vmware-rbd/ssl/rbd-ca.crt
```

## Windows

```
C:\Archivos de programa\VMware\vCenter Server\vmafdd\vecs-cli.exe
```

### Linux

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

- 5 Cree un archivo `castore.pem` que incluya el contenido de `TRUSTED_ROOTS` y coloque el archivo en el directorio `/etc/vmware-rbd/ssl/`.

En el modo personalizado, usted es responsable de mantener este archivo.

- 6 Cambie el modo de certificación del sistema vCenter Server a **custom**.

Consulte [Cambiar el modo de certificado](#).

- 7 Reinicie el servicio de vCenter Server e inicie el servicio de Auto Deploy.

### Resultados

La próxima vez que se aprovisiona un host configurado para utilizar Auto Deploy, el servidor Auto Deploy genera un certificado que utiliza el certificado raíz que se acaba de agregar al almacén `TRUSTED_ROOTS`.

## Restaurar archivos de certificados y claves de ESXi

Al reemplazar un certificado en un host ESXi mediante vSphere Web Services SDK, el certificado y la clave anteriores se anexan a un archivo `.bak`. Para restaurar certificados anteriores, mueva la información del archivo `.bak` al archivo actual de certificados y claves.

El certificado y la clave del host se encuentran en `/etc/vmware/ssl/rui.crt` y `/etc/vmware/ssl/rui.key`. Al reemplazar el certificado y la clave de un host mediante el objeto administrado `vim.CertificateManager` de vSphere Web Services SDK, la clave y el certificado anteriores se anexan al archivo `/etc/vmware/ssl/rui.bak`.

---

**Nota** Si reemplaza el certificado con HTTP PUT, `vifs` o desde ESXi Shell, los certificados existentes no se anexan al archivo `.bak`.

---

### Procedimiento

- 1 En el host ESXi, busque el archivo `/etc/vmware/ssl/rui.bak`.

El archivo tiene el siguiente formato.

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

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

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

- 2 Copie el texto que empieza con -----BEGIN PRIVATE KEY----- y termina con -----END PRIVATE KEY----- en el archivo `/etc/vmware/ssl/rui.key`.

Incluya -----BEGIN PRIVATE KEY----- y -----END PRIVATE KEY-----.

- 3 Copie el texto que está entre -----BEGIN CERTIFICATE----- y -----END CERTIFICATE----- en el archivo `/etc/vmware/ssl/rui.crt`.

Incluya -----BEGIN CERTIFICATE----- y -----END CERTIFICATE-----.

- 4 Reinicie el host o envíe eventos `ssl_reset` a todos los servicios que utilizan las claves.

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

## Personalizar hosts con el perfil de seguridad

Puede personalizar muchos de los valores de seguridad fundamentales del host mediante el panel de perfil de seguridad disponible en vSphere Web Client. El perfil de seguridad es especialmente útil para la administración de un host único. Si debe administrar varios hosts, considere utilizar una de las CLI o los SDK y automatizar las tareas de personalización.

## Configurar firewalls de ESXi

ESXi incluye un firewall que está habilitado de forma predeterminada.

En el momento de realizar la instalación, el firewall de ESXi se configura para bloquear el tráfico entrante y saliente, excepto el tráfico de los servicios que están habilitados en el perfil de seguridad del host.

Al abrir puertos en el firewall, tenga en cuenta que el acceso no restringido a los servicios que se ejecutan en un host ESXi pueden exponer un host a ataques externos y acceso no autorizado. Para reducir el riesgo, configure el firewall de ESXi para que permita el acceso solo desde redes autorizadas.

---

**Nota** El firewall también permite pings del protocolo Control Message Protocol (ICMP) y la comunicación con los clientes DHCP y DNS (solo UDP).

---

Es posible administrar puertos de firewall de ESXi de la siguiente manera:

- Utilice el perfil de seguridad para cada host de vSphere Web Client. Consulte [Administrar la configuración del firewall de ESXi](#)
- Utilice los comandos ESXCLI en la línea de comandos o en los scripts. Consulte [Comandos de firewall ESXCLI de ESXi](#).
- Utilice un VIB si el puerto que desea abrir no está incluido en el perfil de seguridad.



Los VIB personalizados se crean con la herramienta vibauthor disponible en VMware Labs. Para instalar el VIB personalizado, se debe cambiar el nivel de aceptación del host ESXi a CommunitySupported. Consulte el artículo [2007381](#) de la base de conocimientos de VMware.

**Nota** Si pide al soporte técnico de VMware que investigue un problema en un host ESXi con un VIB CommunitySupported instalado, es posible que el soporte de VMware solicite que se desinstale el VIB CommunitySupported como medida de solución de problemas para determinar si este está relacionado con el problema que se investiga.



Conceptos del firewall de ESXi

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_8qp59yqe/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8qp59yqe/uiConfId/49694343/))

El comportamiento del conjunto de reglas del cliente NFS (`nfsClient`) es diferente a otros conjuntos de reglas. Cuando el conjunto de reglas del cliente NFS está habilitado, todos los puertos TCP salientes están abiertos para los hosts de destino que se incluyen en la lista de direcciones IP permitidas. Consulte [Comportamiento de firewall del cliente NFS](#) para obtener más información.

## Administrar la configuración del firewall de ESXi

Puede configurar conexiones entrantes o salientes en el firewall para un servicio o un agente de administración desde vSphere Web Client o en la línea de comandos.

**Nota** Si hay distintos servicios con reglas de puerto superpuestas, al habilitar un servicio, es posible que se habiliten otros servicios de forma implícita. Para evitar este problema, se pueden especificar qué direcciones IP tienen permiso para acceder a cada servicio en el host.

### Procedimiento

- 1 Desplácese hasta el host en el inventario de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 Haga clic en **Perfil de seguridad**.

vSphere Web Client muestra una lista de conexiones activas entrantes y salientes con los correspondientes puertos de firewall.

- 4 En la sección Firewall, haga clic en **Editar**.

La pantalla muestra los conjuntos de reglas de firewall, que incluyen el nombre de la regla y la información asociada.

- 5 Seleccione los conjuntos de reglas para habilitarlos o desactive la casilla para deshabilitarlos.

Columna	Descripción
<b>Puertos entrantes y salientes</b>	Los puertos que vSphere Web Client abre para el servicio.
<b>Protocolo</b>	El protocolo que utiliza un servicio.
<b>Daemon</b>	El estado de los daemons asociados con el servicio.

- 6 En algunos servicios, es posible administrar los detalles de servicio.
  - Utilice los botones **Iniciar**, **Detener** o **Reiniciar** para cambiar el estado de un servicio temporalmente.
  - Cambie la directiva de inicio para que el servicio se inicie con el host o con la utilización de puertos.
- 7 Para algunos servicios, se pueden especificar explícitamente las direcciones IP para las que se permiten conexiones.  
 Consulte [Agregar direcciones IP permitidas para un host ESXi](#).
- 8 Haga clic en **Aceptar**.

## Agregar direcciones IP permitidas para un host ESXi

De forma predeterminada, el firewall de cada servicio permite el acceso a todas las direcciones IP. Para restringir el tráfico, cambie cada servicio para permitir el tráfico solo desde la subred de administración. También puede anular la selección de algunos servicios si el entorno no los usa.

Puede usar vSphere Web Client, vCLI o PowerCLI para actualizar la lista de direcciones IP permitidas para un servicio. De forma predeterminada, todas las direcciones IP están permitidas para un servicio.



Agregar direcciones IP permitidas al firewall de ESXi  
 ([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_Ougsspa2/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_Ougsspa2/uiConfId/49694343/))

### Procedimiento

- 1 Desplácese hasta el host en el inventario de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 En Sistema, haga clic en **Perfil de seguridad**.
- 4 En la sección Firewall, haga clic en **Editar** y seleccione un servicio de la lista.
- 5 En la sección Direcciones IP permitidas, desactive la casilla **Permitir conexiones desde cualquier dirección IP** e introduzca las direcciones IP de las redes que tienen permiso para conectarse al host.

Separe las direcciones IP con comas. Puede utilizar los siguientes formatos de dirección:

- 192.168.0.0/24
- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

- 6 Haga clic en **Aceptar**.

## Puertos de firewall entrantes y salientes para hosts de ESXi

vSphere Web Client permite abrir y cerrar puertos de firewall para cada servicio o para admitir tráfico de las direcciones IP seleccionadas.

En la siguiente tabla, se muestran los firewalls para los servicios que se instalan habitualmente. Si instala otros VIB en el host, es posible que estén disponibles otros puertos de firewall y servicios adicionales.

**Tabla 5-5. Conexiones de firewall entrantes**

Servicio	Puerto	Comentario
Servidor CIM	5988 (TCP)	Servidor para CIM (Common Information Model).
Servidor CIM seguro	5989 (TCP)	Servidor seguro para CIM.
CIM SLP	427 (TCP, UDP)	El cliente CIM usa el protocolo de ubicación de servicios, versión 2 (SLPv2), para buscar servidores CIM.
DHCPv6	546 (TCP, UDP)	Cliente DHCP para IPv6.
DVSSync	8301, 8302 (UDP)	Se usan puertos de DVSSync para sincronizar los estados de los puertos virtuales distribuidos entre los hosts que tienen habilitada la opción de grabación/reproducción de VMware FT. Solo los hosts que ejecutan máquinas virtuales principales o de copia de seguridad deben tener abiertos estos puertos. En los hosts que no usan VMware FT, no es necesario que estos puertos estén abiertos.
NFC	902 (TCP)	Network File Copy (NFC) proporciona un servicio de FTP basado en los tipos de archivos para los componentes de vSphere. Como opción predeterminada, ESXi usa NFC para las operaciones, como la copia y la transferencia de datos entre áreas de almacenamiento de datos.
Servicio de agrupación en clústeres de Virtual SAN	12345, 23451 (UDP)	Servicio de directorio de membresía y supervisión de clústeres de Virtual SAN. Usa multidifusión IP basada en UDP para establecer los miembros del clúster y distribuir los metadatos de Virtual SAN a todos los miembros del clúster. Si se deshabilita, Virtual SAN no funciona.
Cliente DHCP	68 (UDP)	Cliente DHCP para IPv4.
Cliente DNS	53 (UDP)	Cliente DNS.
Fault Tolerance	8200, 8100, 8300 (TCP, UDP)	Tráfico entre hosts para vSphere Fault Tolerance (FT).

Tabla 5-5. Conexiones de firewall entrantes (continuación)

Servicio	Puerto	Comentario
Servicio de enrutador lógico distribuido de NSX	6999 (UDP)	Servicio de enrutador virtual distribuido de NSX. El puerto de firewall asociado con este servicio se abre cuando se instalan los VIB de NSX y se crea el módulo de VDR. Si no hay instancias de VDR asociadas con el host, no es necesario que el puerto esté abierto.  En versiones anteriores del producto, este servicio se llamaba Enrutador lógico distribuido de NSX.
Transporte de Virtual SAN	2233 (TCP)	Transporte fiable de datagramas de Virtual SAN. Emplea TCP y se utiliza para E/S de almacenamiento de Virtual SAN. Si se deshabilita, Virtual SAN no funciona.
Servidor SNMP	161 (UDP)	Permite que el host se conecte a un servidor SNMP.
Servidor SSH	22 (TCP)	Es necesario para el acceso a SSH.
vMotion	8000 (TCP)	Es necesario para la migración de máquinas virtuales con vMotion.
vSphere Web Client	902, 443 (TCP)	Conexiones de clientes
vsanvp	8080 (TCP)	VSAN VASA Vendor Provider. Lo utiliza el servicio de administración de almacenamiento (SMS) que forma parte de vCenter para acceder a la información sobre cumplimiento de normas, funcionalidades y perfiles de almacenamiento de Virtual SAN. Si está deshabilitado, la administración del almacenamiento basada en perfiles (SPBM) de Virtual SAN no funciona.
vSphere Web Access	80 (TCP)	Página principal, con vínculos de descarga para diferentes interfaces.
protocolo RFB	5900-5964 (TCP)	Lo utilizan herramientas de administración como VNC.

Tabla 5-6. Conexiones de firewall salientes

Servicio	Puerto	Comentario
CIM SLP	427 (TCP, UDP)	El cliente CIM usa el protocolo de ubicación de servicios, versión 2 (SLPv2), para buscar servidores CIM.
DHCPv6	547 (TCP, UDP)	Cliente DHCP para IPv6.

Tabla 5-6. Conexiones de firewall salientes (continuación)

Servicio	Puerto	Comentario
DVSSync	8301, 8302 (UDP)	Se usan puertos de DVSSync para sincronizar los estados de los puertos virtuales distribuidos entre los hosts que tienen habilitada la opción de grabación/reproducción de VMware FT. Solo los hosts que ejecutan máquinas virtuales principales o de copia de seguridad deben tener abiertos estos puertos. En los hosts que no usan VMware FT, no es necesario que estos puertos estén abiertos.
HBR	44046, 31031 (TCP)	Se usa para tráfico de replicación continuo de vSphere Replication y VMware Site Recovery Manager.
NFC	902 (TCP)	Network File Copy (NFC) proporciona un servicio de FTP basado en los tipos de archivos para los componentes de vSphere. Como opción predeterminada, ESXi usa NFC para las operaciones, como la copia y la transferencia de datos entre áreas de almacenamiento de datos.
WOL	9 (UDP)	Utilizado por Wake-on-LAN.
Servicio de agrupación en clústeres de Virtual SAN	12345 23451 (UDP)	Servicio de directorio de membresía y supervisión de clústeres utilizado por Virtual SAN.
Cliente DHCP	68 (UDP)	Cliente DHCP.
Cliente DNS	53 (TCP, UDP)	Cliente DNS.
Fault Tolerance	80, 8200, 8100, 8300 (TCP, UDP)	Es compatible con VMware Fault Tolerance.
Cliente iSCSI de software	3260 (TCP)	Es compatible con iSCSI de software.
Servicio de enrutador lógico distribuido de NSX	6999 (UDP)	El puerto de firewall asociado con este servicio se abre cuando se instalan los VIB de NSX y se crea el módulo de VDR. Si no hay instancias de VDR asociadas con el host, no es necesario que el puerto esté abierto.
rabbitmqproxy	5671 (TCP)	Un proxy que se ejecuta en el host ESXi y que permite a las aplicaciones ejecutarse dentro de máquinas virtuales para comunicarse con los agentes de AMQP que se ejecutan en el dominio de red de vCenter. No es necesario que la máquina virtual esté en la red (es decir, no se requiere la NIC). El proxy se conecta con los agentes del dominio de red de vCenter. Por lo tanto, como mínimo, las direcciones IP de las conexiones salientes deben incluir los agentes actuales en uso o los agentes futuros. Pueden agregarse agentes si el cliente desea escalar verticalmente.

Tabla 5-6. Conexiones de firewall salientes (continuación)

Servicio	Puerto	Comentario
Transporte de Virtual SAN	2233 (TCP)	Se utiliza para tráfico de RDT (comunicación de punto a punto de Unicast) entre nodos de Virtual SAN.
vMotion	8000 (TCP)	Es necesario para la migración de máquinas virtuales con vMotion.
VMware vCenter Agent	902 (UDP)	vCenter Server Agent.
vsanvp	8080 (TCP)	Se utiliza para tráfico de proveedores de Virtual SAN.

## Comportamiento de firewall del cliente NFS

El conjunto de reglas de firewall del cliente NFS se comporta de forma diferente a otros conjuntos de reglas de firewall de ESXi. ESXi configura los parámetros del cliente NFS cuando se monta o desmonta un almacén de datos de NFS. El comportamiento varía según la versión de NFS.

Cuando se agrega, monta o desmonta un almacén de datos de NFS, el comportamiento que se obtiene varía según la versión de NFS.

### Comportamiento de firewall de NFS v3

Cuando se agrega o monta un almacén de datos de NFS v3, ESXi comprueba el estado del conjunto de reglas de firewall del cliente NFS (`nfsClient`).

- Si el conjunto de reglas `nfsClient` está deshabilitado, ESXi habilita el conjunto de reglas y deshabilita la directiva Permitir todas las direcciones IP estableciendo la marca `allowedAll` en `FALSE`. La dirección IP del servidor NFS se agrega a la lista de direcciones IP salientes permitidas.
- Si el conjunto de reglas `nfsClient` está habilitado, el estado del conjunto de reglas y la directiva de direcciones IP permitidas no se cambian. La dirección IP del servidor NFS se agrega a la lista de direcciones IP salientes permitidas.

**Nota** Si habilita manualmente el conjunto de reglas `nfsClient` o configura manualmente la directiva Permitir todas las direcciones IP, ya sea antes o después de agregar un almacén de datos de NFS v3 al sistema, la configuración se anula cuando se desmonta el último almacén de datos de NFS v3. El conjunto de reglas `nfsClient` se deshabilita cuando se desmontan todos los almacenes de datos de NFS v3.

Cuando se quita o se desmonta un almacén de datos de NFS v3, ESXi realiza una de las siguientes acciones.

- Si ninguno de los almacenes de datos de NFS v3 restantes se monta desde el servidor del almacén de datos que se desmonta, ESXi quita la dirección IP del servidor de la lista de direcciones IP salientes.

- Si ninguno de los almacenes de datos de NFS v3 permanece después de la operación de desmontaje, ESXi deshabilita el conjunto de reglas de firewall de `nfsClient`.

### Comportamiento de firewall de NFS v4.1

Cuando se monta el primer almacén de datos NFS v4.1, ESXi habilita el conjunto de reglas `nfs41client` y establece su marca `allowedAll` en `TRUE`. Esta acción abre el puerto 2049 para todas las direcciones IP. Cuando se desmonta el almacén de datos NFS v4.1, el estado del firewall no se ve afectado. De esta forma, el primer montaje de NFS v4.1 abre el puerto 2049, y ese puerto permanece habilitado a menos que se cierre explícitamente.

### Comandos de firewall ESXCLI de ESXi

Si el entorno incluye varios hosts ESXi, se recomienda automatizar la configuración del firewall mediante los comandos ESXCLI o vSphere Web Services SDK.

Se pueden utilizar los comandos de ESXi Shell o vSphere CLI en la línea de comandos para configurar ESXi a fin de automatizar la configuración del firewall. Consulte *Introducción a vSphere Command-Line Interface* para ver una introducción y *Ejemplos y conceptos de vSphere Command-Line Interface* para ver ejemplos de uso de ESXCLI para administrar firewalls y reglas de firewall.

**Tabla 5-7. Comandos de firewall**

Comando	Descripción
<code>esxcli network firewall get</code>	Devuelve el estado habilitado o deshabilitado del firewall y enumera las acciones predeterminadas.
<code>esxcli network firewall set --default-action</code>	Se establece en <code>true</code> para que la acción predeterminada pase, y en <code>false</code> para que la acción predeterminada se descarte.
<code>esxcli network firewall set --enabled</code>	Habilita o deshabilita el firewall de ESXi.
<code>esxcli network firewall load</code>	Carga los archivos de configuración del conjunto de módulos y reglas del firewall.
<code>esxcli network firewall refresh</code>	Actualiza la configuración del firewall mediante la lectura de los archivos del conjunto de reglas si se carga el módulo de firewall.
<code>esxcli network firewall unload</code>	Destruye los filtros y descarga el módulo de firewall.
<code>esxcli network firewall ruleset list</code>	Enumera la información de los conjuntos de reglas.
<code>esxcli network firewall ruleset set --allowed-all</code>	Se establece en <code>true</code> para permitir un acceso total a todas las direcciones IP, o en <code>false</code> para utilizar una lista de direcciones IP permitidas.
<code>esxcli network firewall ruleset set --enabled --ruleset-id=&lt;string&gt;</code>	Se establece en <code>true</code> o <code>false</code> para habilitar o deshabilitar el conjunto de reglas especificado.
<code>esxcli network firewall ruleset allowedip list</code>	Enumera las direcciones IP permitidas del conjunto de reglas especificado.

Tabla 5-7. Comandos de firewall (continuación)

Comando	Descripción
<code>esxcli network firewall ruleset allowedip add</code>	Permite acceder al conjunto de reglas desde la dirección IP o el intervalo de direcciones IP especificado.
<code>esxcli network firewall ruleset allowedip remove</code>	Quita el acceso al conjunto de reglas desde la dirección IP o el intervalo de direcciones IP especificados.
<code>esxcli network firewall ruleset rule list</code>	Enumera las reglas de cada conjunto de reglas del firewall.

## Personalizar los servicios de ESXi desde el perfil de seguridad

Un host ESXi incluye varios servicios que se ejecutan de manera predeterminada. Otros servicios, como SSH, están incluidos en el perfil de seguridad del host. Puede habilitar y deshabilitar estos servicios según sea necesario si la directiva de la empresa lo permite.

Usar [vSphere Web Client para habilitar el acceso a ESXi Shell](#) es un ejemplo que muestra cómo habilitar un servicio.

**Nota** La habilitación de servicios afecta la seguridad del host. No habilite un servicio a menos que sea estrictamente necesario.

Los servicios disponibles dependen de los VIB que están instalados en el host ESXi. No puede agregar servicios sin instalar un VIB. Algunos productos de VMware, por ejemplo vSphere HA, instalan los VIB en los hosts para que los servicios y sus correspondientes puertos de firewall estén disponibles.

En una instalación predeterminada, puede modificar el estado de los siguientes servicios desde vSphere Web Client.

Tabla 5-8. Servicios de ESXi en el perfil de seguridad

Servicio	Predeterminado	Descripción
Interfaz de usuario de consola directa	En ejecución	El servicio de la interfaz de usuario de la consola directa (DCUI) permite interactuar con un host ESXi desde el host de la consola local mediante menús basados en texto.
ESXi Shell	Detenido	ESXi Shell está disponible desde la DCUI e incluye un conjunto de comandos totalmente compatibles, así como un conjunto de comandos para solucionar problemas y corregir errores. Debe habilitar el acceso a ESXi Shell desde la consola directa de cada sistema. Puede habilitar el acceso a ESXi Shell local o el acceso a ESXi Shell mediante SSH.
SSH	Detenido	El servicio del cliente SSH del host que permite realizar conexiones remotas mediante Secure Shell.
Daemon para la formación de equipos basada en cargas	En ejecución	Formación de equipos basada en cargas.



Tabla 5-8. Servicios de ESXi en el perfil de seguridad (continuación)

Servicio	Predeterminado	Descripción
Servidor para la autenticación de seguridad local (servicio de Active Directory)	Detenido	Parte del servicio de Active Directory. Este servicio se inicia al configurar ESXi para Active Directory.
Redirector de E/S (servicio de Active Directory)	Detenido	Parte del servicio de Active Directory. Este servicio se inicia al configurar ESXi para Active Directory.
Servidor de inicio de sesión de red (servicio de Active Directory)	Detenido	Parte del servicio de Active Directory. Este servicio se inicia al configurar ESXi para Active Directory.
Daemon de NTP	Detenido	Daemon del protocolo Network Time Protocol.
Servidor CIM	En ejecución	Servicio que las aplicaciones del modelo de información común pueden utilizar (CIM).
Servidor SNMP	Detenido	Daemon del SNMP. Consulte <i>Supervisión y rendimiento de vSphere</i> para obtener información sobre cómo configurar el SNMP v1, v2 y v3.
Servidor de Syslog	Detenido	Daemon de Syslog. Puede habilitar Syslog desde la configuración avanzada del sistema en vSphere Web Client. Consulte <i>Instalación y configuración de vSphere</i> .
vSphere High Availability Agent	Detenido	Admite la funcionalidad de vSphere High Availability.
Daemon de vProbe	Detenido	Daemon de vProbe.
VMware vCenter Agent	En ejecución	Agente de vCenter Server. Permite que vCenter Server se conecte a un host ESXi. Específicamente, vpxa es el canal de comunicación con el daemon del host que, a su vez, se comunica con el kernel de ESXi.
Servidor X.Org	Detenido	Servidor X.Org. Esta característica opcional es de uso interno para los gráficos 3D de las máquinas virtuales.

## Habilitar o deshabilitar un servicio en el perfil de seguridad

Puede habilitar o deshabilitar uno de los servicios enumerados en el perfil de seguridad desde vSphere Web Client.

Después de la instalación, algunos servicios se ejecutan de manera predeterminada, pero otros se interrumpen. En ciertos casos, es necesario realizar otro paso de configuración para que el servicio esté disponible en la UI de vSphere Web Client. Por ejemplo, el servicio NTP es una forma de obtener información de tiempo precisa, pero este servicio solamente funciona cuando se abren los puertos requeridos en el firewall.

### Requisitos previos

Conéctese a vCenter Server con vSphere Web Client.

## Procedimiento

- 1 Desplácese hasta un host en el inventario de vSphere Web Client y seleccione un host.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 En Sistema, seleccione **Perfil de seguridad** y haga clic en **Editar**.
- 4 Desplácese hasta el servicio que desea cambiar.
- 5 En el panel Detalles de servicio, seleccione **Iniciar**, **Detener** o **Reiniciar** para realizar un cambio por única vez en el estado del host, o bien haga la selección desde el menú **Directiva de inicio** para cambiar el estado del host en todos los reinicios.
  - **Iniciar automáticamente si alguno de los puertos está abierto, y detener cuando todos los puertos están cerrados:** la configuración predeterminada para estos servicios. Si existe algún puerto abierto, el cliente intenta comunicarse con los recursos de red del servicio. Si existen algunos puertos abiertos, pero el puerto de un servicio específico está cerrado, se produce un error en el intento. Si el puerto saliente correspondiente está abierto, el servicio comienza a completar el inicio.
  - **Iniciar y detener con host:** el servicio se inicia poco después de que se enciende el host, y se cierra poco después de que se apaga el host. Al igual que con **Iniciar automáticamente si existen puertos abiertos y detener cuando todos los puertos están cerrados**, esta opción indica que el servicio intenta regularmente completar sus tareas, como la comunicación con el servidor NTP especificado. Si el puerto se cerró, pero se abrió posteriormente, el cliente comienza a completar sus tareas poco después de eso.
  - **Iniciar y detener manualmente:** el host conserva la configuración del servicio determinada por el usuario, más allá de que los puertos estén abiertos o cerrados. Cuando un usuario inicia el servicio NTP, el servicio sigue en ejecución hasta que el host se enciende. Si el servicio se inicia y el host está apagado, el servicio se detiene como parte del proceso de apagado; pero en cuanto el host se enciende, el servicio vuelve a iniciarse, y así se conserva el estado determinado por el usuario.

---

**Nota** Esta configuración se aplica únicamente a la configuración de servicio establecida mediante vSphere Web Client o a las aplicaciones creadas en vSphere Web Services SDK. Toda configuración establecida por otros medios, como desde ESXi Shell o mediante archivos de configuración, no se ve afectada por esta configuración.

---

## Modo de bloqueo

Para mejorar la seguridad de los hosts ESXi, puede ponerlos en modo de bloqueo. En el modo de bloqueo, las operaciones deben realizarse mediante vCenter Server de forma predeterminada.

A partir de vSphere 6.0, puede seleccionar el modo de bloqueo normal o el modo de bloqueo estricto, que ofrecen diferentes grados de bloqueo. vSphere 6.0 también incluye la lista de usuarios con excepción. Los usuarios con excepción no pierden sus privilegios cuando el host entra en el modo de bloqueo. Utilice la lista de usuarios con excepción para agregar cuentas de soluciones de terceros y aplicaciones externas que deben tener acceso directo al host cuando este último está en modo de bloqueo. Consulte [Especificar usuarios con excepción para el modo de bloqueo](#).



Modo de bloqueo en vSphere 6

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_zg4ylgu0/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_zg4ylgu0/uiConfId/49694343/))

## Modo de bloqueo normal y modo de bloqueo estricto

A partir de vSphere 6.0, puede seleccionar el modo de bloqueo normal o el modo de bloqueo estricto, que ofrecen diferentes grados de bloqueo.

### Modo de bloqueo normal

En el modo de bloqueo normal, el servicio de la DCUI no se interrumpe. Si se pierde la conexión con el sistema vCenter Server y el acceso a través de vSphere Web Client deja de estar disponible, las cuentas con privilegios pueden iniciar sesión en la interfaz de la consola directa del host ESXi y salir del modo de bloqueo. Solo las siguientes cuentas pueden acceder a la interfaz de usuario de la consola directa:

- Cuentas de la lista de usuarios con excepción para el modo de bloqueo que tienen privilegios administrativos en el host. La lista de usuarios con excepción está pensada para las cuentas de servicio que realizan tareas muy específicas. Al agregar administradores de ESXi a esta lista, se anula el propósito del modo de bloqueo.
- Usuarios definidos en la opción avanzada DCUI.Access del host. Esta opción sirve para tener acceso de emergencia a la interfaz de la consola directa en caso de que se pierda la conexión con vCenter Server. Estos usuarios no necesitan privilegios administrativos en el host.

### Modo de bloqueo estricto

En el modo de bloqueo estricto, nuevo en vSphere 6.0, el servicio de la DCUI se interrumpe. Si se pierde la conexión con vCenter Server y vSphere Web Client deja de estar disponible, el host ESXi deja de estar disponible, a menos que se habiliten los servicios ESXi Shell y SSH, y se definan usuarios con excepción. Si no es posible restaurar la conexión con el sistema vCenter Server, debe volver a instalar el host.

## Modo de bloqueo y servicios ESXi Shell y SSH

El modo de bloqueo estricto interrumpe el servicio de la DCUI. Sin embargo, los servicios ESXi Shell y SSH son independientes del modo de bloqueo. Para que el modo de bloqueo sea una medida de seguridad efectiva, asegúrese de que los servicios ESXi Shell y SSH también estén deshabilitados. Estos servicios están deshabilitados de forma predeterminada.

Cuando un host está en modo de bloqueo, los usuarios que están en la lista de usuarios con excepción pueden acceder a él desde ESXi Shell y a través de SSH si cuentan con la función de administrador en el host. Se puede tener este tipo de acceso incluso en el modo de bloqueo estricto. La opción más segura es dejar los servicios ESXi Shell y SSH deshabilitados.

---

**Nota** La lista de usuarios con excepción no está pensada para administradores, sino para las cuentas de servicio que realizan tareas específicas, como copias de servicio de hosts. Agregar usuarios administradores a la lista de usuarios con excepción va en contra de la finalidad del modo de bloqueo.

---

## Habilitar y deshabilitar el modo de bloqueo

Los usuarios con privilegios pueden habilitar el modo de bloqueo de varias maneras:

- Mediante el asistente **Agregar host** para agregar un host a un sistema vCenter Server.
- Mediante vSphere Web Client. Consulte [Habilitar el modo de bloqueo con vSphere Web Client](#). Puede habilitar el modo de bloqueo normal y el modo de bloqueo estricto desde vSphere Web Client.
- Usar la interfaz de usuario de la consola directa (DCUI). Consulte [Habilitar o deshabilitar el modo normal de bloqueo desde la interfaz de usuario de la consola directa](#).

Los usuarios con privilegios pueden deshabilitar el modo de bloqueo desde vSphere Web Client. Desde la interfaz de usuario de la consola directa, pueden deshabilitar el modo de bloqueo normal, pero no el modo de bloqueo estricto.

---

**Nota** Si habilita o deshabilita el modo de bloqueo mediante la interfaz de usuario de la consola directa, se descartan los permisos para los grupos y los usuarios en el host. Para conservar estos permisos, puede habilitar o deshabilitar el modo de bloqueo mediante vSphere Web Client.

---

## Comportamiento del modo de bloqueo

En el modo de bloqueo, algunos dispositivos se deshabilitan y algunos servicios quedan accesibles solo para ciertos usuarios.

### Servicios de modo de bloqueo para diferentes usuarios

Cuando el host está en ejecución, los servicios disponibles dependen de si el modo de bloqueo está habilitado y del tipo de modo de bloqueo.

- En los modos de bloqueo estricto y normal, los usuarios con privilegios pueden acceder al host mediante vCenter Server, ya sea desde vSphere Web Client o mediante el uso de vSphere Web Services SDK.
- El comportamiento de la interfaz de la consola directa no es igual en el modo de bloqueo estricto que en el modo de bloqueo normal.
  - En el modo de bloqueo estricto, el servicio de interfaz de usuario de la consola directa (DCUI) está deshabilitado.

- En el modo de bloqueo normal, las cuentas de la lista de usuarios con excepción que tienen privilegios de administrador y los usuarios que están especificados en la configuración del sistema avanzado DCUI.Access pueden tener acceso a la interfaz de la consola directa.
- Si ESXi Shell o SSH están habilitados y el host se encuentra en el modo de bloqueo estricto o normal, las cuentas de la lista de usuarios con excepción que tienen privilegios de administrador pueden usar estos servicios. Para los demás usuarios, el acceso a ESXi Shell o SSH queda deshabilitado. A partir de vSphere 6.0, las sesiones de ESXi o SSH se interrumpen para los usuarios que no tienen privilegios de administrador.

Todas las operaciones de acceso se registran para ambos modos de bloqueo, estricto y normal.

**Tabla 5-9. Comportamiento del modo de bloqueo**

Servicio	Modo normal	Modo de bloqueo normal	Modo de bloqueo estricto
vSphere Web Services API	Todos los usuarios, según los permisos	vCenter (vpxuser) Usuarios con excepción, según los permisos vCloud Director (vslauser, si está disponible)	vCenter (vpxuser) Usuarios con excepción, según los permisos vCloud Director (vslauser, si está disponible)
Proveedores de CIM	Usuarios con privilegios de administrador en el host	vCenter (vpxuser) Usuarios con excepción, según los permisos. vCloud Director (vslauser, si está disponible)	vCenter (vpxuser) Excepción, según los permisos. vCloud Director (vslauser, si está disponible)
UI de consola directa (DCUI)	Usuarios con privilegios de administrador en el host y usuarios que se encuentran en la opción avanzada DCUI.Access	Usuarios definidos en la opción avanzada DCUI.Access Usuarios con excepción con privilegios de administrador en el host	El servicio de DCUI se detiene
ESXi Shell (si está habilitado)	Usuarios con privilegios de administrador en el host	Usuarios definidos en la opción avanzada DCUI.Access Usuarios con excepción con privilegios de administrador en el host	Usuarios definidos en la opción avanzada DCUI.Access Usuarios con excepción con privilegios de administrador en el host
SSH (si está habilitado)	Usuarios con privilegios de administrador en el host	Usuarios definidos en la opción avanzada DCUI.Access Usuarios con excepción con privilegios de administrador en el host	Usuarios definidos en la opción avanzada DCUI.Access Usuarios con excepción con privilegios de administrador en el host

## Usuarios con sesión iniciada en ESXi Shell cuando el modo de bloqueo está habilitado

Si los usuarios tienen una sesión iniciada en ESXi Shell o acceden al host mediante SSH antes de que se habilite el modo de bloqueo, los usuarios que estén en la lista de usuarios con excepción y que tengan privilegios de administrador en el host permanecen con la sesión iniciada. Comenzando por vSphere 6.0, la sesión se interrumpe para todos los demás usuarios. Esto se aplica tanto al modo de bloqueo normal como al estricto.

## Habilitar el modo de bloqueo con vSphere Web Client

Habilite el modo de bloqueo para que se requiera que todos los cambios de configuración pasen por vCenter Server. vSphere 6.0 y versiones posteriores admiten el modo de bloqueo normal y el modo de bloqueo estricto.

Para prohibir por completo el acceso directo a un host, se puede seleccionar el modo de bloqueo estricto. El modo de bloqueo estricto permite el acceso a un host si vCenter Server no está disponible y SSH y ESXi Shell están deshabilitados. Consulte [Comportamiento del modo de bloqueo](#).

### Procedimiento

- 1 Desplácese hasta el host en el inventario de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 En Sistema, seleccione **Perfil de seguridad**.
- 4 En el panel Modo de bloqueo, haga clic en **Editar**.
- 5 Haga clic en **Modo de bloqueo** y seleccione una de las opciones del modo de bloqueo.

Opción	Descripción
<b>Normal</b>	Se puede acceder al host desde vCenter Server. Solo los usuarios que están en la lista de usuarios con excepción y tienen privilegios de administrador pueden iniciar sesión en la interfaz de usuario de la consola directa. Si SSH o ESXi Shell están habilitados, es posible que se pueda tener acceso.
<b>Estricto</b>	Se puede acceder al host únicamente desde vCenter Server. Si SSH o ESXi Shell están habilitados, permanecen habilitadas las sesiones en ejecución de las cuentas de la opción avanzada DCUI.Access y las cuentas de usuarios con excepción que tienen privilegios de administrador. Todas las demás sesiones se interrumpen.

- 6 Haga clic en **Aceptar**.

## Deshabilitar el modo de bloqueo mediante vSphere Web Client

Deshabilite el modo de bloqueo para permitir cambios de configuración en las conexiones directas al host ESXi. Si el modo de bloqueo está habilitado, el entorno es más seguro.

En vSphere 6.0, se puede deshabilitar el modo de bloqueo de la siguiente manera:

### Desde vSphere Web Client

Los usuarios pueden deshabilitar el modo de bloqueo normal y el modo de bloque estricto desde vSphere Web Client.

### Desde la interfaz de usuario de la consola directa

Los usuarios que pueden acceder a la interfaz de usuario de la consola directa en el host ESXi pueden deshabilitar el modo de bloqueo normal. En el modo de bloqueo estricto, el servicio de interfaz de la consola directa se detiene.

#### Procedimiento

- 1 Desplácese hasta el host en el inventario de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 En Sistema, seleccione **Perfil de seguridad**.
- 4 En el panel Modo de bloqueo, haga clic en **Editar**.
- 5 Haga clic en **Modo de bloqueo** y seleccione **Ninguno** para deshabilitar el modo de bloqueo.

#### Resultados

El sistema sale del modo de bloqueo, vCenter Server muestra una alarma y se agrega una entrada al registro de auditoría.

### Habilitar o deshabilitar el modo normal de bloqueo desde la interfaz de usuario de la consola directa

Puede habilitar y deshabilitar el modo normal de bloqueo desde la interfaz de usuario de la consola directa (DCUI). El modo estricto de bloqueo puede habilitarse y deshabilitarse únicamente desde vSphere Web Client.

Cuando el host se encuentra en el modo normal de bloqueo, las siguientes cuentas pueden acceder a la interfaz de usuario de la consola directa:

- Cuentas en la lista de usuarios con excepción que tienen privilegios de administrador en el host. La lista de usuarios con excepción sirve para cuentas de servicios, como un agente de copia de seguridad.
- Usuarios definidos en la opción avanzada DCUI.Access del host. Esta opción puede utilizarse para habilitar el acceso en caso de que ocurra un error grave.

En el caso de ESXi 6.0 y versiones posteriores, los permisos de usuarios se conservan al habilitar el modo de bloqueo y se restauran al deshabilitar el modo de bloqueo desde la interfaz de usuario de la consola directa.

---

**Nota** Si actualiza un host que se encuentra en el modo de bloqueo a la versión 6.0 de ESXi sin salir de ese modo, y si sale del modo después de actualizar, se perderán todos los permisos definidos antes de que el host entrara en el modo de bloqueo. El sistema asigna la función de administrador a todos los usuarios que se encuentran en la opción avanzada DCUI.Access para garantizar el acceso al host.

Para conservar los permisos, deshabilite el modo de bloqueo del host desde vSphere Web Client antes de realizar la actualización.

---

#### Procedimiento

- 1 En la interfaz de usuario de la consola directa del host, presione F2 e inicie sesión.
- 2 Desplácese hasta la opción **Configurar el modo de bloqueo** y presione Entrar para alternar la configuración actual.
- 3 Presione Esc hasta que vuelva al menú principal de la interfaz de usuario de la consola directa.

### Especificar cuentas con privilegios de acceso en el modo de bloqueo

Puede especificar cuentas de servicio que puedan acceder al host ESXi. Para ello, agréguelas directamente a la lista de usuarios con excepción. Puede especificar que un único usuario acceda al host ESXi en caso de que ocurra un error grave en vCenter Server.

La versión del entorno de vSphere determina qué pueden hacer de forma predeterminada las diferentes cuentas cuando se habilita el modo de bloqueo y cómo se puede cambiar el comportamiento predeterminado.

- En las versiones de vSphere anteriores a vSphere 5.1, únicamente el usuario raíz puede iniciar sesión en la interfaz de usuario de la consola directa (DCUI) en un host ESXi que se encuentra en el modo de bloqueo.
- En vSphere 5.1 y versiones posteriores, puede agregar un usuario a la configuración avanzada del sistema de DCUI.Access para cada host. La opción está pensada en caso de que ocurra un error grave en vCenter Server. La contraseña del usuario con este acceso generalmente está bloqueada y protegida. Un usuario de la lista DCUI.Access no necesita tener privilegios administrativos completos sobre el host.
- En vSphere 6.0 y las versiones posteriores, la configuración avanzada del sistema de DCUI.Access sigue siendo compatible. Asimismo, vSphere 6.0 y las versiones posteriores admiten una lista de usuarios con excepción, destinada a las cuentas de servicio que deben conectarse al host directamente. Las cuentas con privilegios de administrador que figuran en la lista de usuarios con excepción pueden iniciar sesión en ESXi Shell. Por otra parte, estos usuarios pueden iniciar sesión en la DCUI de un host en el modo de bloqueo normal y pueden salir del modo de bloqueo.



Especifique los usuarios con excepción desde vSphere Web Client.

---

**Nota** Los usuarios con excepción son usuarios locales del host o usuarios de Active Directory con privilegios definidos localmente para el host ESXi. Los usuarios que son miembros de un grupo de Active Directory pierden sus permisos cuando el host se coloca en modo de bloqueo.

---

### Agregar usuarios a la opción avanzada DCUI.Access

La finalidad principal de la opción avanzada DCUI.Access es permitir al usuario salir del modo de bloqueo en caso de que se produzca un error grave, cuando no se puede acceder al host desde vCenter Server. Para agregar usuarios a la lista, edite las opciones de configuración avanzada del host desde vSphere Web Client.

---

**Nota** Los usuarios de la lista de DCUI.Access pueden cambiar la configuración del modo de bloqueo independientemente de los privilegios que tengan. Esto puede influir en la seguridad del host. En el caso de las cuentas de servicio que necesitan acceso directo al host, puede ser conveniente agregar usuarios a la lista de usuarios con excepción. Un usuario con excepción solamente puede realizar tareas para las cuales tiene privilegios. Consulte [Especificar usuarios con excepción para el modo de bloqueo](#).

---

### Procedimiento

- 1 Desplácese hasta el host en el navegador de objetos de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y seleccione **Configuración**.
- 3 Haga clic en **Configuración avanzada del sistema** y seleccione **DCUI.Access**.
- 4 Haga clic en **Editar** e introduzca los nombres de usuario, separados por comas.

Se incluye al usuario raíz de forma predeterminada. Considere quitar la raíz de la lista de DCUI.Access y especifique una cuenta con nombre para mejorar el proceso de auditoría.

- 5 Haga clic en **Aceptar**.

### Especificar usuarios con excepción para el modo de bloqueo

En vSphere 6.0 y versiones posteriores, se pueden agregar usuarios a la lista de usuarios con excepción desde vSphere Web Client. Estos usuarios no pierden sus permisos cuando el host entra en el modo de bloqueo. Por lo tanto, es lógico agregar cuentas de servicio, como un agente de copia de seguridad, a la lista de usuarios con excepción.

Los usuarios con excepción no pierden sus privilegios cuando el host entra en el modo de bloqueo. Es frecuente que estas cuentas representen soluciones y aplicaciones externas que necesitan seguir funcionando en el modo de bloqueo.

---

**Nota** La lista de usuarios con excepción no está pensada para administradores sino para las cuentas de servicio que realizan tareas muy específicas. Agregar usuarios administradores a la lista de usuarios con excepción va en contra de la finalidad del modo de bloqueo.

---

Los usuarios con excepción son usuarios locales del host o usuarios de Active Directory con privilegios definidos localmente para el host ESXi. No son miembros de un grupo de Active Directory y no son usuarios de vCenter Server. Estos usuarios tienen permitido realizar operaciones en el host en función de sus privilegios. Esto significa que, por ejemplo, un usuario con privilegios de solo lectura no puede deshabilitar el modo de bloqueo en un host.

#### Procedimiento

- 1 Desplácese hasta el host en el inventario de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 En Sistema, seleccione **Perfil de seguridad**.
- 4 En el panel Modo de bloqueo, haga clic en **Editar**.
- 5 Haga clic en **Usuarios con excepción** y, a continuación, haga clic en el icono con el símbolo más (+) para agregar usuarios con excepción.

## Comprobar los niveles de aceptación de hosts y VIB

Para conservar la integridad del host ESXi, no permita que los usuarios instalen VIB no firmados (creados por la comunidad). Un VIB no firmado contiene un código no certificado, aceptado ni admitido por VMware o sus partners. Los VIB creados por la comunidad no tienen una firma digital.

Es posible utilizar los comandos ESXCLI para establecer un nivel de aceptación de un host. El nivel de aceptación del host debe ser igual de restrictivo o menos restrictivo que el nivel de aceptación de cualquier VIB que se desee agregar al host. Para proteger la seguridad y la integridad de los hosts ESXi, no permita que se instalen VIB no firmados (CommunitySupported) en los hosts de sistemas de producción.

Los siguientes niveles de aceptación son compatibles.

#### VMwareCertified

El nivel de aceptación VMwareCertified tiene los requisitos más estrictos. Los VIB con este nivel se someten a pruebas completamente equivalentes a las pruebas de control de calidad internas de VMware para la misma tecnología. Hoy en día, solo los controladores IOVP se publican en este nivel. VMware responde a las llamadas de soporte para VIB con este nivel de aceptación.

#### VMwareAccepted

Los VIB con este nivel de aceptación pasan por pruebas de comprobación, pero estas no prueban completamente todas las funciones del software. El partner realiza pruebas y VMware comprueba el resultado. Hoy en día, los proveedores de CIM y los complementos de PSA son algunos de los VIB que se publican en este nivel. VMware dirige las llamadas de soporte para VIB con este nivel de aceptación a la organización de soporte del partner.

#### PartnerSupported

Los VIB con el nivel de aceptación **PartnerSupported** los publica un partner de confianza de VMware. El partner realiza todas las pruebas. VMware no comprueba los resultados. Este nivel se utiliza para una tecnología nueva o alternativa que los partners desean habilitar para los sistemas VMware. Hoy en día, las tecnologías de VIB de controlador, como Infiniband, ATAoE y SSD, se encuentran en este nivel con controladores de hardware que no son estándar. VMware dirige las llamadas de soporte para VIB con este nivel de aceptación a la organización de soporte del partner.

### CommunitySupported

El nivel de aceptación **CommunitySupported** es para VIB creados por personas o empresas por fuera de los programas de partners de VMware. Los VIB de este nivel de aceptación no pasaron por un programa de pruebas aprobado por VMware y no son compatibles con el soporte técnico de VMware ni los partners de VMware.

#### Procedimiento

- 1 Conéctese a cada host ESXi y compruebe que el nivel de aceptación esté establecido en **VMwareCertified** o **VMwareAccepted** mediante el siguiente comando.

```
esxcli software acceptance get
```

- 2 Si el nivel de aceptación del host no es **VMwareCertified** o **VMwareAccepted**, ejecute los siguientes comandos para determinar si alguno de los VIB no está en el nivel **VMwareCertified** o **VMwareAccepted**.

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

- 3 Quite los VIB que estén en los niveles **PartnerSupported** o **CommunitySupported** mediante el siguiente comando.

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

- 4 Cambie el nivel de aceptación del host mediante el siguiente comando.

```
esxcli software acceptance set --level acceptance_level
```

## Asignar permisos para ESXi

En la mayoría de los casos, se le otorgan privilegios a los usuarios asignándoles permisos para los objetos de los hosts ESXi que administra un sistema vCenter Server. Si se utiliza un host ESXi independiente, se pueden asignar los privilegios directamente.

### Asignar permisos para hosts ESXi administrados por vCenter Server

Si el host ESXi está administrado por vCenter Server, realice las tareas de administración a través de vSphere Web Client.

Puede seleccionar el objeto de host ESXi en la jerarquía de objetos de vCenter Server y asignar la función de administrador a una cantidad limitada de usuarios que podrían realizar la administración directa en el host ESXi. Consulte [Usar funciones para asignar privilegios](#).

La práctica recomendada implica crear al menos una cuenta de usuario designado, asignarle privilegios administrativos completos en el host y utilizar esta cuenta en lugar de la cuenta raíz. Establezca una contraseña de alta complejidad para la cuenta raíz y limite la utilización de la cuenta raíz. (No quite la cuenta raíz).

## Asignar permisos para hosts independientes de ESXi

Si el entorno no incluye un sistema vCenter Server, están predefinidos los siguientes usuarios.

- usuario raíz. Consulte [Privilegios de usuario raíz](#).
- usuario vpxuser. Consulte [Privilegios del usuario vpxuser](#).
- usuario dcui. Consulte [Privilegios de usuario dcui](#).

Se pueden agregar usuarios locales y definir roles personalizados desde la pestaña Administración de vSphere Client.

Para todas las versiones de ESXi, puede ver la lista de usuarios predefinidos en el archivo `/etc/passwd`.

Las siguientes funciones están predefinidas:

### Solo lectura

Permite que un usuario vea los objetos asociados con el host ESXi, pero no le permite realizar cambios en los objetos.

### Administrador

Función de administrador.

### Sin acceso

Sin acceso. Esta es la opción predeterminada. Es posible anular el valor predeterminado según corresponda.

Se pueden administrar grupos y usuarios locales, y agregar roles locales personalizados a un host ESXi mediante una instancia de vSphere Client conectada directamente al host ESXi.

A partir de vSphere 6.0, es posible utilizar los comandos ESXCLI para la administración de cuentas de usuarios locales de ESXi. Los comandos ESXCLI de administración de permisos se pueden utilizar para configurar o quitar permisos tanto en cuentas de Active Directory (usuarios y grupos) como en cuentas locales de ESXi (usuarios únicamente).

---

**Nota** Si se define un usuario para el host ESXi mediante una conexión directa al host, y existe un usuario con el mismo nombre en vCenter Server, los usuarios son diferentes. Si se asigna una función a uno de los usuarios, al otro usuario no se le asigna la misma función.

---

## Privilegios de usuario raíz

Cada host ESXi tiene, de manera predeterminada, una sola cuenta de usuario raíz con la función de administrador. Esa cuenta de usuario raíz puede utilizarse para la administración local y para conectar el host a vCenter Server.

Esta cuenta raíz común puede facilitar la intromisión en un host ESXi y hacer que resulte más difícil relacionar un administrador específico con determinadas acciones.

Establezca una contraseña de complejidad alta para la cuenta raíz y limite el uso de la cuenta, por ejemplo, para utilizar en el momento de agregar un host a vCenter Server. No elimine la cuenta raíz. En vSphere 5.1 y versiones posteriores, únicamente el usuario raíz y ningún otro usuario designado con la función de administrador tiene permiso para agregar un host a vCenter Server.

La práctica recomendada es que todas las cuentas con la función de administrador en un host ESXi se asignen a un usuario específico que tenga una cuenta con nombre. Utilice las funcionalidades de ESXi Active Directory, que permiten administrar las credenciales de Active Directory cuando es posible.

---

**Importante** Si elimina los privilegios de acceso del usuario raíz, primero debe crear otro permiso en el nivel de raíz que tenga un usuario distinto asignado a la función de administrador.

---

## Privilegios del usuario vpxuser

vCenter Server utiliza los privilegios del usuario vpxuser cuando se administran actividades del host.

vCenter Server tiene privilegios de administrador para el host que administra. Por ejemplo, vCenter Server puede mover máquinas virtuales desde y hacia los hosts, y realizar cambios en la configuración necesarios para admitir a las máquinas virtuales.

El administrador de vCenter Server puede realizar casi todas las mismas tareas en el host que el usuario raíz y, también, programar tareas, trabajar con plantillas, etc. Sin embargo, el administrador de vCenter Server no puede crear, eliminar o editar usuarios y grupos locales para los hosts de forma directa. Estas tareas solo puede realizarlas un usuario con permisos de administrador directamente en cada host.

---

**Nota** No se puede administrar el usuario vpxuser mediante Active Directory.

---

**Precaución** No modifique el usuario vpxuser de ninguna manera. No cambie su contraseña. No cambie sus permisos. Si lo hace, podría experimentar problemas al trabajar con los hosts a través de vCenter Server.

---

## Privilegios de usuario dcui

El usuario dcui se ejecuta en hosts y actúa con derechos de administrador. El fin principal de este usuario es configurar los hosts para el modo de bloqueo desde la interfaz de usuario de la consola directa (DCUI).

Este usuario actúa como agente para la consola directa, y los usuarios interactivos no pueden modificarlo ni usarlo.

## Usar Active Directory para administrar usuarios de ESXi

Se puede configurar ESXi para utilizar un servicio de directorio como Active Directory con el fin de administrar usuarios.

La creación de cuentas de usuarios locales en cada host presenta desafíos para la sincronización de los nombres y las contraseñas de las cuentas en varios hosts. Conecte los hosts ESXi a un dominio de Active Directory para que no sea necesario crear y mantener cuentas de usuarios locales. La utilización de Active Directory para autenticar usuarios simplifica la configuración del host ESXi y reduce el riesgo de que ocurran problemas de configuración que podrían permitir un acceso no autorizado.

Al utilizar Active Directory, los usuarios suministran sus credenciales de Active Directory y el nombre de dominio del servidor de Active Directory cuando se agrega un host a un dominio.

## Instalar o actualizar vSphere Authentication Proxy

Instale vSphere Authentication Proxy para permitir que los hosts ESXi se unan a un dominio sin utilizar credenciales de Active Directory. vSphere Authentication Proxy mejora la seguridad para hosts con arranque PXE y hosts que se aprovisionan con Auto Deploy mediante la eliminación de la necesidad de almacenar credenciales de Active Directory en la configuración del host.

Si hay una versión anterior de vSphere Authentication Proxy instalada en el sistema, este procedimiento actualiza vSphere Authentication Proxy a la versión actual.

Puede instalar vSphere Authentication Proxy en la misma máquina que la instancia de vCenter Server asociada o en una máquina diferente que tenga conexión de red con vCenter Server. vSphere Authentication Proxy es compatible con vCenter Server versiones 5.0 y posteriores.

El servicio de vSphere Authentication Proxy se enlaza a una dirección IPv4 para comunicarse con vCenter Server y no admite IPv6. La instancia de vCenter Server puede ser un equipo host en un entorno de red solo de IPv4, de modo mixto IPv4/IPv6 o solo de IPv6, pero la máquina que se conecta a vCenter Server a través de vSphere Web Client debe tener una dirección IPv4 para que el servicio de vSphere Authentication Proxy funcione.

### Requisitos previos

- Instale Microsoft .NET Framework 3.5 en la máquina donde desea instalar vSphere Authentication Proxy.
- Compruebe que dispone de privilegios de administrador.
- Compruebe que el equipo host tenga un procesador y sistema operativo compatibles.

- Compruebe que el equipo host tenga una dirección IPv4 válida. Puede instalar vSphere Authentication Proxy en una máquina en un entorno de red solo de IPv4 o de modo mixto IPv4/IPv6, pero no puede instalar vSphere Authentication Proxy en una máquina en un entorno solo de IPv6.
- Si va a instalar vSphere Authentication Proxy en un equipo host Windows Server 2008 R2, descargue e instale el hotfix de Windows que se describe en el artículo 981506 de la base de conocimientos de Windows en el sitio web support.microsoft.com. Si este hotfix no está instalado, el adaptador de vSphere Authentication Proxy no se inicializa. Este problema viene acompañado de mensajes de error en `camadapter.log` de forma similar a `Failed to bind CAM website with CTL` y `Failed to initialize CAMAdapter..`
- Descargue el instalador de vCenter Server.

Recopile la siguiente información para completar la instalación o actualización:

- La ubicación para instalar vSphere Authentication Proxy, en caso de que no use la ubicación predeterminada.
- La dirección y las credenciales para la instancia de vCenter Server a la que se conectará vSphere Authentication Proxy: dirección IP o nombre, puerto HTTP, nombre de usuario y contraseña.
- Nombre de host o dirección IP para identificar vSphere Authentication Proxy en la red.

#### Procedimiento

- 1 Agregue el equipo host en el que instalará el servicio de proxy de autenticación al dominio.
- 2 Utilice la cuenta del administrador del dominio para iniciar sesión en el equipo host.
- 3 En el directorio del instalador del software, haga doble clic en el archivo `autorun.exe` para iniciar el instalador.
- 4 Seleccione **VMware vSphere Authentication Proxy** y haga clic en **Instalar**.
- 5 Siga las indicaciones del asistente para realizar la instalación o actualización.

Durante la instalación, el servicio de autenticación se registra en la instancia de vCenter Server donde se registra Auto Deploy.

#### Resultados

Cuando se instala el servicio de vSphere Authentication Proxy, el instalador crea una cuenta de dominio con los privilegios correspondientes para ejecutar el servicio de proxy de autenticación. El nombre de cuenta comienza con el prefijo `CAM-` y se asocia con una contraseña de 32 caracteres generada de forma aleatoria. La contraseña está configurada para nunca caducar. No cambie la configuración de la cuenta.

## Configurar un host para utilizar Active Directory

Si desea administrar usuarios y grupos, puede configurar un host para el uso de un servicio de directorio como Active Directory.

Cuando agrega un host ESXi en Active Directory, el grupo DOMAIN **ESX Admins** recibe acceso administrativo completo al host si este existe. Si no desea que haya disponible un acceso administrativo completo, consulte el artículo 1025569 de la base de conocimientos de VMware para encontrar una solución alternativa.

Si se aprovisiona un host con Auto Deploy, las credenciales de Active Directory no pueden almacenarse en los hosts. Puede usar vSphere Authentication Proxy para unir el host a un dominio de Active Directory. Dado que existe una cadena de confianza entre vSphere Authentication Proxy y el host, Authentication Proxy puede unir el host al dominio de Active Directory. Consulte [Usar vSphere Authentication Proxy](#).

---

**Nota** Al momento de definir la configuración de la cuenta de usuario en Active Directory, es posible definir un límite para los equipos en los que un usuario puede iniciar sesión por el nombre de equipo. De forma predeterminada, no se establecen restricciones similares en una cuenta de usuario. Si se establece dicho límite, las solicitudes de enlaces LDAP de la cuenta de usuario generan errores y muestran el mensaje `Error en el enlace LDAP`, incluso si la solicitud proviene de un equipo que figura en la lista. Para evitar este problema, agregue el nombre netBIOS en el servidor de Active Directory a la lista de equipos en los cuales se puede iniciar sesión con la cuenta de usuario.

---

#### Requisitos previos

- Compruebe que tenga un dominio de Active Directory. Consulte la documentación del servidor del directorio.
- Compruebe que el nombre de host ESXi esté completo con el nombre de dominio del bosque de Active Directory.

*fully qualified domain name = host\_name.domain\_name*

#### Procedimiento

- 1 Sincronice el tiempo entre ESXi y el sistema de servicio del directorio que utiliza NTP.  
Consulte [Sincronización de los relojes de ESXi con un servidor horario de red](#) o la base de conocimientos de VMware para obtener información sobre cómo sincronizar la hora de ESXi con una controladora de dominio de Microsoft.
- 2 Asegúrese de que los servidores DNS que configuró en el host puedan resolver los nombres de host en las controladoras de Active Directory.
  - a Desplácese hasta el host en el navegador de objetos de vSphere Web Client.
  - b Haga clic en la pestaña **Administrar** y en **Redes**.
  - c Haga clic en DNS y verifique que el nombre de host y la información del servidor DNS correspondiente al host sean correctos.



### Pasos siguientes

Use vSphere Web Client para unirse a un dominio de servicio de directorio. En los hosts que se aprovisionan con Auto Deploy, configure vSphere Authentication Proxy. Consulte [Usar vSphere Authentication Proxy](#).

## Agregar un host a un dominio de servicio de directorio

Para que el host utilice un servicio de directorio, se debe conectar el host al dominio del servicio de directorio.

Es posible introducir el nombre de dominio con uno de los dos métodos siguientes:

- **name.tld** (por ejemplo, **domain.com**): la cuenta se crea en el contenedor predeterminado.
- **name.tld/container/path** (por ejemplo, **domain.com/OU1/OU2**): la cuenta se crea en una unidad organizativa (OU) en particular.

Para utilizar el servicio vSphere Authentication Proxy, consulte [Usar vSphere Authentication Proxy](#).

### Procedimiento

- 1 Desplácese hasta el host en el inventario de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 En Sistema, seleccione **Servicios de autenticación**.
- 4 Haga clic en **Unir dominio**.
- 5 Introduzca un dominio.  
Utilice el formulario **name.tld** o **name.tld/container/path**.
- 6 Introduzca el nombre de usuario y la contraseña de un usuario de servicio de directorio que tenga permisos para unir el host al dominio y, a continuación, haga clic en **Aceptar**.
- 7 (opcional) Si desea utilizar un proxy de autenticación, introduzca la dirección IP del servidor proxy.
- 8 Haga clic en **Aceptar** para cerrar el cuadro de diálogo Configuración de servicios de directorio.

## Ver la configuración del servicio de directorio

Puede ver el tipo de servidor de directorio (si lo hubiera) que utiliza el host para autenticar usuarios y su respectiva configuración.

### Procedimiento

- 1 Desplácese hasta el host en el inventario de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.

### 3 En Sistema, seleccione **Servicios de autenticación**.

En la página Servicios de autenticación se muestra el servicio del directorio y la configuración del dominio.

## Usar vSphere Authentication Proxy

Al utilizar vSphere Authentication Proxy, no es necesario transmitir las credenciales de Active Directory al host. Los usuarios suministran el nombre de dominio del servidor de Active Directory y la dirección IP del servidor proxy de autenticación cuando agregan un usuario a un dominio.

vSphere Authentication Proxy resulta muy útil cuando se lo utiliza junto con Auto Deploy. Se configura un host de referencia que apunta a Authentication Proxy y se configura una regla que aplica el perfil del host de referencia a cualquier host ESXi aprovisionado con Auto Deploy. Incluso cuando se utiliza vSphere Authentication Proxy en un entorno con certificados aprovisionados por VMCA o certificados de terceros, el proceso funciona sin problemas mientras se sigan las instrucciones para utilizar certificados personalizados con Auto Deploy. Consulte [Usar certificados personalizados con Auto Deploy](#).

---

**Nota** No se puede utilizar vSphere Authentication Proxy en un entorno compatible solo con IPv6.

---

## Instalar o actualizar vSphere Authentication Proxy

Instale vSphere Authentication Proxy para permitir que los hosts ESXi se unan a un dominio sin utilizar credenciales de Active Directory. vSphere Authentication Proxy mejora la seguridad para hosts con arranque PXE y hosts que se aprovisionan con Auto Deploy mediante la eliminación de la necesidad de almacenar credenciales de Active Directory en la configuración del host.

Si hay una versión anterior de vSphere Authentication Proxy instalada en el sistema, este procedimiento actualiza vSphere Authentication Proxy a la versión actual.

Puede instalar vSphere Authentication Proxy en la misma máquina que la instancia de vCenter Server asociada o en una máquina diferente que tenga conexión de red con vCenter Server. vSphere Authentication Proxy es compatible con vCenter Server versiones 5.0 y posteriores.

El servicio de vSphere Authentication Proxy se enlaza a una dirección IPv4 para comunicarse con vCenter Server y no admite IPv6. La instancia de vCenter Server puede ser un equipo host en un entorno de red solo de IPv4, de modo mixto IPv4/IPv6 o solo de IPv6, pero la máquina que se conecta a vCenter Server a través de vSphere Web Client debe tener una dirección IPv4 para que el servicio de vSphere Authentication Proxy funcione.

### Requisitos previos

- Instale Microsoft .NET Framework 3.5 en la máquina donde desea instalar vSphere Authentication Proxy.
- Compruebe que dispone de privilegios de administrador.
- Compruebe que el equipo host tenga un procesador y sistema operativo compatibles.

- Compruebe que el equipo host tenga una dirección IPv4 válida. Puede instalar vSphere Authentication Proxy en una máquina en un entorno de red solo de IPv4 o de modo mixto IPv4/IPv6, pero no puede instalar vSphere Authentication Proxy en una máquina en un entorno solo de IPv6.
- Si va a instalar vSphere Authentication Proxy en un equipo host Windows Server 2008 R2, descargue e instale el hotfix de Windows que se describe en el artículo 981506 de la base de conocimientos de Windows en el sitio web support.microsoft.com. Si este hotfix no está instalado, el adaptador de vSphere Authentication Proxy no se inicializa. Este problema viene acompañado de mensajes de error en `camadapter.log` de forma similar a `Failed to bind CAM website with CTL` y `Failed to initialize CAMAdapter..`
- Descargue el instalador de vCenter Server.

Recopile la siguiente información para completar la instalación o actualización:

- La ubicación para instalar vSphere Authentication Proxy, en caso de que no use la ubicación predeterminada.
- La dirección y las credenciales para la instancia de vCenter Server a la que se conectará vSphere Authentication Proxy: dirección IP o nombre, puerto HTTP, nombre de usuario y contraseña.
- Nombre de host o dirección IP para identificar vSphere Authentication Proxy en la red.

#### Procedimiento

- 1 Agregue el equipo host en el que instalará el servicio de proxy de autenticación al dominio.
- 2 Utilice la cuenta del administrador del dominio para iniciar sesión en el equipo host.
- 3 En el directorio del instalador del software, haga doble clic en el archivo `autorun.exe` para iniciar el instalador.
- 4 Seleccione **VMware vSphere Authentication Proxy** y haga clic en **Instalar**.
- 5 Siga las indicaciones del asistente para realizar la instalación o actualización.

Durante la instalación, el servicio de autenticación se registra en la instancia de vCenter Server donde se registra Auto Deploy.

#### Resultados

Cuando se instala el servicio de vSphere Authentication Proxy, el instalador crea una cuenta de dominio con los privilegios correspondientes para ejecutar el servicio de proxy de autenticación. El nombre de cuenta comienza con el prefijo `CAM-` y se asocia con una contraseña de 32 caracteres generada de forma aleatoria. La contraseña está configurada para nunca caducar. No cambie la configuración de la cuenta.

## Configurar un host para que utilice vSphere Authentication Proxy para autenticar

Después de instalar el servicio vSphere Authentication Proxy (servicio CAM), debe configurar el host para que utilice el servidor del proxy de autenticación para autenticar a los usuarios.

### Requisitos previos

Instale el servicio vSphere Authentication Proxy (servicio CAM) en un host. Consulte [Instalar o actualizar vSphere Authentication Proxy](#).

### Procedimiento

- 1 Utilice el administrador de IIS en el host para configurar el rango de DHCP.

La configuración del rango permite que los hosts que utilizan DHCP en la red de administración puedan utilizar el servicio de proxy de autenticación.

Opción	Acción
Para IIS 6	<ol style="list-style-type: none"><li>a Desplácese hasta <b>Sitio web de administración de cuentas del equipo</b>.</li><li>b Haga clic con el botón derecho en el directorio virtual <b>CAM ISAPI</b>.</li><li>c Seleccione <b>Propiedades &gt; Seguridad del directorio &gt; Editar restricciones para la dirección IP y el nombre de dominio &gt; Agregar grupo de equipos</b>.</li></ol>
Para IIS 7	<ol style="list-style-type: none"><li>a Desplácese hasta <b>Sitio web de administración de cuentas del equipo</b>.</li><li>b Haga clic en el directorio virtual <b>CAM ISAPI</b> ubicado en el panel izquierdo y abra <b>Restricciones para la dirección IPv4 y el nombre de dominio</b>.</li><li>c Seleccione <b>Agregar entrada de permiso &gt; Rango de direcciones IPv4</b>.</li></ol>

- 2 Si un host no es aprovisionado por Auto Deploy, cambie el certificado SSL predeterminado por un certificado autofirmado o por un certificado firmado por una entidad de certificación (CA) comercial.

Opción	Descripción
<b>Certificado de VMCA</b>	<p>Si va a utilizar los certificados firmados por VMCA predeterminados, debe asegurarse de que el host del proxy de autenticación confíe en el certificado de VMCA.</p> <ol style="list-style-type: none"> <li>Agregue manualmente el certificado de VMCA al almacén de certificados de entidades de certificación raíz de confianza.</li> <li>Agregue el certificado firmado por VMCA (<code>root.cer</code>) al almacén de certificados de confianza local del sistema en el que está instalado el servicio de proxy de autenticación. Puede encontrar el archivo en <code>C:\ProgramData\VMware\CIS\data\vmca</code>.</li> <li>Reinicie el servicio de vSphere Authentication Proxy.</li> </ol>
<b>Certificado firmado por CA de terceros</b>	<p>Agregue el certificado firmado por la entidad de certificación (codificado con DER) al almacén de certificados de confianza local del sistema en el que está instalado el servicio de proxy de autenticación y, a continuación, reinicie el servicio de vSphere Authentication Proxy.</p> <ul style="list-style-type: none"> <li>■ En Windows 2003, copie el archivo del certificado en <code>C:\Documents and Settings\All Users\Application Data\VMware\vsphere Authentication Proxy\trust</code>.</li> <li>■ En Windows 2008, copie el archivo del certificado en <code>C:\Program Data\VMware\vsphere Authentication Proxy\trust</code>.</li> </ul>

## Configurar vSphere Authentication Proxy

Los hosts ESXi pueden utilizar vSphere Authentication Proxy si tienen la información de certificado de Authentication Proxy.

Solo se debe autenticar el servidor una única vez.

**Nota** ESXi y el servidor Authentication Proxy deben poder autenticarse. Asegúrese de que esta funcionalidad de autenticación esté habilitada en todo momento. Si se debe deshabilitar la autenticación, se puede utilizar el cuadro de diálogo Configuración avanzada para establecer el valor del atributo `UserVars.ActiveDirectoryVerifyCAMCertificate` en 0.

## Exportar certificados de vSphere Authentication Proxy

Para autenticar vSphere Authentication Proxy en ESXi, se debe aprovisionar a ESXi con el certificado de servidor proxy.

### Requisitos previos

Instale el servicio de vSphere Authentication Proxy (servicio CAM) en un host. Consulte [Instalar o actualizar vSphere Authentication Proxy](#).

## Procedimiento

- 1 En el sistema del servidor proxy de autenticación, utilice el administrador de IIS para exportar el certificado.

Opción	Acción
Para IIS 6	<ol style="list-style-type: none"> <li>a Haga clic con el botón derecho en <b>Sitio web de administración de cuentas de equipos</b>.</li> <li>b Seleccione <b>Propiedades &gt; Seguridad del directorio &gt; Ver certificado</b>.</li> </ol>
Para IIS 7	<ol style="list-style-type: none"> <li>a Haga clic en <b>Sitio web de administración de cuentas de equipos</b> en el panel izquierdo.</li> <li>b Seleccione <b>Enlaces</b> para abrir el cuadro de diálogo Enlaces de sitios.</li> <li>c Seleccione el enlace <b>https</b>.</li> <li>d Seleccione <b>Editar &gt; Ver certificado SSL</b>.</li> </ol>

- 2 Seleccione **Detalles > Copiar en archivo**.
- 3 Seleccione las opciones **No exportar la clave privada** y **X.509 codificado base 64 (CER)**.

## Pasos siguientes

Importe el certificado a ESXi.

## Importar un certificado de servidor proxy en ESXi

Para autenticar el servidor vSphere Authentication Proxy en ESXi, cargue el certificado de servidor proxy en ESXi.

Puede usar la interfaz de usuario de vSphere Web Client para cargar el certificado del servidor vSphere Authentication Proxy en ESXi.

## Requisitos previos

Instale el servicio vSphere Authentication Proxy (servicio CAM) en un host. Consulte [Instalar o actualizar vSphere Authentication Proxy](#).

Explore el certificado del servidor de vSphere Authentication Proxy, tal como se describe en [Exportar certificados de vSphere Authentication Proxy](#).

## Procedimiento

- 1 Desplácese hasta el host, haga clic en la pestaña **Administrar**, haga clic en **Configuración** y, a continuación, haga clic en **Servicios de autenticación**.
- 2 Haga clic en **Importar certificado**.
- 3 Introduzca la ruta completa del archivo de certificado de servidor proxy de autenticación en el host y la dirección IP del servidor proxy de autenticación.  
  
Utilice el formulario `[datastore name] file path` para introducir la ruta de acceso al servidor proxy.
- 4 Haga clic en **Aceptar**.

## Usar vSphere Authentication Proxy para agregar un host a un dominio

Al asociar un host al dominio de un servicio de directorio, se puede utilizar el servidor vSphere Authentication Proxy para la autenticación en lugar de transmitir credenciales de Active Directory suministradas por el usuario.

Es posible introducir el nombre de dominio con uno de los dos métodos siguientes:

- **name.tld** (por ejemplo, **domain.com**): la cuenta se crea en el contenedor predeterminado.
- **name.tld/container/path** (por ejemplo, **domain.com/OU1/OU2**): la cuenta se crea en una unidad organizativa (OU) en particular.

### Requisitos previos

- Conéctese a un sistema vCenter Server con vSphere Web Client.
- Si ESXi está configurado con una dirección de DHCP, configure el intervalo de DHCP.
- Si ESXi está configurado con una dirección IP estática, compruebe que su perfil asociado esté configurado para utilizar el servicio de vSphere Authentication Proxy para unir un dominio, a fin de que el servidor proxy de autenticación pueda confiar en la dirección IP de ESXi.
- Si ESXi está utilizando un certificado firmado por VMCA, compruebe que el host se haya agregado a vCenter Server. Esto permite al servidor proxy de autenticación confiar en ESXi.
- Si ESXi usa un certificado firmado por CA y no cuenta con aprovisionamiento de Auto Deploy, compruebe que el certificado de CA se haya agregado al almacén de certificados de confianza local del servidor proxy de autenticación, tal como se describe en [Configurar un host para que utilice vSphere Authentication Proxy para autenticar](#).
- Autentique el servidor vSphere Authentication Proxy en el host.

### Procedimiento

- 1 Desplácese hasta el host en vSphere Web Client y haga clic en la pestaña **Administrar**.
- 2 Haga clic en **Configuración** y seleccione **Servicios de autenticación**.
- 3 Haga clic en **Unir dominio**.
- 4 Introduzca un dominio.  
Utilice el formulario **name.tld** o **name.tld/container/path**.
- 5 Seleccione **Utilizar servidor proxy**.
- 6 Introduzca la dirección IP del servidor proxy de autenticación.
- 7 Haga clic en **Aceptar**.

## Reemplazar el certificado del proxy de autenticación en el host ESXi

Puede importar un certificado desde una entidad de certificación de confianza en vSphere Web Client

#### Requisitos previos

- Cargue el archivo de certificado del proxy de autenticación en el host ESXi.

#### Procedimiento

- 1 En vSphere Web Client, seleccione el host ESXi.
- 2 En la pestaña **Configuración**, seleccione **Servicios de autenticación** en el área **Sistema**.
- 3 Haga clic en **Importar certificado**.
- 4 Introduzca la ruta de acceso del certificado SSL y el servidor vSphere Authentication Proxy.

## Prácticas recomendadas de seguridad de ESXi

Siga las prácticas recomendadas de seguridad de ESXi para garantizar la integridad de la implementación de vSphere. Para obtener información adicional, consulte la *Guía de fortalecimiento*.

#### Comprobación de los medios de instalación

Revise siempre el hash del archivo después de descargar una ISO, un paquete sin conexión o una revisión para garantizar la integridad y la autenticidad de los archivos descargados. Si obtiene los soportes físicos desde VMware y el sello de seguridad está roto, devuelva el software a VMware para su reemplazo.

Después de descargar los elementos multimedia, utilice el valor de suma MD5 para comprobar la integridad de la descarga. Compare el resultado de la suma de MD5 con el valor publicado en el sitio web de VMware. Cada sistema operativo usa un método y herramientas distintos para comprobar los valores de suma de MD5. En Linux, utilice el comando "md5sum". En Microsoft Windows, puede descargar un producto complementario.

#### Revisión manual de CRL

De manera predeterminada, un host ESXi no admite la comprobación de las listas de revocación de certificados (CRL). Los certificados revocados se deben buscar y quitar manualmente. Generalmente, se trata de certificados generados en forma personalizada de una entidad de certificación corporativa o una entidad de certificación externa. Muchas empresas usan scripts para buscar y reemplazar los certificados SSL revocados en hosts ESXi.

#### Supervisión del grupo ESX Admins en Active Directory

El grupo de Active Directory que utiliza vSphere está definido en la configuración avanzada del sistema `plugins.hostsvc.esxAdminsGroup`. La opción predeterminada es ESX Admins. Todos los miembros del grupo ESX Admins tienen acceso administrativo completo sobre todos los hosts ESXi del dominio. Supervise Active Directory para la creación de este grupo y limite la pertenencia a los usuarios y los grupos de mucha confianza.



## Supervisión de archivos de configuración

Si bien la mayoría de los valores de configuración de ESXi se controlan mediante una API, una cantidad limitada de archivos de configuración afectan al host directamente. Estos archivos quedan expuestos a través de la API de transferencia de archivos de vSphere, que utiliza el protocolo HTTPS. Si se hacen cambios en estos archivos, también se debe realizar la acción administrativa correspondiente, como efectuar un cambio de configuración.

---

**Nota** No intente supervisar los archivos que NO están expuestos mediante esta API de transferencia archivos.

---

## Utilización de vmkfstools para borrar datos confidenciales

Cuando elimine un archivo de VMDK con datos confidenciales, apague o detenga la máquina virtual y, a continuación, ejecute el comando de vCLI `vmkfstools --writezeros` en ese archivo. Posteriormente, puede eliminar el archivo del almacén de datos.

## Dispositivos PCI/PCIe y ESXi

El uso de VMware DirectPath I/O para establecer el acceso directo de un dispositivo PCI o PCIe a una máquina virtual representa una vulnerabilidad potencial de la seguridad. Esta vulnerabilidad se puede activar debido un código malintencionado o defectuoso, como un controlador de dispositivo, que se ejecute en modo privilegiado en el sistema operativo invitado. Actualmente, el hardware y el firmware estándar del sector no incluyen soporte de contención de errores suficiente como para que ESXi pueda anular por completo esta vulnerabilidad.

VMware recomienda utilizar el acceso directo de PCI o PCIe a una máquina virtual únicamente si una entidad de confianza es la propietaria y la administradora de la máquina virtual. Es necesario tener la certeza de que esta entidad no intentará bloquear o aprovechar el host de la máquina virtual.

Es posible que el host quede comprometido de una de las siguientes maneras.

- El sistema operativo invitado puede generar un error de PCI o PCIe irreparable. Un error de ese tipo no daña los datos, pero puede bloquear el host ESXi. Esos errores pueden ser el resultado de fallas o incompatibilidades en los dispositivos de hardware en los que se establece el acceso directo, o bien problemas con los controladores en el sistema operativo invitado.
- El sistema operativo invitado puede generar una operación de acceso directo a memoria (DMA) por la cual se puede producir un error en la página de IOMMU en el host ESXi, por ejemplo, cuando la operación de DMA se dirige a una dirección fuera de la memoria de la máquina virtual. En algunas máquinas, el firmware del host configura los errores de IOMMU de modo que se notifique un error irreparable a través de una interrupción no enmascarable (NMI), por la cual el host ESXi se bloquea. La causa de esto pueden ser problemas con los controladores en el sistema operativo invitado.
- Si el sistema operativo en el host ESXi no utiliza la reasignación de interrupciones, es posible que el sistema operativo invitado inyecte una interrupción falsa en el host ESXi en cualquier

vector. Actualmente, ESXi utiliza la reasignación de interrupciones en las plataformas Intel donde se encuentra disponible; la asignación de interrupciones forma parte del conjunto de características de Intel VT-d. ESXi no utiliza la asignación de interrupciones en las plataformas AMD. Lo más probable es que una interrupción falsa bloquee el host ESXi; no obstante, en teoría, es posible que existan otras maneras de aprovechar estas interrupciones.

## Configurar la autenticación de tarjeta inteligente de ESXi

Se puede utilizar la autenticación de tarjeta inteligente para iniciar sesión en la interfaz de usuario de la consola directa (DCUI) de ESXi mediante la comprobación de identidad personal (PIV), la tarjeta de acceso común (CAC) o la tarjeta inteligente SC650, en lugar de la solicitud predeterminada de nombre de usuario y contraseña.

Una tarjeta inteligente es una tarjeta plástica pequeña con un chip de circuito integrado. Muchas agencias gubernamentales y empresas grandes utilizan la autenticación en dos fases basada en tarjeta inteligente para incrementar la seguridad de los sistemas y cumplir con las normas de seguridad.

Cuando se habilita la autenticación de tarjeta inteligente en un host ESXi, la DCUI solicita una combinación válida de tarjeta inteligente y PIN, en lugar de la solicitud predeterminada de nombre de usuario y contraseña.

- 1 Cuando se introduce la tarjeta inteligente en el lector de tarjetas inteligentes, el host ESXi lee las credenciales de la tarjeta.
- 2 La DCUI de ESXi muestra el identificador de inicio de sesión y solicita un PIN.
- 3 Una vez introducido el PIN, el host ESXi busca coincidencias con el PIN almacenado en la tarjeta inteligente y comprueba el certificado en la tarjeta inteligente con Active Directory.
- 4 Después de una comprobación exitosa del certificado de la tarjeta inteligente, ESXi inicia sesión en la DCUI.

Para pasar a la autenticación mediante nombre de usuario y contraseña desde la DCUI, presione F3.

El chip de la tarjeta inteligente se bloquea después de una serie de ingresos de PIN incorrecto; por lo general, después de tres intentos. Si se bloquea la tarjeta inteligente, únicamente el personal designado puede desbloquearla.

## Habilitar la autenticación de tarjeta inteligente

Habilite la autenticación de tarjeta inteligente para que el sistema solicite la combinación de tarjeta inteligente y PIN para iniciar sesión en la DCUI de ESXi.

### Requisitos previos

- Configure la infraestructura para que controle la autenticación de tarjeta inteligente, como cuentas del dominio de Active Directory, lectores de tarjetas inteligentes y tarjetas inteligentes.

- Configure ESXi para que se una a un dominio de Active Directory que admita la autenticación de tarjeta inteligente. Para obtener más información, consulte [Usar Active Directory para administrar usuarios de ESXi](#).
- Utilice vSphere Web Client para agregar certificados raíz. Consulte [Administrar certificados para hosts ESXi](#).

#### Procedimiento

- 1 En vSphere Web Client, desplácese hasta el host.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 En Sistema, seleccione **Servicios de autenticación**.  
Puede ver el estado actual de autenticación de tarjeta inteligente y una lista con los certificados importados.
- 4 En el panel Autenticación de tarjeta inteligente, haga clic en **Editar**.
- 5 En el cuadro de diálogo Editar autenticación de tarjeta inteligente, seleccione la página Certificados.
- 6 Agregue certificados de una entidad de certificación (CA) de confianza, por ejemplo, certificados de una CA raíz o intermediaria.
- 7 Abra la página Autenticación de tarjeta inteligente, active la casilla **Habilitar autenticación de tarjeta inteligente** y haga clic en **Aceptar**.

## Deshabilitar la autenticación de tarjeta inteligente

Deshabilite la autenticación de tarjeta inteligente para regresar a la autenticación predeterminada de nombre de usuario y contraseña que permite iniciar sesión en la DCUI de ESXi.

#### Procedimiento

- 1 En vSphere Web Client, desplácese hasta el host.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 En Sistema, seleccione **Servicios de autenticación**.  
Puede ver el estado actual de autenticación de tarjeta inteligente y una lista con los certificados importados.
- 4 En el panel Autenticación de tarjeta inteligente, haga clic en **Editar**.
- 5 En la página Autenticación de tarjeta inteligente, desactive la casilla **Habilitar autenticación de tarjeta inteligente** y haga clic en **Aceptar**.

## Autenticar credenciales de usuario durante problemas de conectividad

Si no se puede tener acceso al servidor de dominios de Active Directory (AD), puede iniciar sesión en la DCUI de ESXi con la autenticación de nombre de usuario y contraseña para realizar acciones de emergencia en el host.

En raras ocasiones, no se puede tener acceso al servidor de dominio de AD para autenticar las credenciales de usuario en la tarjeta inteligente debido a problemas de conectividad, cortes de red o desastres. Si se pierde la conexión al servidor de AD, puede iniciar sesión en la DCUI de ESXi con las credenciales de un usuario local de ESXi. Esto permite realizar diagnósticos u otras acciones de emergencia. La reserva del inicio de sesión con nombre de usuario y contraseña queda registrada. Cuando la conectividad a AD se restaura, se vuelve a habilitar la autenticación de tarjeta inteligente.

---

**Nota** La pérdida de la conectividad de red con vCenter Server no afecta la autenticación de tarjeta inteligente si el servidor de Active Directory (AD) está disponible.

---

## Usar la autenticación de tarjeta inteligente en el modo de bloqueo

Cuando el modo de bloqueo está habilitado en el host ESXi, aumenta la seguridad del host y se limita el acceso a la interfaz de usuario de la consola directa (DCUI). El modo de bloqueo puede deshabilitar la característica de autenticación de tarjeta inteligente.

En el modo normal de bloqueo, únicamente los usuarios que figuran en la lista de usuarios con excepción con privilegios de administrador pueden acceder a la DCUI. Los usuarios con excepción son usuarios locales del host o usuarios de Active Directory con permisos definidos localmente para el host ESXi. Si desea utilizar la autenticación de tarjeta inteligente en el modo normal de bloqueo, debe agregar usuarios a la lista de usuarios con excepción desde vSphere Web Client. Estos usuarios no pierden sus permisos cuando el host entra en el modo de bloqueo normal y pueden iniciar sesión en la DCUI. Para obtener más información, consulte [Especificar usuarios con excepción para el modo de bloqueo](#).

En el modo de bloqueo estricto, el servicio de la DCUI se interrumpe. Como consecuencia, no se puede acceder al host con la autenticación de tarjeta inteligente.

## Claves SSH de ESXi

Puede usar claves SSH para restringir, controlar y proteger el acceso a un host ESXi. Al utilizar una clave SSH, puede permitir a usuarios o scripts confiables iniciar sesión en un host sin especificar una contraseña.

Puede copiar la clave SSH en el host mediante el comando de CLI `vifs vSphere`. Consulte *Introducción a vSphere Command-Line Interface* para obtener información sobre cómo instalar y utilizar el conjunto de comandos de CLI de vSphere. También es posible utilizar el método PUT de HTTPS para copiar la clave SSH en el host.

En lugar de generar claves de forma externa y cargarlas, es posible crearlas en el host ESXi y descargarlas. Consulte el artículo [1002866](#) de la base de conocimientos de VMware.

Habilitar SSH y agregar claves SSH en el host conlleva riesgos inherentes, y no son acciones recomendadas en un entorno fortalecido. Consulte [Deshabilitar claves autorizadas \(SSH\)](#).

---

**Nota** En ESXi 5.0 y versiones anteriores, un usuario con una clave SSH puede acceder al host incluso si este se encuentra en modo de bloqueo. Este problema está solucionado en ESXi 5.1.

---

## Seguridad de SSH

Puede usar SSH para iniciar sesión de forma remota en ESXi Shell y realizar tareas de solución de problemas en el host.

La configuración de SSH en ESXi se mejora para proporcionar un nivel mayor de seguridad.

### Protocolo SSH versión 1 deshabilitado

VMware no admite el protocolo SSH versión 1 y usa el protocolo versión 2 de forma exclusiva. La versión 2 elimina determinados problemas de seguridad que tiene la versión 1 y ofrece una forma segura de comunicarse con la interfaz de administración.

### Intensidad de cifrado mejorada

SSH admite solo cifrados AES de 256 y 128 bits para las conexiones.

Esta configuración está diseñada para proporcionar una protección sólida de los datos que se transmiten a la interfaz de administración a través de SSH. Esta configuración no se puede cambiar.

## Cargar una clave SSH mediante un comando vifs

Si decide que desea utilizar claves autorizadas para iniciar sesión en un host con SSH, puede cargarlas con un comando `vifs`.

---

**Nota** Debido a que las claves autorizadas permiten el acceso SSH sin requerir autenticación de usuario, evalúe detenidamente si desea usar claves SSH en el entorno.

---

Las claves autorizadas permiten autenticar el acceso remoto a un host. Cuando los usuarios o scripts intentan acceder a un host con SSH, la clave proporciona la autenticación sin solicitar una contraseña. Las claves autorizadas permiten automatizar la autenticación, lo cual resulta útil para escribir scripts que realizan tareas de rutina.

Puede cargar en un host los siguientes tipos de claves SSH.

- Archivo de claves autorizadas para el usuario raíz
- Clave de RSA
- Clave pública de RSA

A partir de la versión vSphere 6.0 Update 2, las claves DSS/DSA ya no son compatibles.

---

**Importante** No modifique el archivo `/etc/ssh/sshd_config`.

---

#### Procedimiento

- ◆ En la línea de comandos o en un servidor de administración, use el comando `vifs` para cargar la clave SSH en la ubicación correcta en el host ESXi.

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

Tipo de clave	Ubicación
Archivos de claves autorizadas para el usuario raíz	/host/ssh_root_authorized_keys Debe tener privilegios de administrador completos para poder cargar el archivo.
Claves RSA	/host/ssh_host_rsa_key
Claves públicas RSA	/host/ssh_host_rsa_key_pub

## Cargar una clave SSH mediante el método PUT de HTTPS

Puede utilizar claves autorizadas para iniciar sesión en un host con SSH. Puede cargar las claves autorizadas mediante el método PUT de HTTPS.

Las claves autorizadas permiten autenticar el acceso remoto a un host. Cuando los usuarios o scripts intentan acceder a un host con SSH, la clave proporciona la autenticación sin solicitar una contraseña. Las claves autorizadas permiten automatizar la autenticación, lo cual resulta útil para escribir scripts que realizan tareas de rutina.

Puede cargar en un host los siguientes tipos de claves SSH mediante el método PUT de HTTPS:

- Archivo de claves autorizadas para el usuario raíz
- Clave DSA
- Clave pública de DSA
- Clave de RSA
- Clave pública de RSA

---

**Importante** No modifique el archivo `/etc/ssh/sshd_config`.

---

#### Procedimiento

- 1 En la aplicación de carga, abra el archivo de claves.

## 2 Publique el archivo en las siguientes ubicaciones.

Tipo de clave	Ubicación
Archivos de claves autorizadas para el usuario raíz	<code>https://hostname_or_IP_address/host/ssh_root_authorized_keys</code> Debe tener privilegios completos de administrador sobre el host para poder cargar el archivo.
Claves DSA	<code>https://hostname_or_IP_address/host/ssh_host_dsa_key</code>
Claves públicas DSA	<code>https://hostname_or_IP_address/host/ssh_host_dsa_key_pub</code>
Claves RSA	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key</code>
Claves públicas RSA	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key_pub</code>

## Usar ESXi Shell

ESXi Shell está deshabilitado de manera predeterminada en los hosts ESXi. Es posible habilitar el acceso local y remoto al shell, si es necesario.

Para reducir el riesgo de accesos no autorizados, habilite ESXi Shell solo para solucionar problemas.

ESXi Shell es independiente del modo de bloqueo. Incluso si el host se ejecuta en modo de bloqueo, todavía puede iniciar sesión en ESXi Shell si está habilitado.

### ESXi Shell

Habilite este servicio para acceder a ESXi Shell de forma local.

### SSH

Habilite este servicio para acceder a ESXi Shell de forma remota mediante SSH.

Consulte *Seguridad de vSphere*.

El usuario raíz y los usuarios con la función de administrador pueden acceder a ESXi Shell. Los usuarios que se encuentran en el grupo de Administradores de ESX reciben automáticamente la función de administrador. De forma predeterminada, solamente el usuario raíz puede ejecutar comandos del sistema (como `vmware -v`) mediante ESXi Shell.

---

**Nota** No habilite ESXi Shell a menos que necesite el acceso.

---

- [Usar vSphere Web Client para habilitar el acceso a ESXi Shell](#)

Puede utilizar vSphere Web Client para habilitar el acceso local o remoto (SSH) a ESXi Shell, y para establecer el tiempo de espera de inactividad y de disponibilidad.

- [Usar la interfaz de usuario de la consola directa \(DCUI\) para habilitar el acceso a ESXi Shell](#)

La interfaz de usuario de la consola directa (DCUI) permite interactuar con el host de forma local mediante los menús basados en texto. Determine si los requisitos de seguridad de su entorno admiten la habilitación de la interfaz de usuario de la consola directa.

## ■ Iniciar sesión en ESXi Shell para solucionar problemas

Realice tareas de configuración de ESXi con vSphere Web Client, vSphere CLI o vSphere PowerCLI. Inicie sesión en ESXi Shell (anteriormente Tech Support Mode o TSM) solo para fines de solución de problemas.

## Usar vSphere Web Client para habilitar el acceso a ESXi Shell

Puede utilizar vSphere Web Client para habilitar el acceso local o remoto (SSH) a ESXi Shell, y para establecer el tiempo de espera de inactividad y de disponibilidad.

---

**Nota** Acceda al host con vSphere Web Client, las herramientas remotas de línea de comandos (vCLI y PowerCLI) y las API publicadas. No habilite el acceso remoto al host con SSH a menos que se presenten circunstancias especiales que requieran que habilite el acceso de SSH.

---

### Requisitos previos

Si desea utilizar una clave de SSH autorizada, puede cargarla. Consulte [Claves SSH de ESXi](#).

### Procedimiento

- 1 Desplácese hasta el host en el inventario de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 En Sistema, seleccione **Perfil de seguridad**.
- 4 En el panel Servicios, haga clic en **Editar**.
- 5 Seleccione un servicio de la lista.
  - ESXi Shell
  - SSH
  - Interfaz de usuario de consola directa
- 6 Haga clic en **Detalles de servicio** y seleccione la directiva de inicio **Iniciar y detener manualmente**.

Cuando se selecciona **Iniciar y detener manualmente**, el servicio no se inicia al reiniciar el host. Si desea que el servicio se inicie al reiniciar el host, seleccione **Iniciar y detener con el host**.

- 7 Seleccione **Iniciar** para habilitar el servicio.
- 8 Haga clic en **Aceptar**.

### Pasos siguientes

Establezca los tiempos de espera de disponibilidad e inactividad para ESXi Shell. Consulte [Crear un tiempo de espera para la disponibilidad de ESXi Shell en vSphere Web Client](#) y [Crear un tiempo de espera para sesiones de ESXi Shell inactivas en vSphere Web Client](#).



## Crear un tiempo de espera para la disponibilidad de ESXi Shell en vSphere Web Client

La instancia de ESXi Shell está deshabilitada de forma predeterminada. Puede establecer un tiempo de espera de disponibilidad para ESXi Shell a fin de aumentar la seguridad cuando se habilita el shell.

La configuración de tiempo de espera de disponibilidad corresponde a la cantidad de tiempo que puede transcurrir antes de que pueda iniciar sesión tras la habilitación de ESXi Shell. Una vez que transcurre el período de espera, el servicio se deshabilita y los usuarios no pueden iniciar sesión.

### Procedimiento

- 1 Desplácese hasta el host en el inventario de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración..**
- 3 En Sistema, seleccione **Configuración avanzada del sistema**.
- 4 Seleccione UserVars.ESXiShellTimeOut y haga clic en el icono **Editar**.
- 5 Introduzca la configuración de tiempo de espera de inactividad.

Debe reiniciar el servicio SSH y el servicio ESXi Shell para que se aplique el tiempo de espera.

- 6 Haga clic en **Aceptar**.

### Resultados

Si inicia sesión y se agota el tiempo de espera, la sesión se mantiene activa. No obstante, una vez que se cierra o se interrumpe la sesión, los usuarios no pueden iniciar sesión.

## Crear un tiempo de espera para sesiones de ESXi Shell inactivas en vSphere Web Client

Si un usuario habilita ESXi Shell en un host, pero olvida cerrar la sesión, la sesión inactiva permanece conectada de forma indefinida. La conexión abierta puede aumentar la posibilidad de que alguien obtenga acceso privilegiado al host. Para impedir esta situación, configure un tiempo de espera para las sesiones inactivas.

El tiempo de espera de inactividad corresponde a la cantidad de tiempo que puede transcurrir antes de que se cierre la sesión interactiva inactiva de un usuario. Es posible controlar la cantidad de tiempo que duran una sesión local y una sesión remota (SSH) desde la interfaz de usuario de la consola directa (DCUI) o desde vSphere Web Client.

### Procedimiento

- 1 Desplácese hasta el host en el inventario de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración..**
- 3 En Sistema, seleccione **Configuración avanzada del sistema**.
- 4 Seleccione UserVars.ESXiShellInteractiveTimeOut, haga clic en el icono **Editar** e introduzca el valor para el tiempo de espera.

- 5 Reinicie el servicio de ESXi Shell y el servicio SSH para que se aplique el tiempo de espera.

### Resultados

Si la sesión está inactiva, se cerrará la sesión de los usuarios una vez transcurrido el período de tiempo de espera.

## Usar la interfaz de usuario de la consola directa (DCUI) para habilitar el acceso a ESXi Shell

La interfaz de usuario de la consola directa (DCUI) permite interactuar con el host de forma local mediante los menús basados en texto. Determine si los requisitos de seguridad de su entorno admiten la habilitación de la interfaz de usuario de la consola directa.

Se puede utilizar la interfaz de usuario de la consola directa para habilitar el acceso local o remoto a ESXi Shell.

---

**Nota** Los cambios que se realizan en el host desde la interfaz de usuario de la consola directa, vSphere Web Client, ESXCLI u otras herramientas administrativas se envían al almacenamiento permanente cada una hora o después de un apagado correcto. Si se produce un problema en el host antes de que se envíen los cambios, estos cambios pueden perderse.

---

### Procedimiento

- 1 En la interfaz de usuario de la consola directa, presione F2 para acceder al menú Personalización del sistema.
- 2 Seleccione **Opciones de solución de problemas** y presione Intro.
- 3 En el menú Opciones del modo de solución de problemas, seleccione un servicio para habilitar.
  - Habilitar ESXi Shell
  - Habilitar SSH
- 4 Presione Intro para habilitar el servicio.
- 5 Presione Esc hasta que vuelva al menú principal de la interfaz de usuario de la consola directa.

### Pasos siguientes

Establezca los tiempos de espera de disponibilidad e inactividad para ESXi Shell. Consulte [Crear un valor de tiempo de espera de disponibilidad de ESXi Shell en la interfaz de usuario de la consola directa](#) y [Crear un tiempo de espera para sesiones de ESXi Shell inactivas](#).

## Crear un valor de tiempo de espera de disponibilidad de ESXi Shell en la interfaz de usuario de la consola directa

La instancia de ESXi Shell está deshabilitada de forma predeterminada. Puede establecer un tiempo de espera de disponibilidad para ESXi Shell a fin de aumentar la seguridad cuando se habilita el shell.

La configuración de tiempo de espera de disponibilidad corresponde a la cantidad de tiempo que puede transcurrir antes de que pueda iniciar sesión tras la habilitación de ESXi Shell. Una vez que transcurre el período de espera, el servicio se deshabilita y los usuarios no pueden iniciar sesión.

#### Procedimiento

- 1 En el menú Opciones del modo de solución de problemas, seleccione **Modificar tiempos de espera de SSH y ESXi Shell** y presione Intro.

- 2 Introduzca el tiempo de espera de disponibilidad.

Debe reiniciar el servicio SSH y el servicio ESXi Shell para que se aplique el tiempo de espera.

- 3 Presione Entrar y Esc hasta regresar al menú principal de la interfaz de usuario de la consola directa.

- 4 Haga clic en **Aceptar**.

#### Resultados

Si inicia sesión y se agota el tiempo de espera, la sesión se mantiene activa. No obstante, una vez que se cierra o se interrumpe la sesión, los usuarios no pueden iniciar sesión.

### Crear un tiempo de espera para sesiones de ESXi Shell inactivas

Si un usuario habilita ESXi Shell en un host, pero olvida cerrar la sesión, la sesión inactiva permanece conectada de forma indefinida. La conexión abierta puede aumentar la posibilidad de que alguien obtenga acceso privilegiado al host. Para impedir esta situación, configure un tiempo de espera para las sesiones inactivas.

El tiempo de espera de inactividad corresponde a la cantidad de tiempo que puede transcurrir antes de que se cierren las sesiones interactivas inactivas. Los cambios en el tiempo de espera de inactividad se aplican la próxima vez que un usuario inicia sesión en ESXi Shell y no afectan las sesiones actuales.

Puede especificar el tiempo de espera en segundos desde la interfaz de usuario de la consola directa o en minutos desde vSphere Web Client.

#### Procedimiento

- 1 En el menú Opciones del modo de solución de problemas, seleccione **Modificar tiempos de espera de SSH y ESXi Shell** y presione Intro.

- 2 Introduzca el tiempo de espera de inactividad en segundos.

Debe reiniciar el servicio SSH y el servicio ESXi Shell para que se aplique el tiempo de espera.

- 3 Presione Entrar y Esc hasta regresar al menú principal de la interfaz de usuario de la consola directa.

#### Resultados

Si la sesión está inactiva, se cerrará la sesión de los usuarios una vez transcurrido el período de tiempo de espera.

## Iniciar sesión en ESXi Shell para solucionar problemas

Realice tareas de configuración de ESXi con vSphere Web Client, vSphere CLI o vSphere PowerCLI. Inicie sesión en ESXi Shell (anteriormente Tech Support Mode o TSM) solo para fines de solución de problemas.

### Procedimiento

- 1 Inicie sesión en ESXi Shell con uno de los siguientes métodos.
  - Si tiene acceso directo al host, presione Alt + F1 para abrir la página de inicio de sesión en la consola física de la máquina.
  - Si se conecta al host de forma remota, utilice SSH u otra conexión de consola remota para iniciar una sesión en el host.
- 2 Escriba un nombre de usuario y una contraseña que reconozca el host.

## Modificar la configuración del proxy web de ESXi

Al modificar la configuración del proxy web, hay varias directrices de seguridad del usuario y del cifrado que se deben tener en cuenta.

---

**Nota** Reinicie el proceso del host después de realizar cualquier cambio en los directorios o los mecanismos de autenticación del host.

---

- No configure certificados que utilicen una contraseña o frases de contraseña. ESXi no es compatible con proxies web que utilizan contraseñas o frases de contraseña, llamadas también claves cifradas. Si se configura un proxy web que requiere una contraseña o una frase de contraseña, los procesos de ESXi no podrán iniciarse correctamente.
- Para que resulte compatible el cifrado de los nombres de usuario, las contraseñas y los paquetes, SSL se habilita de forma predeterminada en las conexiones de vSphere Web Services SDK. Si se desea configurar estas conexiones de modo que no cifren las transmisiones, deshabilite SSL en la conexión de vSphere Web Services SDK. Para ello, cambie la conexión de HTTPS a HTTP.

Considere deshabilitar SSL solo si creó un entorno de plena confianza para estos clientes, donde los firewalls estén establecidos y las transmisiones desde y hacia el host estén aisladas por completo. Si se deshabilita SSL, se puede mejorar el rendimiento debido a que se evita la sobrecarga requerida para el cifrado.

- Para evitar la utilización incorrecta de los servicios de ESXi, se puede acceder a la mayoría de los servicios internos de ESXi únicamente mediante el puerto 443, el puerto utilizado para la transmisión de HTTPS. El puerto 443 funciona como un proxy inverso de ESXi. Se puede ver la lista de servicios en ESXi a través de la página principal de HTTP, pero no se puede acceder directamente a los servicios de adaptadores de almacenamiento sin la debida autorización.

Se puede cambiar esta configuración de modo que los servicios individuales sean accesibles directamente a través de las conexiones de HTTP. No realice este cambio, a menos que utilice ESXi en un entorno de plena confianza.

- Al actualizar el entorno, el certificado permanece en su ubicación.

## Consideraciones de seguridad de vSphere Auto Deploy

Para optimizar la protección del entorno, tenga en cuenta los riesgos de seguridad que pueden existir cuando se utiliza Auto Deploy con perfiles de host.

### Seguridad de redes

Proteja la red de la misma manera que lo haría con cualquier otro método de implementación basado en PXE. vSphere Auto Deploy transfiere datos por SSL para evitar la interferencia y la intromisión casuales. Sin embargo, la autenticidad del cliente o del servidor Auto Deploy no se comprueba durante un arranque PXE.

Puede reducir ampliamente el riesgo de seguridad de Auto Deploy aislando por completo la red donde se utiliza Auto Deploy.

### Imagen de arranque y seguridad de perfil de host

La imagen de arranque que descarga el servidor vSphere Auto Deploy en una máquina puede tener los siguientes componentes.

- Los paquetes de VIB que componen el perfil de imagen se incluyen siempre en la imagen de arranque.
- El perfil de host y la personalización del host se incluyen en la imagen de arranque si las reglas de Auto Deploy se configuran para aprovisionar el host con un perfil de imagen o una configuración de personalización del host.

- La contraseña del administrador (raíz) y las contraseñas de usuario que se incluyen con el perfil de host y la personalización del host poseen un cifrado MD5.
- Cualquier otra contraseña asociada a los perfiles quedará excluida. Si configura Active Directory utilizando perfiles de host, las contraseñas no poseen protección.

Utilice vSphere Authentication Service para configurar Active Directory con el fin de evitar la exposición de las contraseñas de Active Directory. Si configura Active Directory utilizando perfiles de host, las contraseñas no están protegidas.

- El certificado y la clave SSL públicas y privadas del host se incluyen en la imagen de arranque.

## Administrar archivos de registro de ESXi

Los archivos de registro son un componente importante para la solución de problemas de ataques y la obtención de información sobre las vulneraciones de la seguridad de los hosts. El registro en

un servidor de registro centralizado y seguro puede ayudar a prevenir la adulteración de registros. El registro remoto también proporciona un registro de auditoría a largo plazo.

Tome las medidas siguientes para mejorar la seguridad del host.

- Configure los registros persistentes en un almacén de datos. De forma predeterminada, los registros en los hosts ESXi se almacenan en el sistema de archivos en la memoria. Por lo tanto, se pierden con cada reinicio del host y solo se almacenan 24 horas de datos de registros. Al habilitar los registros persistentes, tiene un registro dedicado de la actividad del servidor que está disponible para el host.
- El registro remoto en un host central le permite recopilar archivos de registro en un host central, desde donde puede supervisar todos los hosts con una sola herramienta. También puede combinar análisis y búsqueda de datos de registro, lo que puede ayudar a revelar información sobre aspectos como ataques coordinados en varios hosts.
- Configure syslog remoto seguro en los hosts ESXi que usan una línea de comandos remota, como vCLI o PowerCLI, o que usan un cliente de API.
- Consulte la configuración de syslog para asegurarse de que se haya configurado un servidor de syslog válido, incluido el puerto correcto.

## Configurar Syslog en hosts ESXi

Todos los hosts ESXi ejecutan un servicio de Syslog (`vm syslogd`), que registra mensajes de VMkernel y otros componentes del sistema en archivos de registro.

Puede utilizar vSphere Web Client o el comando `esxcli system syslog` de vCLI para configurar el servicio de Syslog.

Para obtener más información sobre los comandos de vCLI, consulte *Introducción a vSphere Command-Line Interface*.

### Procedimiento

- 1 En el inventario de vSphere Web Client, seleccione el host.
- 2 Haga clic en la pestaña **Administrar**.
- 3 En el panel Sistema, haga clic en **Configuración avanzada del sistema**.
- 4 Encuentre la sección **Syslog** de la lista Configuración avanzada del sistema.
- 5 Para configurar el registro de manera global, seleccione la configuración que desea cambiar y haga clic en el icono Editar.

Opción	Descripción
<code>Syslog.global.defaultRotate</code>	Establece el número máximo de archivos que se van a mantener. Puede configurar este número en forma global y para subregistradores individuales.
<code>Syslog.global.defaultSize</code>	Configure el tamaño predeterminado del registro, en KB, antes de que el sistema rote los registros. Puede configurar este número en forma global y para subregistradores individuales.

Opción	Descripción
<b>Syslog.global.LogDir</b>	El directorio en el que se almacenan los registros. El directorio puede estar ubicado en volúmenes de NFS o VMFS montados. Solo el directorio <code>/scratch</code> del sistema de archivos local se mantiene en todos los reinicios. El directorio debería especificarse como <code>[datastorename] path_to_file</code> , donde la ruta de acceso es relativa a la raíz del volumen que respalda el almacén de datos. Por ejemplo, la ruta de acceso <code>[storage1] /systemlogs</code> se asigna a la ruta de acceso <code>/vmfs/volumes/storage1/systemlogs</code> .
<b>Syslog.global.logDirUnique</b>	Al seleccionar esta opción, se crea un subdirectorio con el nombre del host ESXi del directorio especificado por <b>Syslog.global.LogDir</b> . Un directorio único es útil si varios hosts ESXi utilizan el mismo directorio NFS.
<b>Syslog.global.LogHost</b>	El host remoto al que se reenvían los mensajes de syslog y el puerto en el que el host remoto recibe mensajes de syslog. Puede incluir el protocolo y el puerto; por ejemplo, <code>ssl://hostname1:1514</code> . Se admiten UDP (predeterminado), TCP y SSL. El host remoto debe tener syslog instalado y configurado correctamente para recibir los mensajes de syslog reenviados. Consulte la documentación del servicio de Syslog instalado en el host remoto para obtener información sobre la configuración.

6 (Opcional) Para sobrescribir los valores predeterminados del tamaño de registro y la rotación de registros de cualquier registro.

- Haga clic en el nombre del registro que desea personalizar.
- Haga clic en el icono Editar y escriba el número de rotaciones y el tamaño de registro que desea.

7 Haga clic en **Aceptar**.

## Resultados

Los cambios en las opciones de syslog se aplican de inmediato.

## Ubicaciones de archivos de registro de ESXi

ESXi registra la actividad de los hosts en los archivos de registro, mediante una funcionalidad de Syslog.

Componente	Ubicación	Propósito
VMkernel	<code>/var/log/vmkernel.log</code>	Registra las actividades relacionadas con máquinas virtuales y ESXi.
Advertencias de VMkernel	<code>/var/log/vmkwarning.log</code>	Registra las actividades relacionadas con máquinas virtuales.
Resumen de VMkernel	<code>/var/log/vmksummary.log</code>	Se utiliza para determinar las estadísticas de disponibilidad y tiempo de actividad de ESXi (valores separados por comas).
Registro del agente del host ESXi	<code>/var/log/hostd.log</code>	Contiene información sobre el agente que administra y configura el host ESXi y sus máquinas virtuales.

Componente	Ubicación	Propósito
Registro del agente de vCenter	<code>/var/log/vpxa.log</code>	Contiene información sobre el agente que se comunica con vCenter Server (si el host es administrado por vCenter Server).
Registro del shell	<code>/var/log/shell.log</code>	Contiene un registro de todos los comandos introducidos en ESXi Shell y también de todos los eventos del shell (por ejemplo, el momento en que se habilitó el shell).
Autenticación	<code>/var/log/auth.log</code>	Contiene todos los eventos relacionados con la autenticación para el sistema local.
Mensajes del sistema	<code>/var/log/syslog.log</code>	Contiene todos los mensajes del registro general y puede usarse para solución de problemas. Esta información antes se encontraba en los mensajes del archivo de registro.
Máquinas virtuales	El mismo directorio en el que se encuentran los archivos de configuración de la máquina virtual afectada, denominados <code>vmware.log</code> y <code>vmware*.log</code> . Por ejemplo, <code>/vmfs/volumes/datastore/virtual machine/vmware.log</code>	Contiene todos los eventos relacionados con el encendido de la máquina virtual, la información de errores del sistema, la actividad y el estado de las herramientas, la sincronización de hora, los cambios en el hardware virtual, las migraciones de vMotion, los clones de la máquina, etc.

## Proteger tráfico de registro de Fault Tolerance

Al habilitar Fault Tolerance (FT), VMware vLockstep captura las entradas y los eventos que se producen en una máquina virtual principal y los envía a la máquina virtual secundaria, que se ejecuta en otro host.

Este tráfico de registro entre la máquina virtual principal y la secundaria está descifrado y contiene datos de la red invitada y de la E/S de almacenamiento, como también contenido de memoria del sistema operativo invitado. Este tráfico puede incluir datos sensibles como contraseñas en texto sin formato. Para evitar que estos datos se divulguen, asegúrese de que la red esté segura, especialmente contra ataques de intermediarios ("man-in-the-middle"). Por ejemplo, use una red privada para el tráfico de registro de FT.



# Proteger sistemas vCenter Server

# 6

La protección de vCenter Server incluye la seguridad del host en el que se ejecuta vCenter Server, el cumplimiento de las prácticas recomendadas para asignar privilegios y funciones, y la comprobación de la integridad de los clientes que se conectan a vCenter Server.

Este capítulo incluye los siguientes temas:

- [Prácticas recomendadas de seguridad de vCenter Server](#)
- [Comprobar huellas digitales para hosts ESXi heredados](#)
- [Comprobar que la validación de certificados SSL mediante una copia de archivos de red está habilitada](#)
- [Puertos TCP y UDP de vCenter Server](#)
- [Controlar el acceso a la herramienta de supervisión de hardware basada en CIM](#)

## Prácticas recomendadas de seguridad de vCenter Server

Seguir las prácticas recomendadas de seguridad para vCenter Server ayuda a garantizar la integridad del entorno de vSphere.

## Prácticas recomendadas sobre el control de acceso a vCenter Server

Realice un control estricto del acceso a los diferentes componentes de vCenter Server a fin de aumentar la seguridad del sistema.

Las siguientes instrucciones ayudan a garantizar la seguridad del entorno.

### Usar cuentas con nombre

- Si la cuenta de administrador local de Windows actualmente otorga derechos administrativos completos para vCenter Server, elimine esos derechos de acceso y otórguelos a una o más cuentas de administrador de vCenter Server con nombre. Otorgue derechos administrativos completos únicamente a aquellos administradores que los necesitan. No le otorgue este privilegio a cualquier grupo cuya pertenencia no esté estrictamente controlada.

---

**Nota** A partir de vSphere 6.0, el administrador local ya no cuenta con derechos administrativos completos para acceder a vCenter Server de forma predeterminada. No se recomienda el uso de usuarios de sistemas operativos locales.

---

- Instale vCenter Server mediante una cuenta de servicio en lugar de hacerlo desde una cuenta de Windows. La cuenta de servicio debe ser un administrador en la máquina local.
- Compruebe que las aplicaciones usen cuentas de servicio únicas al conectarse a un sistema vCenter Server.

## Minimizar el acceso

Evite otorgar permiso para que los usuarios inicien sesión directamente en el equipo host de vCenter Server. Los usuarios cuya sesión en vCenter Server está iniciada pueden llegar a causar daños, ya sea intencionales o involuntarios, al alterar la configuración y modificar los procesos. También pueden llegar a acceder a las credenciales de vCenter, como el certificado SSL. Permítalos solo a los usuarios con tareas legítimas para realizar que inicien sesión en el sistema y asegúrese de que se auditen los eventos de inicio de sesión.

## Supervisar los privilegios de los usuarios administradores de vCenter Server

No todos los usuarios administradores deben tener la función de administrador. En cambio, se puede crear una función personalizado con el conjunto adecuado de privilegios y asignárselo a otros administradores.

Los usuarios con la función de administrador de vCenter Server tienen privilegios sobre todos los objetos de la jerarquía. Por ejemplo, la función de administrador permite, de forma predeterminada, que los usuarios interactúen con los archivos y los programas que se encuentran en el sistema operativo invitado de la máquina virtual. Si se asigna esa función a demasiados usuarios, se puede reducir la confidencialidad, la disponibilidad o la integridad de los datos de la máquina virtual. Cree una función que les otorgue a los administradores los privilegios que necesitan, pero elimine algunos de los privilegios de administración de la máquina virtual.

## Otorgar privilegios mínimos a los usuarios de bases de datos de vCenter Server

El usuario de base de datos precisa solamente ciertos privilegios específicos para el acceso a la base de datos. Asimismo, algunos privilegios son necesarios solamente para la instalación y las actualizaciones. Estos privilegios pueden eliminarse una vez instalado o actualizado el producto.

## Restringir el acceso al explorador del almacén de datos

La funcionalidad de explorador de almacén de datos permite que los usuarios con los privilegios correspondientes vean, actualicen o descarguen archivos en almacenes de datos asociados con la implementación de vSphere a través del explorador web o vSphere Web Client. Asigne el privilegio **Almacén de datos.Examinar almacén de datos** solo a los usuarios o grupos que realmente lo necesitan.

## Restringir la ejecución de comandos en una máquina virtual a los usuarios

De forma predeterminada, un usuario con función de administrador de vCenter Server puede interactuar con archivos y programas dentro del sistema operativo invitado de una máquina virtual. Para reducir el riesgo de infracciones de confidencialidad, disponibilidad o integridad del invitado, cree una función de acceso que no sea de invitado sin el privilegio **Operaciones de invitado**. Consulte [Restringir la ejecución de comandos dentro de una máquina virtual a los usuarios](#).

## Comprobar la directiva sobre contraseñas de vpxuser

De manera predeterminada, vCenter Server cambia la contraseña de vpxuser automáticamente cada 30 días. Asegúrese de que esta configuración cumpla con sus directivas, o bien configúrela para que se adapte a las directivas de caducidad de contraseñas de su empresa. Consulte [Configurar la directiva de contraseñas de vCenter Server](#).

---

**Nota** Compruebe que la directiva de caducidad de contraseñas no sea demasiado corta.

---

## Comprobar los privilegios después de reiniciar vCenter Server

Revise la reasignación de privilegios al reiniciar vCenter Server. Si el usuario o el grupo de usuarios al que se asignó la función de administrador en la carpeta raíz no pueden verificarse como usuario o grupo de usuarios válido durante el reinicio, se elimina la función para ese usuario o ese grupo. En su lugar, vCenter Server otorga la función de administrador a la cuenta de vCenter Single Sign-On administrator@vsphere.local. Esta cuenta puede funcionar como administrador.

Restablezca la cuenta de administrador con nombre y asigne la función de administrador a dicha cuenta para evitar usar la cuenta administrator@vsphere.local anónima.

## Usar niveles altos de cifrado RDP

Asegúrese de que en cada equipo con Windows de la infraestructura se establezca una configuración del host mediante Remote Desktop a fin de garantizar el nivel más alto de cifrado adecuado para el entorno.

## Comprobar certificados de vSphere Web Client

Indique a los usuarios de una de las instancias de vSphere Web Client o de otras aplicaciones cliente que nunca omitan las advertencias de comprobación de certificados. Sin la comprobación de certificados, el usuario puede ser víctima de un ataque de MiTM.

## Configurar la directiva de contraseñas de vCenter Server

De manera predeterminada, vCenter Server cambia la contraseña de vpxuser automáticamente cada 30 días. Puede cambiar este valor desde vSphere Web Client.

### Procedimiento

- 1 Seleccione vCenter Server en la jerarquía de objetos de vSphere Web Client.

- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 Haga clic en **Configuración avanzada** e introduzca **VimPasswordExpirationInDays** en la casilla de filtro.
- 4 Configure `VirtualCenter.VimPasswordExpirationInDays` para que cumpla con sus requisitos.

## Proteger el host de Windows para vCenter Server

Para proteger el host de Windows donde se ejecuta vCenter Server contra vulnerabilidades y ataques, garantice que el entorno del host sea lo más seguro posible.

- Mantenga un sistema operativo, una base de datos y hardware compatibles para el sistema vCenter Server. Si vCenter Server no se ejecuta en un sistema operativo compatible, es posible que no funcione correctamente, y vCenter Server queda vulnerable a posibles ataques.
- Mantenga el sistema vCenter Server actualizado con las revisiones adecuadas. Cuando el servidor está actualizado con las revisiones del sistema operativo, es menos vulnerable a posibles ataques.
- Proteja al sistema operativo en el host de vCenter Server. La protección incluye software antivirus y antimalware.
- Asegúrese de que en cada equipo con Windows de la infraestructura se establezca una configuración del host mediante Remote Desktop (RDP) a fin de garantizar el nivel más alto de cifrado, conforme a las directrices estándar de la industria o a las instrucciones internas.

Para obtener información sobre la compatibilidad del sistema operativo y la base de datos, consulte *Matrices de compatibilidad de vSphere*.

## Quitar certificados caducados o revocados, y registros de instalaciones con errores

Dejar certificados caducados o revocados, o dejar registros de instalación incorrecta de vCenter Server en el sistema vCenter Server puede perjudicar el entorno.

Los certificados caducados o revocados deben eliminarse por los siguientes motivos.

- Si los certificados caducados o revocados no se eliminan del sistema vCenter Server, el entorno puede quedar vulnerable a un ataque de MiTM.
- En ciertos casos, si la instalación de vCenter Server no se realiza correctamente, se crea en el sistema un archivo de registro que contiene la contraseña de la base de datos en texto sin formato. Un atacante que logre entrar al sistema vCenter Server puede tener acceso a esta contraseña y, al mismo tiempo, acceder a la base de datos de vCenter Server.

## Limitar la conectividad de red de vCenter Server

Para mejorar la seguridad, evite colocar el sistema vCenter Server en otra red distinta de la red de administración, y asegúrese de que el tráfico de administración de vSphere se encuentre en una red restringida. Al limitar la conectividad de red, se limitan ciertos tipos de ataques.

vCenter Server requiere acceso solamente a una red de administración. Evite colocar el sistema vCenter Server en otras redes, como la red de producción o la de almacenamiento, o en otra red con acceso a Internet. vCenter Server no necesita acceder a la red donde funciona vMotion.

vCenter Server requiere conectividad de red con los siguientes sistemas.

- Todos los hosts ESXi.
- La base de datos de vCenter Server.
- Otros sistemas de vCenter Server (si los sistemas de vCenter Server forman parte de un dominio de vCenter Single Sign-On común con fines de replicación de etiquetas, permisos, etc.).
- Los sistemas que están autorizados para ejecutar clientes de administración. Por ejemplo, vSphere Web Client, un sistema Windows donde se utiliza PowerCLI o cualquier otro cliente basado en SDK.
- Los sistemas que ejecutan componentes complementarios como VMware vSphere Update Manager.
- Los servicios de infraestructura como DNS, Active Directory y NTP.
- Otros sistemas que ejecutan componentes fundamentales para la funcionalidad del sistema vCenter Server.

Utilice un firewall local en el sistema Windows donde el sistema vCenter Server se está ejecutando o utilice un firewall de red. Incluya restricciones de acceso basadas en IP de modo que solo los componentes necesarios puedan comunicarse con el sistema vCenter Server.

## Restringir el uso de clientes Linux

Las comunicaciones entre los componentes del cliente y el sistema vCenter Server o los hosts ESXi están protegidas por un cifrado basado en SSL de forma predeterminada. Las versiones de Linux de estos componentes no realizan la validación de certificados. Considere restringir el uso de estos clientes.

Aunque haya reemplazado los certificados firmados por VMCA en el sistema vCenter Server y los hosts ESXi por certificados firmados por una entidad de certificación externa, algunas comunicaciones con clientes Linux siguen siendo vulnerables a ataques de tipo "Man in the middle" (intermedio). Los siguientes componentes son vulnerables cuando se ejecutan en el sistema operativo Linux.

- Comandos de vCLI
- Scripts de vSphere SDK for Perl
- Programas escritos con vSphere Web Services SDK

Si aplica los controles correspondientes, puede reducir la restricción contra el uso de clientes Linux.

- Restrinja el acceso a la red de administración únicamente a los sistemas autorizados.
- Utilice firewalls para garantizar que únicamente los hosts autorizados tengan permiso para acceder a vCenter Server.
- Utilice sistemas JumpBox para garantizar que los clientes Linux sean supervisados.

## Examinar los complementos instalados

Las extensiones de vSphere Web Client se ejecutan en el mismo nivel de privilegio que el usuario que inició sesión. Una extensión maliciosa puede enmascararse como si fuera un complemento útil y realizar operaciones dañinas, como el robo de credenciales o cambios en la configuración del sistema. Para aumentar la seguridad, utilice la instalación de vSphere Web Client que incluya únicamente extensiones autorizadas de orígenes confiables.

La instalación de vCenter incluye el marco de extensibilidad de vSphere Web Client, que proporciona la capacidad de extender vSphere Web Client con selecciones de menú o iconos de la barra de herramientas que proporcionan acceso a componentes de complementos de vCenter o a la funcionalidad externa basada en la Web. Esta flexibilidad puede introducir funcionalidades no intencionadas. Por ejemplo, si un administrador instala un complemento en una instancia de vSphere Web Client, el complemento podrá ejecutar comandos arbitrarios con el nivel de privilegio de ese administrador.

Para evitar una posible transigencia de vSphere Web Client, puede examinar periódicamente todos los complementos instalados y asegurarse de que tengan un origen confiable.

### Requisitos previos

Debe tener los privilegios necesarios para acceder al servicio vCenter Single Sign-On. Estos privilegios difieren de los de vCenter Server.

### Procedimiento

- 1 Inicie sesión en vSphere Web Client como `administrator@vsphere.local` o como usuario con privilegios de vCenter Single Sign-On.
- 2 En la página de inicio, seleccione **Administración** y, a continuación, seleccione **Complementos del cliente** y **Soluciones**.
- 3 Examine la lista de complementos del cliente.

## Prácticas recomendadas de seguridad de vCenter Server Appliance

Siga todas las prácticas recomendadas de seguridad del sistema vCenter Server para proteger vCenter Server Appliance. Se proporcionan pasos adicionales a modo de ayuda para aumentar la seguridad del entorno.

### Configure NTP

Compruebe que todos los sistemas tengan el mismo origen de hora relativo (incluida la correspondiente compensación por localización), y que este pueda ser correlativo con una hora estándar acordada (como la hora universal coordinada-UTC). Para que el certificado tenga validez es fundamental que los sistemas estén sincronizados. NTP también facilita el rastreo de intrusos en los archivos de registro. Una configuración incorrecta de la hora puede dificultar la inspección y la correlación de los archivos de registro a fin de detectar ataques; también puede hacer imprecisas las auditorías. Consulte [Sincronizar la hora de vCenter Server Appliance con un servidor NTP](#).

### Restrinja el acceso a la red de vCenter Server Appliance.

Restrinja el acceso únicamente a los componentes esenciales que se necesitan para comunicarse con vCenter Server Appliance. Si bloquea el acceso desde sistemas innecesarios, reduce las posibilidades de que el sistema operativo reciba ataques generales. La restricción del acceso únicamente a los componentes esenciales minimiza riesgos.

## Comprobar huellas digitales para hosts ESXi heredados

En vSphere 6 y las versiones posteriores, se asignan certificados de VMCA a los hosts de forma predeterminada. Si cambia el modo de certificación a Huella digital, puede continuar usando este modo para los hosts heredados. Puede comprobar las huellas digitales en vSphere Web Client.

---

**Nota** De manera predeterminada, los certificados se conservan en todas las actualizaciones.

---

### Procedimiento

- 1 Desplácese hasta el sistema vCenter Server en el navegador de objetos de vSphere Web Client.
- 2 Seleccione la pestaña **Administrar**, haga clic en **Configuración** y seleccione **General**.
- 3 Haga clic en **Editar**.
- 4 Haga clic en **Configuración de SSL**.
- 5 Si alguno de los hosts ESXi 5.5 o de versiones anteriores necesita una validación manual, compare las huellas digitales detalladas para los hosts con las huellas digitales de la consola del host.

Para obtener la huella digital del host, use la interfaz de usuario de la consola directa (DCUI).

- a Inicie sesión en la consola directa y presione F2 para acceder al menú Personalización del sistema.
- b Seleccione **Ver información de soporte**.

La huella digital del host se muestra en la columna a la derecha.

- 6 Si la huella digital coincide, active la casilla **Comprobar** ubicada junto al host.

Los hosts no seleccionados se desconectan después de hacer clic en **Aceptar**.

- 7 Haga clic en **Aceptar**.

## Comprobar que la validación de certificados SSL mediante una copia de archivos de red está habilitada

Network File Copy (NFC) proporciona un servicio de FTP basado en los tipos de archivos para los componentes de vSphere. A partir de vSphere 5.5, de forma predeterminada, ESXi utiliza NFC para operaciones tales como copiar y mover datos entre almacenes de datos, pero es posible que deba habilitar esta opción si se encuentra deshabilitada.

Cuando se habilita SSL en NFC, las conexiones entre los componentes de vSphere en NFC son seguras. Esta conexión puede ayudar a evitar ataques de intermediario en un centro de datos.

Debido a que NFC en SSL provoca la degradación del rendimiento, considere deshabilitar esta configuración avanzada en algunos entornos de desarrollo.

---

**Nota** Si utiliza scripts para comprobar el valor, establezca este valor de forma explícita en True.

---

### Procedimiento

- 1 Conéctese a vCenter Server con vSphere Web Client.
- 2 Seleccione la pestaña **Configuración** y haga clic en **Configuración avanzada**.
- 3 Haga clic en **Editar**.
- 4 En la parte inferior del cuadro de diálogo, introduzca la clave y el valor siguientes.

Campo	Valor
Clave	config.nfc.useSSL
Valor	true

- 5 Haga clic en **Aceptar**.

## Puertos TCP y UDP de vCenter Server

Se puede acceder a vCenter Server a través de los puertos TCP y UDP predeterminados. Si administra componentes de red desde afuera de un firewall, es posible que se le pida que vuelva a configurar el firewall para permitir el acceso en los puertos necesarios.

En la tabla, se enumeran los puertos TCP y UDP, y se indican el propósito y el tipo de cada uno de ellos. Los puertos que están abiertos de forma predeterminada en el momento de la instalación se indican con la etiqueta (Valor predeterminado). Para obtener una lista actualizada de los puertos de todos los componentes de vSphere correspondientes a diferentes versiones de vSphere, consulte el [artículo 1012382 de la base de conocimientos de VMware](#).



Tabla 6-1. Puertos TCP y UDP de vCenter Server

Puerto	Propósito
80 (valor predeterminado)	Acceso HTTP vCenter Server requiere el puerto 80 para las conexiones HTTP directas. El puerto 80 redirige solicitudes al puerto HTTPS 443. Esta redirección es de suma utilidad si utiliza accidentalmente http://server en lugar de https://server WS-Management (también requiere que el puerto 443 se encuentre abierto)
88, 2013	Interfaz de control RPC para Kerberos, utilizada por vCenter Single Sign-On.
123	Ciente NTP
135 (valor predeterminado)	Para vCenter Server Appliance, este puerto está designado para la autenticación de Active Directory. Para una instalación en Windows de vCenter Server, este puerto se utiliza para el modo vinculado, mientras que el puerto 88 se utiliza para la autenticación de Active Directory.
161 (valor predeterminado)	Servidor SNMP. Este es el puerto predeterminado en un host ESXi y en vCenter Server Appliance.
389	LDAP de vCenter Single Sign-On (6.0 y versiones posteriores)
636	LDAPS de vCenter Single Sign-On (6.0 y versiones posteriores)
443 (valor predeterminado)	Los sistemas vCenter Server usa el puerto 443 para supervisar la transferencia de datos desde los clientes de SDK. Este puerto también se utiliza para los siguientes servicios: <ul style="list-style-type: none"> <li>■ WS-Management (también requiere que el puerto 80 se encuentre abierto)</li> <li>■ Conexiones del cliente de administración de red de terceros con vCenter Server</li> <li>■ Acceso de clientes de administración de red de terceros a los hosts</li> </ul>
2012	Puerto RPC para VMware Directory Service (vmdir).
2014	Puerto RPC para el servicio VMware Certificate Authority (VMCA).
2020	Puerto RPC para VMware Authentication Framework Service (vmafd).
31031, 44046 (predeterminado)	vSphere Replication
7444	vCenter Single Sign-On HTTPS.
8093	El complemento de integración de clientes utiliza un nombre de host de bucle local, y utiliza el puerto 8093 y puertos aleatorios en el rango de 50100 a 60099. El complemento de integración de clientes utiliza el puerto 8093 solo para comunicación local. El puerto puede permanecer bloqueado por el firewall.
8109	VMware Syslog Collector.
9443	Acceso HTTP de vSphere Web Client a hosts ESXi.
10080	Inventory Service.
11711	LDAP de vCenter Single Sign-On (entornos actualizados desde vSphere 5.5)
11712	LDAPS de vCenter Single Sign-On (entornos actualizados desde vSphere 5.5)

**Tabla 6-1. Puertos TCP y UDP de vCenter Server (continuación)**

Puerto	Propósito
12721	VMware Identity Management Service.
15005	ESX Agent Manager (EAM). Un agente de ESX puede ser una máquina virtual o un VIB opcional. El agente amplía las funciones de un host ESXi para ofrecer los servicios adicionales que requiere una solución de vSphere como NSX-v o vRealize Automation.
15007	vService Manager (VSM). Este servicio registra extensiones de vCenter Server. Abra este puerto solo si lo requieren las extensiones que desea usar.
50100-60099	El complemento de integración de clientes utiliza un nombre de host de bucle local, y utiliza el puerto 8093 y puertos aleatorios en el rango de 50100 a 60099. El complemento de integración de clientes utiliza solamente este rango de puertos para la comunicación local. El puerto puede permanecer bloqueado por el firewall.

Además de estos puertos, puede configurar otros puertos según sus necesidades.

## Controlar el acceso a la herramienta de supervisión de hardware basada en CIM

El sistema del modelo de información común (CIM) proporciona una interfaz que habilita la administración en el nivel del hardware desde aplicaciones remotas que usan un conjunto de interfaces de programación de aplicaciones (API) estándar. Para que la interfaz del CIM sea segura, proporcione únicamente el acceso mínimo y necesario a estas aplicaciones. Si una aplicación se aprovisionó con una cuenta raíz o una cuenta de administrador completa y la aplicación se ve comprometida, todo el entorno virtual puede quedar comprometido.

El CIM es un estándar abierto que establece un marco para la supervisión de recursos de hardware sin agente basada en estándares en ESXi. Este marco consta de un administrador de objetos CIM, a menudo llamado agente CIM, y un conjunto de proveedores CIM.

Los proveedores CIM se usan como mecanismo para proporcionar acceso de administración a los controladores de dispositivos y al hardware subyacente. Los distribuidores de hardware, incluidos los fabricantes de servidores y los distribuidores de dispositivos de hardware específicos, pueden escribir a los proveedores para que proporcionen supervisión y administración de sus dispositivos particulares. VMware también escribe a los proveedores que implementan la supervisión del hardware de servidor, de la infraestructura de almacenamiento de ESXi y de los recursos específicos de virtualización. Estos proveedores operan en el sistema ESXi y, por lo tanto, su diseño es extremadamente ligero y se centra en tareas de administración específicas. El agente CIM recibe información de todos los proveedores CIM y la presenta al mundo exterior mediante las API estándar, de las cuales la más frecuente es WS-MAN.

No proporcione credenciales de raíz a aplicaciones remotas para acceder a la interfaz de CIM. En lugar de eso, cree una cuenta de servicio específica para estas aplicaciones y otorgue acceso de solo lectura a la información de CIM a cualquier cuenta local que figure en el sistema ESXi, así como a cualquier función establecida en vCenter Server.

## Procedimiento

- 1 Cree una cuenta de servicio específica para las aplicaciones de CIM.
- 2 Otorgue acceso de solo lectura a la información de CIM a cualquier cuenta local que figure en el sistema ESXi, así como a cualquier función establecida en vCenter Server.
- 3 (opcional) Si la aplicación requiere acceso de escritura en la interfaz de CIM, cree una función que se aplique a la cuenta de servicio únicamente con dos privilegios:
  - **Host.Configuración.Administración del sistema**
  - **Host.CIM.Interacción con CIM**

Esta función puede ser local para el host o establecerse de forma central en vCenter Server, según cómo funcione la aplicación de supervisión.

## Resultados

Cuando un usuario inicia sesión en el host con la cuenta de servicio que se creó para las aplicaciones de CIM, el usuario solo tiene los privilegios **Administración del sistema** e **Interacción con CIM**, o bien acceso de solo lectura.

# Proteger máquinas virtuales

# 7

El sistema operativo invitado que se ejecuta en la máquina virtual está sujeto a los mismos riesgos de seguridad que un sistema físico. Proteja las máquinas virtuales del mismo modo en que protege a las máquinas físicas.

Este capítulo incluye los siguientes temas:

- Limitación de los mensajes informativos de máquinas virtuales a archivos VMX
- Evitar la reducción de discos virtuales
- Prácticas recomendadas de seguridad para las máquinas virtuales

## Limitación de los mensajes informativos de máquinas virtuales a archivos VMX

Limite los mensajes informativos de la máquina virtual al archivo VMX para evitar llenar el almacén de datos y provocar la denegación de servicio (DoS). La denegación de servicio se produce cuando no se controla el tamaño del archivo VMX de una máquina virtual y la cantidad de información supera la capacidad del almacén de datos.

El archivo de configuración que contiene los pares nombre-valor informativos está limitado a 1 MB de forma predeterminada. Esta capacidad es suficiente en la mayoría de los casos, pero es posible cambiar este valor si fuera necesario. Por ejemplo, puede aumentar el límite si se almacenan grandes cantidades de información personalizada en el archivo de configuración.

---

**Nota** Determine cuidadosamente la cantidad de información que necesita. Si la cantidad de información supera la capacidad del almacén de datos, puede producirse una denegación de servicio.

---

El límite predeterminado de 1 MB se aplica incluso cuando el parámetro `tools.setInfo.sizeLimit` no figura en la lista de opciones avanzadas.

### Procedimiento

- 1 Busque la máquina virtual en el inventario de vSphere Web Client.
  - a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host.
  - b Haga clic en la pestaña **Objetos relacionados** y en **Máquinas virtuales**.

- 2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.
- 3 Seleccione **Opciones de máquina virtual**.
- 4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.
- 5 Agregue o edite el parámetro `tools.setInfo.sizeLimit`.

## Evitar la reducción de discos virtuales

Los usuarios no administrativos del sistema operativo invitado pueden reducir discos virtuales. La reducción de un disco virtual recupera el espacio no utilizado en el disco. Sin embargo, si se reduce un disco virtual varias veces, el disco deja de estar disponible y provoca una denegación de servicio. Para evitar esto, deshabilite la capacidad para reducir discos virtuales.

### Requisitos previos

- Apague la máquina virtual.
- Compruebe si cuenta con privilegios de raíz o administrador en la máquina virtual.

### Procedimiento

- 1 Busque la máquina virtual en el inventario de vSphere Web Client.
  - a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host.
  - b Haga clic en la pestaña **Objetos relacionados** y en **Máquinas virtuales**.
- 2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.
- 3 Seleccione **Opciones de máquina virtual**.
- 4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.
- 5 Agregue o edite los siguientes parámetros.

Nombre	Valor
<code>isolation.tools.diskWiper.disable</code>	TRUE
<code>isolation.tools.diskShrink.disable</code>	TRUE

- 6 Haga clic en **Aceptar**.

### Resultados

Si se deshabilita esta característica, no se pueden reducir los discos de máquinas virtuales cuando un almacén de datos se queda sin espacio.

# Prácticas recomendadas de seguridad para las máquinas virtuales

Seguir las prácticas recomendadas de seguridad para las máquinas virtuales ayuda a garantizar la integridad de la implementación de vSphere.

## ■ Protección general de la máquina virtual

La máquina virtual es, en muchos aspectos, el equivalente a un servidor físico. Implemente las mismas medidas de seguridad en las máquinas virtuales que las que implementa en los sistemas físicos.

## ■ Usar plantillas para implementar máquinas virtuales

Cuando instala manualmente sistemas operativos invitados y aplicaciones en una máquina virtual, se introduce el riesgo de una configuración incorrecta. Mediante el uso de una plantilla que captura la imagen del sistema operativo base, protegido, sin aplicaciones instaladas, es posible garantizar que todas las máquinas virtuales se creen con un nivel de línea base conocido de seguridad.

## ■ Minimizar el uso de la consola de máquina virtual

La consola de máquina virtual cumple la misma función en la máquina virtual que el monitor de un servidor físico. Los usuarios con acceso a la consola de máquina virtual tienen acceso a controles de conectividad de dispositivos extraíbles y de administración de energía de la máquina virtual, lo cual puede permitir un ataque malicioso en la máquina virtual.

## ■ Evitar que las máquinas virtuales asuman el control de los recursos

Cuando una máquina virtual consume tantos recursos del host que las demás máquinas virtuales presentes en el host no pueden realizar sus respectivas funciones, es posible que se produzca una denegación de servicio (DoS). Para evitar que una máquina virtual provoque una DoS, use las características de administración de recursos del host, como los recursos compartidos de configuración y los grupos de recursos.

## ■ Deshabilitar funciones innecesarias en máquinas virtuales

Cualquier servicio que se esté ejecutando en una máquina virtual conlleva un potencial ataque. Al deshabilitar los componentes del sistema que no son necesarios para admitir la aplicación o el servicio que están en ejecución en el sistema, se reduce la cantidad de componentes que pueden recibir ataques.

## Protección general de la máquina virtual

La máquina virtual es, en muchos aspectos, el equivalente a un servidor físico. Implemente las mismas medidas de seguridad en las máquinas virtuales que las que implementa en los sistemas físicos.

Siga estas prácticas recomendadas para proteger la máquina virtual:

### Revisiones y otros tipos de protección

Mantenga todas las medidas de seguridad actualizadas, incluidas las revisiones adecuadas. Es fundamental realizar un seguimiento de las actualizaciones para las máquinas virtuales inactivas que están apagadas, ya que podrían pasarse por alto. Por ejemplo, asegúrese de que el software antivirus, el software antispyware, la detección de intrusos y otros tipos de protección estén habilitados para cada máquina virtual de la infraestructura virtual. También debe asegurarse de que tiene suficiente espacio para los registros de las máquinas virtuales.

### **Análisis antivirus**

Debido a que las máquinas virtuales alojan un sistema operativo estándar, se deben proteger contra virus con un software antivirus. Según cómo utilice la máquina virtual, es posible que también sea necesario instalar un firewall de software.

Escalone la programación de análisis de virus, particularmente en las implementaciones que tengan gran cantidad de máquinas virtuales. El rendimiento de los sistemas en el entorno disminuye notablemente si examina todas las máquinas virtuales a la vez. Como los firewalls de software y los software antivirus pueden tener un gran consumo de la capacidad de virtualización, equilibre el uso de estas dos medidas de seguridad según el rendimiento de las máquinas virtuales, en especial si sabe que las máquinas virtuales están en un entorno de plena confianza.

### **Puertos serie**

Los puertos serie son interfaces para conectar periféricos con la máquina virtual. Se utilizan a menudo en sistemas físicos para proporcionar una conexión directa y de bajo nivel con la consola de un servidor. El puerto serie virtual permite el mismo acceso a una máquina virtual. Los puertos serie permiten el acceso de bajo nivel, que por lo general no tiene un control estricto como el registro o los privilegios.

## **Usar plantillas para implementar máquinas virtuales**

Cuando instala manualmente sistemas operativos invitados y aplicaciones en una máquina virtual, se introduce el riesgo de una configuración incorrecta. Mediante el uso de una plantilla que captura la imagen del sistema operativo base, protegido, sin aplicaciones instaladas, es posible garantizar que todas las máquinas virtuales se creen con un nivel de línea base conocido de seguridad.

Puede utilizar plantillas que contengan un sistema operativo protegido, revisado y adecuadamente configurado para crear otras plantillas específicas de la aplicación, o bien puede utilizar la plantilla de la aplicación para implementar máquinas virtuales.

### Procedimiento

- ◆ Proporcione plantillas para la creación de máquinas virtuales que contengan implementaciones de sistemas operativos protegidos, revisados y adecuadamente configurados.

De ser posible, también implemente aplicaciones en las plantillas. Asegúrese de que las aplicaciones no dependan de la información específica de la máquina virtual para poder implementarlas.

### Pasos siguientes

Para obtener más información sobre las plantillas, consulte la documentación de *Administración de máquinas virtuales de vSphere*.

## Minimizar el uso de la consola de máquina virtual

La consola de máquina virtual cumple la misma función en la máquina virtual que el monitor de un servidor físico. Los usuarios con acceso a la consola de máquina virtual tienen acceso a controles de conectividad de dispositivos extraíbles y de administración de energía de la máquina virtual, lo cual puede permitir un ataque malicioso en la máquina virtual.

### Procedimiento

- 1 Utilice servicios nativos de administración remota, como servicios de terminal y SSH, para interactuar con las máquinas virtuales.

Otorgue acceso a la consola de máquina virtual solo cuando sea necesario.

- 2 Limite las conexiones a la consola a la menor cantidad posible.

Por ejemplo, en un entorno muy seguro, límitela a una conexión. En algunos entornos, se puede incrementar el límite según cuántas conexiones simultáneas se necesiten para realizar las tareas normales.

## Evitar que las máquinas virtuales asuman el control de los recursos

Cuando una máquina virtual consume tantos recursos del host que las demás máquinas virtuales presentes en el host no pueden realizar sus respectivas funciones, es posible que se produzca una denegación de servicio (DoS). Para evitar que una máquina virtual provoque una DoS, use las características de administración de recursos del host, como los recursos compartidos de configuración y los grupos de recursos.

De forma predeterminada, todas las máquinas virtuales de un host ESXi comparten los recursos de forma equitativa. Puede utilizar los recursos compartidos y los grupos de recursos para evitar un ataque por denegación de servicio que haga que una máquina virtual consuma tantos recursos del host que las demás máquinas virtuales del mismo host no puedan realizar sus respectivas funciones.

No use los límites a menos que conozca por completo los efectos que tienen.



**Procedimiento**

- 1 Aprovechne cada máquina virtual solo con los recursos (CPU y memoria) suficientes para que funcione de forma adecuada.
- 2 Utilice los recursos compartidos para garantizar que las máquinas virtuales fundamentales tengan los recursos necesarios.
- 3 Agrupe las máquinas virtuales con requisitos similares en grupos de recursos.
- 4 En cada grupo de recursos, deje la opción de recursos compartidos con los valores predeterminados para que cada máquina virtual del grupo tenga aproximadamente la misma prioridad de recursos.

Con esta configuración, una máquina virtual individual no puede usar más recursos que las demás máquinas virtuales del grupo de recursos.

**Pasos siguientes**

Consulte la documentación de *Administración de recursos de vSphere* para obtener información sobre recursos compartidos y límites.

**Deshabilitar funciones innecesarias en máquinas virtuales**

Cualquier servicio que se esté ejecutando en una máquina virtual conlleva un potencial ataque. Al deshabilitar los componentes del sistema que no son necesarios para admitir la aplicación o el servicio que están en ejecución en el sistema, se reduce la cantidad de componentes que pueden recibir ataques.

Las máquinas virtuales no suelen precisar tantos servicios o tantas funciones como los servidores físicos. A la hora de virtualizar un sistema, evalúe si es necesario ese servicio o esa función en particular.

**Procedimiento**

- ◆ Deshabilite los servicios que no se utilizan en el sistema operativo.  
Por ejemplo, si el sistema ejecuta un servidor de archivos, desconecte los servicios web.
- ◆ Desconecte los dispositivos físicos que no se utilizan, como unidades de CD/DVD, unidades de disquete y adaptadores USB.
- ◆ Deshabilite las funcionalidades que no se utilizan, como las características de visualización o de sistema de archivos invitado del host (HGFS).
- ◆ Apague los protectores de pantalla.
- ◆ No ejecute el sistema X Window en los sistemas operativos invitados Linux, BSD o Solaris a menos que sea necesario.

**Quitar dispositivos de hardware innecesarios**

Todo dispositivo habilitado o conectado constituye un canal de ataque potencial. Los usuarios y los procesos sin privilegios sobre una máquina virtual pueden conectar o desconectar dispositivos

de hardware, como adaptadores de red o unidades de CD-ROM. Los atacantes pueden usar esta funcionalidad para infringir la seguridad de la máquina virtual. La eliminación de los dispositivos de hardware innecesarios permite evitar ataques.

Un atacante con acceso a una máquina virtual puede conectar un dispositivo de hardware desconectado y acceder a información confidencial en los soportes físicos olvidados en la unidad, o bien puede desconectar un adaptador de red para aislar a la máquina virtual de la red, lo cual puede provocar una denegación de servicio.

- Asegúrese de que no queden dispositivos sin autorización conectados y extraiga los dispositivos de hardware que no se necesiten o no se usen.
- Deshabilite los dispositivos virtuales innecesarios desde una máquina virtual.
- Asegúrese de que no quede ningún dispositivo conectado a una máquina virtual si no es necesario. En un centro de datos, es poco común que se usen los puertos serie y paralelos para las máquinas virtuales, y las unidades de CD/DVD suelen conectarse únicamente de manera temporal durante la instalación de software.

#### Procedimiento

- 1 Inicie sesión en un sistema vCenter Server a través de vSphere Web Client.
- 2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.
- 3 Revise cada dispositivo de hardware y compruebe si desea mantenerlo conectado.

Compruebe también los siguientes dispositivos:

- Unidades de disquete
- Puertos serie
- Puertos paralelos
- controladoras USB
- unidades de CD-ROM

#### Deshabilitar las características de visualización que no se utilizan

Los atacantes pueden aprovechar una característica de visualización que no se utiliza para introducir un código malicioso en el entorno. Deshabilite las características que no se estén utilizando en el entorno.

#### Procedimiento

- 1 Busque la máquina virtual en el inventario de vSphere Web Client.
  - a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host.
  - b Haga clic en la pestaña **Objetos relacionados** y en **Máquinas virtuales**.
- 2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

- 3 Seleccione **Opciones de máquina virtual**.
- 4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.
- 5 Si corresponde, agregue o edite los siguientes parámetros según el caso.

Opción	Descripción
<code>svga.vgaonly</code>	Si establece este parámetro en el valor TRUE, las funciones avanzadas de gráficos dejarán de funcionar. Solo estará disponible el modo de consola de celda con caracteres. Si utiliza esta configuración, <code>mks.enable3d</code> no tendrá efecto.  <b>Nota</b> Aplique esta configuración únicamente a las máquinas virtuales que no necesitan una tarjeta de vídeo virtualizada.
<code>mks.enable3d</code>	Establezca este parámetro en el valor FALSE en las máquinas virtuales que no necesitan la funcionalidad 3D.

## Deshabilitar características no expuestas

Las máquinas virtuales VMware están diseñadas para funcionar tanto con sistemas vSphere como con plataformas de virtualización alojadas como Workstation y Fusion. Algunos parámetros de la máquina virtual no necesitan estar habilitados para ejecutar una máquina virtual en un sistema vSphere. Deshabilite estos parámetros para reducir las vulnerabilidades posibles.

### Requisitos previos

Apague la máquina virtual.

### Procedimiento

- 1 Busque la máquina virtual en el inventario de vSphere Web Client.
  - a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host.
  - b Haga clic en la pestaña **Objetos relacionados** y en **Máquinas virtuales**.
- 2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.
- 3 Seleccione **Opciones de máquina virtual**.
- 4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.
- 5 Agregue o edite los siguientes parámetros para establecerlos en el valor TRUE.
  - `isolation.tools.unity.push.update.disable`
  - `isolation.tools.ghi.launchmenu.change`
  - `isolation.tools.memSchedFakeSampleStats.disable`
  - `isolation.tools.getCreds.disable`
  - `isolation.tools.ghi.autologon.disable`

- `isolation.bios.bbs.disable`
- `isolation.tools.hgfsServerSet.disable`

6 Haga clic en **Aceptar**.

## Deshabilitar transferencias de archivos por HGFS

Algunas operaciones, como las actualizaciones de herramientas automatizadas, utilizan un componente en el hipervisor que se conoce como sistema de archivos invitado del host (HGFS). En entornos de seguridad alta, es posible deshabilitar este componente para minimizar el riesgo de que un atacante utilice HGFS para transferir archivos dentro del sistema operativo invitado.

### Procedimiento

- 1 Busque la máquina virtual en el inventario de vSphere Web Client.
  - a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host.
  - b Haga clic en la pestaña **Objetos relacionados** y en **Máquinas virtuales**.
- 2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.
- 3 Seleccione **Opciones de máquina virtual**.
- 4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.
- 5 Compruebe que el parámetro `isolation.tools.hgfsServerSet.disable` esté establecido en TRUE.

### Resultados

Al hacer este cambio, el proceso de VMX ya no responde a los comandos del proceso de herramientas. Las API que utilizan HGFS para transferir archivos hacia y desde el sistema operativo invitado, como algunos comandos VIX o la utilidad de actualización automática VMware Tools, ya no funcionan.

## Deshabilitar las operaciones para copiar y pegar entre el sistema operativo invitado y la consola remota

Las operaciones para copiar y pegar entre el sistema operativo invitado y la consola remota están deshabilitadas de forma predeterminada. Para lograr un entorno seguro, conserve la configuración predeterminada. Si necesita utilizar las operaciones para copiar y pegar, debe habilitarlas por medio de vSphere Web Client.

De forma predeterminada, estas opciones están establecidas en el valor recomendado. Sin embargo, debe establecerlas en True de forma explícita si desea habilitar herramientas de auditoría para comprobar si la configuración es correcta.

### Requisitos previos

Apague la máquina virtual.

**Procedimiento**

- 1 Inicie sesión en un sistema vCenter Server a través de vSphere Web Client.
- 2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.
- 3 Haga clic en **Opciones de máquina virtual** y en **Editar configuración**.
- 4 Asegúrese de que los siguientes valores estén en las columnas Nombre y Valor o haga clic en **Agregar fila** para agregarlos.

Nombre	Valor recomendado
isolation.tools.copy.disable	true
isolation.tools.paste.disable	true
isolation.tools.setGUIOptions.enable	false

Estas opciones anulan la configuración realizada en el panel de control de VMware Tools del sistema operativo invitado.

- 5 Haga clic en **Aceptar**.
- 6 (opcional) Si realizó cambios en los parámetros de configuración, reinicie la máquina virtual.

**Limitar la exposición de los datos confidenciales copiados al portapapeles**

De forma predeterminada, las operaciones para copiar y pegar están deshabilitadas para los hosts a fin de evitar la exposición de los datos confidenciales que se copiaron al portapapeles.

Cuando la función copiar y pegar está habilitada en una máquina virtual que ejecuta VMware Tools, se pueden copiar y pegar elementos entre el sistema operativo invitado y la consola remota. Una vez que la ventana de la consola entra en foco, los usuarios sin privilegios y los procesos que se ejecutan en la máquina virtual pueden acceder al portapapeles de la consola de la máquina virtual. Si un usuario copia información confidencial en el portapapeles antes de utilizar la consola, expone (quizás sin saberlo) datos confidenciales a la máquina virtual. Para evitar este problema, las operaciones para copiar y pegar del sistema operativo invitado están deshabilitadas de forma predeterminada.

De ser necesario, es posible habilitarlas para las máquinas virtuales.

**Restringir la ejecución de comandos dentro de una máquina virtual a los usuarios**

De forma predeterminada, un usuario con función de administrador de vCenter Server puede interactuar con archivos y programas dentro del sistema operativo invitado de una máquina virtual. Para reducir el riesgo de infracciones de confidencialidad, disponibilidad o integridad del invitado, cree una función de acceso que no sea de invitado sin el privilegio **Operaciones de invitado**.

Por motivos de seguridad, aplique las mismas restricciones en los permisos de acceso al centro de datos virtual que en el centro de datos físico. Para evitar otorgar a los usuarios acceso total de administrador, cree una función personalizada que deshabilite el acceso de invitado y aplíquelo a los usuarios que requieren privilegios de administrador, pero que no están autorizados a interactuar con archivos y programas dentro de un sistema operativo invitado.

Por ejemplo, la configuración puede incluir una máquina virtual en la infraestructura que tenga información confidencial. Las tareas como la migración con vMotion y Storage vMotion requieren que la función de TI tenga acceso a la máquina virtual. En este caso, deshabilite algunas operaciones remotas dentro del sistema operativo invitado para garantizar que la función de TI no tenga acceso a la información confidencial.

#### Requisitos previos

Compruebe que tenga privilegios de **Administrador** en el sistema vCenter Server en el que crea la función.

#### Procedimiento

- 1 Inicie sesión en vSphere Web Client como un usuario con privilegios de **Administrador** en el sistema vCenter Server donde creará la función.
- 2 Haga clic en **Administración** y seleccione **Funciones**.
- 3 Haga clic en el icono **Crear acción de función** y escriba un nombre de la función.  
Por ejemplo, escriba **Administrator No Guest Access**.
- 4 Seleccione **Todos los privilegios**.
- 5 Anule la selección de **Todos los privilegios.Máquina virtual.Operaciones de invitado** para quitar el conjunto de privilegios Operaciones de invitado.
- 6 Haga clic en **Aceptar**.

#### Pasos siguientes

Seleccione el sistema vCenter Server o el host, y asigne un permiso que se asocie con el usuario o el grupo que debe tener los nuevos privilegios con la función recién creado. Quite esos usuarios de la función de administrador predeterminado.

### Evitar que un usuario o proceso de máquina virtual desconecten dispositivos

Los usuarios y los procesos sin privilegios de raíz o administrador en máquinas virtuales tienen la capacidad de conectar o desconectar dispositivos, como adaptadores de red y unidades de CD-ROM, y de modificar la configuración de dispositivos. Para mejorar la seguridad de la máquina virtual, quite estos dispositivos. Si no desea quitar un dispositivo de forma permanente, puede evitar que un usuario o proceso de máquina virtual conecten o desconecten el dispositivo desde dentro del sistema operativo invitado.

#### Requisitos previos

Apague la máquina virtual.

**Procedimiento**

- 1 Busque la máquina virtual en el inventario de vSphere Web Client.
  - a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host.
  - b Haga clic en la pestaña **Objetos relacionados** y en **Máquinas virtuales**.
- 2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.
- 3 Seleccione **Opciones de máquina virtual**.
- 4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.
- 5 Compruebe que los siguientes valores estén en las columnas Nombre y Valor, o haga clic en **Agregar fila** para agregarlos.

Nombre	Valor
isolation.device.connectable.disable	true
isolation.device.edit.disable	true

Estas opciones anulan la configuración realizada en el panel de control de VMware Tools del sistema operativo invitado.

- 6 Haga clic en **Aceptar** para cerrar el cuadro de diálogo Parámetros de configuración y, a continuación, haga clic nuevamente en **Aceptar**.

**Modificar el límite de memoria variable del sistema operativo invitado**

Puede aumentar el límite de memoria variable del sistema operativo invitado si se almacenan grandes cantidades de información personalizada en el archivo de configuración.

**Requisitos previos**

Apague la máquina virtual.

**Procedimiento**

- 1 Busque la máquina virtual en el inventario de vSphere Web Client.
  - a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host.
  - b Haga clic en la pestaña **Objetos relacionados** y en **Máquinas virtuales**.
- 2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.
- 3 Seleccione **Opciones de máquina virtual > Opciones avanzadas** y haga clic en **Editar configuración**.
- 4 Agregue o edite el parámetro `tools.setInfo.sizeLimit`, y establezca el valor para la cantidad de bytes.
- 5 Haga clic en **Aceptar**.

## Evitar que los procesos del sistema operativo invitado envíen mensajes de configuración al host

Puede evitar que los sistemas operativos invitados escriban pares nombre-valor en el archivo de configuración. Esta acción es adecuada cuando se debe evitar que los sistemas operativos invitados modifiquen las opciones de configuración.

### Requisitos previos

Apague la máquina virtual.

### Procedimiento

- 1 Busque la máquina virtual en el inventario de vSphere Web Client.
  - a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host.
  - b Haga clic en la pestaña **Objetos relacionados** y en **Máquinas virtuales**.
- 2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.
- 3 Seleccione **Opciones de máquina virtual**.
- 4 Haga clic en **Opciones avanzadas** y en **Editar configuración**.
- 5 Haga clic en **Agregar fila** y escriba los siguientes valores en las columnas Nombre y Valor.
  - En la columna Nombre: **isolation.tools.setinfo.disable**
  - En la columna Valor: **true**
- 6 Haga clic en **Aceptar** para cerrar el cuadro de diálogo Parámetros de configuración y, a continuación, haga clic nuevamente en **Aceptar**.

## Evitar utilizar discos independientes no persistentes

Al utilizar discos independientes no persistentes, los atacantes exitosos pueden apagar o reiniciar el sistema y así eliminar cualquier evidencia de que la máquina fue vulnerada. Sin un registro persistente de la actividad de la máquina virtual, los administradores podrían desconocer el ataque. Por lo tanto, debe evitar utilizar discos independientes no persistentes.

### Procedimiento

- ◆ Asegúrese de que la actividad de la máquina virtual se registre de forma remota en un servidor separado, como un servidor syslog o un recopilador de eventos basado en Windows.
- Si el registro remoto de eventos y de actividad no está configurado para el invitado, el modo scsiX:Y. debe estar configurado de alguna de las siguientes formas:
- No presente
  - No establecido en independiente no persistente



## Resultados

Cuando el modo no persistente no está habilitado, no se puede revertir la máquina virtual a un estado conocido al reiniciar el sistema.

# Proteger las redes de vSphere

## 8

La protección de las redes de vSphere es una parte fundamental de la seguridad del entorno. Los diferentes componentes de vSphere se protegen de varias maneras. Consulte la documentación de *Redes de vSphere* para obtener información detallada sobre las redes del entorno de vSphere.

Este capítulo incluye los siguientes temas:

- Introducción a la seguridad de red de vSphere
- Proteger la red con firewalls
- Proteger el conmutador físico
- Proteger puertos de conmutadores estándar con directivas de seguridad
- Proteger conmutadores estándar de vSphere
- Proteger conmutadores distribuidos y grupos de puertos distribuidos de vSphere
- Proteger las máquinas virtuales con VLAN
- Crear una DMZ de una red en un único host ESXi
- Crear varias redes en un único host ESXi
- Seguridad del protocolo de Internet
- Garantizar la correcta configuración de SNMP
- Usar conmutadores virtuales con vSphere Network Appliance API solo cuando es necesario
- Prácticas recomendadas de seguridad de redes de vSphere

## Introducción a la seguridad de red de vSphere

La seguridad de red para el entorno de vSphere contiene muchas características similares a la protección de un entorno de red física, pero también incluye algunas otras que se aplican solamente a las máquinas virtuales.

### Firewalls

Agregue protección de firewall a la red virtual mediante la instalación y la configuración de firewalls basados en host en algunas o todas las máquinas virtuales.

Para mejorar la eficiencia, puede configurar redes virtuales o redes Ethernet de máquinas virtuales privadas. En las redes virtuales, se instala un firewall basado en host en una máquina virtual en el encabezado de la red virtual. Este firewall funciona como búfer de protección entre el adaptador de red físico y las máquinas virtuales restantes de la red virtual.

Dado que los firewalls basados en host también pueden disminuir el rendimiento, pondere las necesidades de seguridad y los objetivos de rendimiento antes de instalar firewalls basados en host en las máquinas virtuales de alguna otra parte de la red virtual.

Consulte [Proteger la red con firewalls](#).

## Segmentar

Mantenga las zonas de máquinas virtuales diferentes dentro de un host en distintos segmentos de red. Al aislar cada zona de máquinas virtuales en su propio segmento de red, es posible minimizar el riesgo de pérdidas de datos entre una zona y la siguiente. La segmentación evita diversas amenazas, como la suplantación de protocolo Address Resolution Protocol (ARP), por la cual un atacante manipula la tabla de ARP y reasigna direcciones MAC e IP con el fin de acceder al tráfico de red que entra y sale de un host. Los atacantes usan la suplantación de protocolo ARP para generar ataques de tipo "Man in the middle" (MITM), realizar ataques por denegación de servicio (DoS), secuestrar el sistema de destino y desestabilizar la red virtual de otras maneras.

Si la segmentación se planifica minuciosamente, se reducen las posibilidades de transmisiones de paquetes entre las zonas de máquinas virtuales. Esto evita los ataques de analizadores de protocolos (sniffer) que implican enviar tráfico de red a la víctima. Asimismo, un atacante no puede usar un servicio que no sea seguro en una zona de máquinas virtuales para acceder a otras zonas del host. El usuario puede elegir entre dos enfoques para implementar la segmentación. Cada enfoque aporta distintos beneficios.

- Use adaptadores de red físicos separados para las zonas de máquinas virtuales a fin de garantizar que las zonas queden aisladas. Probablemente, este es el método más seguro y menos proclive a producir errores de configuración después de la creación inicial del segmento.
- Configure redes de área local virtuales (VLAN) para ayudar a proteger la red. Dado que proporcionan casi todos los beneficios de seguridad inherentes a la implementación de redes físicamente separadas sin la sobrecarga de hardware, las VLAN representan una solución viable que permite evitar los costos de implementación y mantenimiento de dispositivos adicionales, cableado, etc. Consulte [Proteger las máquinas virtuales con VLAN](#).

## Evitar el acceso no autorizado

Si la red de máquinas virtuales está conectada a una red física, puede quedar expuesta a infracciones, al igual que una red compuesta de máquinas físicas. Aunque la red de máquinas virtuales esté aislada de la red física, las máquinas virtuales de la red pueden ser víctimas de ataques procedentes de otras máquinas virtuales de la red. Los requisitos para proteger las máquinas virtuales suelen ser los mismos que para proteger máquinas físicas.

Las máquinas virtuales permanecen aisladas unas de otras. Una máquina virtual no puede leer ni escribir la memoria de otra máquina virtual, acceder a sus datos, usar sus aplicaciones, etc. Sin embargo, dentro de la red, cualquier máquina virtual o grupo de máquinas virtuales puede continuar siendo objeto de acceso no autorizado desde otras máquinas virtuales y requerir más protección a través de medios externos.

## Proteger la red con firewalls

Los administradores de seguridad usan firewalls para proteger la red o los componentes seleccionados en la red de las intromisiones.

Los firewalls controlan el acceso a los dispositivos dentro de su perímetro mediante el cierre de todos los puertos, excepto los puertos que el administrador designa explícita o implícitamente como autorizados. Los puertos que el administrador abre permiten el tráfico entre dispositivos en diferentes lados del firewall.

---

**Importante** El firewall de ESXi en ESXi 5.5 y versiones posteriores no permite filtrar el tráfico de vMotion por red. Por lo tanto, se deben instalar reglas en el firewall externo para que no se puedan establecer conexiones entrantes con el socket de vMotion.

---

En un entorno de máquina virtual, se puede planear la distribución de los firewalls entre los componentes.

- Firewalls entre máquinas físicas, tales como los sistemas vCenter Server y los hosts ESXi.
- Los firewalls entre una máquina virtual y otra, por ejemplo, entre una máquina virtual que actúa como servidor web externo y una máquina virtual conectada a la red interna de la empresa.
- Firewalls entre una máquina física y una máquina virtual, como cuando se coloca un firewall entre una tarjeta de adaptador de red física y una máquina virtual.

El modo de usar firewalls en la configuración de ESXi depende de cómo se planea utilizar la red y qué tan seguro debe ser un componente determinado. Por ejemplo, si crea una red virtual en la que cada máquina virtual está dedicada a ejecutar un conjunto de pruebas de referencia diferente para el mismo departamento, el riesgo de que se produzca un acceso no deseado de una máquina virtual a la siguiente es mínimo. Por lo tanto, no se necesita una configuración en la que haya firewalls entre las máquinas virtuales. Sin embargo, para evitar la interrupción de la ejecución de una prueba por parte de un host externo, puede configurar un firewall en el punto de entrada de la red virtual a fin de proteger todo el conjunto de máquinas virtuales.

Para ver un diagrama de los puertos de firewall, consulte el artículo [2131180](#) de la base de conocimientos de VMware.

## Firewalls para configuraciones con vCenter Server

Si se accede a los hosts ESXi a través de vCenter Server, generalmente se protege vCenter Server con un firewall. El firewall ofrece una protección básica para la red.

Un firewall puede estar entre los clientes y vCenter Server. O bien, según la implementación, tanto vCenter Server como los clientes pueden estar detrás del firewall. Lo fundamental es que haya un firewall en lo que se considere un punto de entrada al sistema.

Para obtener una lista completa de puertos TCP y UDP, incluidos los correspondientes a vSphere vMotion™ y vSphere Fault Tolerance, consulte [Puertos TCP y UDP de vCenter Server](#).

Las redes configuradas con vCenter Server pueden recibir comunicaciones a través de vSphere Web Client o de clientes de administración de redes externos que usan el SDK como interfaz con el host. Durante un funcionamiento normal, vCenter Server escucha los datos de sus hosts y clientes administrados en los puertos designados. vCenter Server también asume que sus hosts administrados escuchan datos de vCenter Server en los puertos designados. Si hay un firewall entre cualquiera de estos elementos, el firewall debe tener puertos abiertos para admitir la transferencia de datos.

También se pueden incluir firewalls en otros puntos de acceso de la red diversos, según cómo se piense utilizar la red y el nivel de seguridad que requieran los diferentes dispositivos. Seleccione las ubicaciones de los firewalls según los riesgos de seguridad que haya identificado en la configuración de red. La siguiente es una lista de ubicaciones comunes de los firewalls en implementaciones de ESXi.

- Entre vSphere Web Client o un cliente de administración de redes externo y vCenter Server.
- Si sus usuarios acceden a las máquinas virtuales a través de un explorador web, entre el explorador web y el host ESXi.
- Si sus usuarios acceden a las máquinas virtuales a través de vSphere Web Client, entre vSphere Web Client y el host ESXi. Esta conexión es adicional a la conexión entre vSphere Web Client y vCenter Server, y requiere un puerto diferente.
- Entre vCenter Server y los hosts ESXi.
- Entre los hosts ESXi de la red. A pesar de que el tráfico entre hosts generalmente se considera confiable, puede agregar firewalls entre ellos si sospecha que hay infracciones de seguridad entre una máquina y la otra.

Si agrega firewalls entre los hosts ESXi y desea migrar máquinas virtuales entre los servidores, realizar una clonación o utilizar vMotion, también debe abrir puertos en todos los firewalls que dividan el host de origen de los hosts de destino, a fin de que el origen y los destinos puedan comunicarse.

- Entre los hosts ESXi y el almacenamiento de red, como el almacenamiento NFS o de iSCSI. Estos puertos no son exclusivos de VMware, y se configuran de acuerdo con las especificaciones de la red.

## Conexión con vCenter Server mediante un firewall

vCenter Server usa el puerto TCP 443 para escuchar la transferencia de datos de sus clientes. Si se usa un firewall entre vCenter Server y sus clientes, es necesario configurar una conexión a través de la cual vCenter Server pueda recibir los datos de sus clientes.

Abra el puerto TCP 443 en el firewall para que vCenter Server pueda recibir datos de vSphere Web Client. La configuración del firewall depende de lo que se use en el sitio. Solicite información al administrador del sistema de firewall local.

Si no desea usar el puerto 443 como puerto de comunicación entre vSphere Web Client y vCenter Server, puede elegir otro puerto. Para eso, cambie la configuración de vCenter Server desde vSphere Web Client. Consulte la documentación de *Administración de vCenter Server y hosts*.

Si sigue usando vSphere Client, consulte la *documentación sobre la administración de vSphere con vSphere Client*.

## Firewalls para configuraciones sin vCenter Server

Puede conectar clientes directamente con su red de ESXi en lugar de usar vCenter Server.

Las redes que se configuran sin vCenter Server reciben comunicaciones a través de vSphere Client, una de las interfaces de la línea de comandos de vSphere, vSphere Web Services SDK, o clientes externos. En la gran mayoría, las necesidades del firewall son las mismas que cuando está vCenter Server presente, pero existen varias diferencias de claves.

- Tal como lo haría con configuraciones que incluyen vCenter Server, asegúrese de que haya un firewall presente para proteger su capa de ESXi o, según la configuración, sus clientes y su capa de ESXi. El firewall ofrece una protección básica para la red.
- La concesión de licencias en este tipo de configuración es parte del paquete de ESXi que instala en cada uno de los hosts. Ya que la concesión de licencias reside en el servidor, no se requiere otro servidor de licencias. Esto hace que no sea necesario un firewall entre el servidor de licencias y la red de ESXi.

Puede configurar los puertos del firewall con ESXCLI, vSphere Client o la reglas del firewall. Consulte [Configurar firewalls de ESXi](#).

## Conectar hosts ESXi mediante firewalls

Si tiene un firewall entre dos hosts ESXi y desea permitir transacciones entre ellos o utilizar vCenter Server para realizar cualquier actividad en el origen o el destino, como tráfico de vSphere High Availability (vSphere HA), migración, clonación o vMotion, debe configurar una conexión mediante la cual los hosts administrados puedan recibir datos.

Para configurar una conexión a fin de recibir datos, abra los puertos para el tráfico proveniente de los servicios, como vSphere High Availability, vMotion y vSphere Fault Tolerance. Consulte [Configurar firewalls de ESXi](#) para ver una explicación de los archivos de configuración, del acceso de vSphere Web Client y de los comandos de firewall. Consulte [Puertos de firewall entrantes y salientes para hosts de ESXi](#) para obtener una lista de los puertos. Solicite más información sobre cómo configurar puertos al administrador del sistema de firewall.

## Conectar con la consola de la máquina virtual mediante un firewall

Algunos puertos deben estar abiertos para que el usuario y el administrador se comuniquen con la consola de la máquina virtual. Los puertos que deben estar abiertos dependen del tipo de consola

de máquina virtual y de si se establece la conexión mediante vCenter Server con vSphere Web Client o directamente con el host ESXi desde vSphere Client.

## Conectarse a una consola de máquina virtual basada en explorador mediante vSphere Web Client

Cuando se conecta con vSphere Web Client, se conecta siempre al sistema vCenter Server que administra el host ESXi, y se accede desde allí a la consola de máquina virtual.

Si utiliza vSphere Web Client y se conecta a una consola de máquina virtual basada en explorador, el acceso siguiente debe ser posible:

- El firewall debe permitir que vSphere Web Client acceda a vCenter Server en el puerto 9443.
- El firewall debe permitir que vCenter Server acceda al host ESXi en el puerto 902.

## Conectarse a una consola de máquina virtual independiente mediante vSphere Web Client

Si utiliza vSphere Web Client y se conecta a una consola de máquina virtual independiente, el acceso siguiente debe ser posible:

- El firewall debe permitir que vSphere Web Client acceda a vCenter Server en el puerto 9443.
- El firewall debe permitir que la consola de máquina virtual independiente acceda a vCenter Server en el puerto 9443 y al host ESXi en el puerto 902.

## Conectar con los hosts ESXi directamente con vSphere Client

Es posible utilizar la consola de máquina virtual de vSphere Client si se conecta directamente al host ESXi.

---

**Nota** No utilice vSphere Client para conectarse directamente a hosts administrados por el sistema vCenter Server. Si hace cambios en esos hosts desde vSphere Client, se producirá una inestabilidad en el entorno.

---

El firewall debe permitir el acceso al host ESXi en los puertos 443 y 902

vSphere Client utiliza el puerto 902 para ofrecer una conexión de las actividades de MKS del sistema operativo invitado en las máquinas virtuales. A través de este puerto, los usuarios interactúan con los sistemas operativos invitados y las aplicaciones de la máquina virtual. VMware no admite la configuración de otro puerto para esta función.

## Proteger el conmutador físico

Proteja el conmutador físico de cada host ESXi para evitar que los atacantes tengan acceso al host y sus máquinas virtuales.

Para optimizar la protección de los hosts, compruebe que los puertos de conmutadores físicos estén configurados con el árbol de expansión deshabilitado, y que la opción de no negociación esté configurada para los vínculos troncales entre conmutadores físicos externos y conmutadores virtuales en el modo de etiquetado de conmutador virtual (VST).

#### Procedimiento

- 1 Inicie sesión en el conmutador físico y compruebe que el protocolo de árbol de expansión esté deshabilitado o que Port Fast esté configurado para todos los puertos de conmutadores físicos conectados a los hosts ESXi.
- 2 Para las máquinas virtuales que hacen puente y enrutamiento, compruebe periódicamente que el primer puerto de conmutador físico ascendente esté configurado con las opciones BPDU Guard y Port Fast deshabilitadas, y con el protocolo de árbol de expansión habilitado.

En vSphere 5.1 y versiones posteriores, para evitar ataques potenciales de denegación de servicio (DoS) en el conmutador físico, puede activar el filtro de BPDU invitado en los hosts ESXi.

- 3 Inicie sesión en el conmutador físico y asegúrese de que el protocolo Dynamic Trunking Protocol (DTP) no esté habilitado en los puertos de conmutadores físicos conectados a los hosts ESXi.
- 4 De forma regular, revise los puertos de conmutadores físicos para asegurarse de que estén correctamente configurados como puertos troncales si están conectados a los puertos de enlace troncal de VLAN de conmutadores virtuales.

## Proteger puertos de conmutadores estándar con directivas de seguridad

Al igual que con los adaptadores de red físicos, un adaptador de red de máquina virtual puede enviar tramas que parecen pertenecer a una máquina diferente, o suplantar a otra máquina para poder recibir las tramas de red destinadas a la máquina original. Además, al igual que los adaptadores de red físicos, un adaptador de red de máquina virtual puede configurarse para que reciba tramas destinadas a otras máquinas. Ambos casos presentan un riesgo de seguridad.

Al crear un conmutador estándar para la red, se agregan grupos de puertos a vSphere Web Client con el fin de establecer una directiva para las máquinas virtuales y los adaptadores VMkernel del tráfico del sistema asociados al conmutador.

Al agregar un grupo de puertos VMkernel o un grupo de puertos de máquinas virtuales a un conmutador estándar, ESXi configura una directiva de seguridad para los puertos del grupo. Esta directiva de seguridad se puede utilizar para garantizar que el host evite que los sistemas operativos invitados de sus máquinas virtuales suplanten a otras máquinas en la red. Esta característica de seguridad se implementa de modo tal que el sistema operativo invitado responsable de realizar la suplantación no detecte que se evitó la suplantación.



La directiva de seguridad determina el nivel de seguridad con que se aplica la protección contra ataques de suplantación o interceptación en máquinas virtuales. Para utilizar la configuración del perfil de seguridad de forma correcta, es necesario comprender el modo en que los adaptadores de red de las máquinas virtuales controlan las transmisiones y la forma en que se producen los ataques en este nivel. Consulte la sección Directiva de seguridad en la publicación *Redes de vSphere*.

## Proteger conmutadores estándar de vSphere

Puede proteger el tráfico de un conmutador estándar contra ataques de Capa 2. Para ello, restrinja algunos de los modos de la dirección MAC por medio de la configuración de seguridad de los conmutadores.

Cada adaptador de red de máquina virtual tiene una dirección MAC inicial y una dirección MAC efectiva.

### Dirección MAC inicial

La dirección MAC inicial se asigna con la creación del adaptador. Si bien la dirección MAC inicial puede volver a configurarse desde afuera del sistema operativo invitado, este sistema no puede modificarla.

### Dirección MAC efectiva

Cada adaptador tiene una dirección MAC efectiva que filtra el tráfico de red entrante con una dirección MAC de destino distinta de la dirección MAC efectiva. El sistema operativo invitado es responsable de configurar la dirección MAC efectiva y, por lo general, hace coincidir la dirección MAC efectiva con la dirección MAC inicial.

Al crear un adaptador de red de máquina virtual, la dirección MAC efectiva y la dirección MAC inicial son iguales. El sistema operativo invitado puede modificar la dirección MAC efectiva con otro valor en cualquier momento. Si el sistema operativo modifica la dirección MAC efectiva, su adaptador de red recibe el tráfico de red destinado para la nueva dirección MAC.

Cuando se envían paquetes a través del adaptador de red, el sistema operativo invitado por lo general coloca su propia dirección MAC efectiva de adaptador en el campo de la dirección MAC de origen de las tramas Ethernet. Coloca la dirección MAC del adaptador de red receptor en el campo de la dirección MAC de destino. El adaptador receptor acepta los paquetes únicamente si la dirección MAC de destino del paquete coincide con su propia dirección MAC efectiva.

El sistema operativo puede enviar tramas con una dirección MAC de origen suplantada. Esto significa que el sistema operativo puede aplicar por etapas ataques maliciosos en los dispositivos de una red al suplantar un adaptador de red que la red receptora autoriza.

Puede proteger el tráfico virtual contra ataques de suplantación e interceptación de la Capa 2 si configura una directiva de seguridad en los puertos o grupos de puertos.

La directiva de seguridad en los puertos y grupos de puertos distribuidos incluye las siguientes opciones:

- Modo promiscuo (consulte [Operación en modo promiscuo](#)).
- Cambios en la dirección MAC (consulte [Cambios de dirección MAC](#)).
- Transmisiones falsificadas (consulte [Transmisiones falsificadas](#)).

Puede ver y cambiar la configuración predeterminada si selecciona el conmutador virtual asociado con el host desde vSphere Web Client. Consulte la documentación de *Redes de vSphere*.

## Cambios de dirección MAC

La directiva de seguridad de un conmutador virtual incluye la opción **Cambios de dirección MAC**. Esta opción afecta el tráfico que recibe una máquina virtual.

Cuando la opción **Cambios de dirección MAC** está establecida en **Aceptar**, ESXi acepta las solicitudes de cambiar la dirección MAC efectiva por una dirección diferente a la inicial.

Cuando la opción **Cambios de dirección MAC** está establecida en **Rechazar**, ESXi no admite las solicitudes de cambiar la dirección MAC efectiva por una dirección diferente a la inicial. Esta configuración protege el host de la suplantación de MAC. El puerto que utilizó el adaptador de la máquina virtual para enviar la solicitud se deshabilita, y el adaptador de la máquina virtual no recibe más tramas hasta que la dirección MAC efectiva coincida con la dirección MAC inicial. El sistema operativo invitado no detecta el rechazo de la solicitud de cambio de dirección MAC.

---

**Nota** El iniciador iSCSI confía en poder obtener los cambios en la dirección MAC a partir de determinados tipos de almacenamiento. Si utiliza iSCSI de ESXi con almacenamiento iSCSI, establezca la opción **Cambios de dirección MAC** en **Aceptar**.

---

En ciertos casos, es posible que realmente necesite que más de un adaptador tenga la misma dirección MAC en una red (por ejemplo, si utiliza el equilibrio de carga de red de Microsoft en modo de unidifusión). Cuando el equilibrio de carga de red de Microsoft se utiliza en el modo de multidifusión estándar, los adaptadores no comparten las direcciones MAC.

## Transmisiones falsificadas

La opción **Transmisiones falsificadas** afecta el tráfico que se transmite desde una máquina virtual.

Cuando la opción **Transmisiones falsificadas** está establecida en **Aceptar**, ESXi no compara las direcciones MAC de origen y efectivas.

Para evitar la suplantación de MAC, puede establecer la opción **Transmisiones falsificadas** en **Rechazar**. Si lo hace, el host compara la dirección MAC de origen que transmite el sistema operativo invitado con la dirección MAC efectiva de su adaptador de máquina virtual para ver si coinciden. Si las direcciones no coinciden, el host ESXi descarta el paquete.

El sistema operativo invitado no detecta que su adaptador de máquina virtual no puede enviar paquetes con la dirección MAC suplantada. El host ESXi intercepta los paquetes con direcciones suplantadas antes de que estos se envíen, y el sistema operativo invitado puede asumir que los paquetes se descartan.

## Operación en modo promiscuo

El modo promiscuo quita el filtrado de recepción que realiza el adaptador de la máquina virtual a fin de que el sistema operativo invitado reciba todo el tráfico que se observa en la conexión. De forma predeterminada, el adaptador de la máquina virtual no puede operar en modo promiscuo.

A pesar de que el modo promiscuo puede ser útil para hacer un seguimiento de la actividad de la red, es un modo de operación no seguro, ya que cualquier adaptador en modo promiscuo tiene acceso a los paquetes, incluso si algunos de estos paquetes se reciben solamente en un adaptador de red en particular. Esto significa que un administrador o un usuario raíz que estén en una máquina virtual pueden ver potencialmente el tráfico destinado a otros sistemas operativos host o invitados.

---

**Nota** En ciertas ocasiones, es posible que tenga una razón válida para configurar un conmutador virtual estándar o distribuido para operar en modo promiscuo, por ejemplo, si está ejecutando un software de detección de intrusiones de red o un analizador de protocolos (sniffer).

---

## Proteger conmutadores distribuidos y grupos de puertos distribuidos de vSphere

Los administradores tienen varias opciones para proteger a vSphere Distributed Switch en su entorno de vSphere.

### Procedimiento

- 1 Para los grupos de puertos distribuidos con enlace estático, compruebe que la característica Expansión automática esté deshabilitada.

Expansión automática está habilitada de forma predeterminada en vSphere 5.1 y versiones posteriores.

Para habilitar Expansión automática, configure la propiedad `autoExpand` en el grupo de puertos distribuidos con vSphere Web Services SDK o con una interfaz de línea de comandos. Consulte la documentación de *vSphere Web Services SDK*.

- 2 Asegúrese de que todos los identificadores de VLAN privadas de vSphere Distributed Switch estén documentados detalladamente.

- 3 Si utiliza el etiquetado de VLAN en un dvPortgroup, los identificadores de VLAN deben coincidir con los identificadores de los conmutadores ascendentes externos con reconocimiento de VLAN. Si no se hace un seguimiento completo de los identificadores de VLAN, la reutilización de identificadores por error puede producir tráfico entre las máquinas virtuales y físicas inadecuadas. De forma similar, la presencia de identificadores de VLAN incorrectos o faltantes puede hacer que el tráfico no pase entre las máquinas físicas y virtuales.
- 4 Asegúrese de que no haya puertos sin utilizar en un grupo de puertos virtuales asociado con vSphere Distributed Switch.
- 5 Etiquete todos los conmutadores distribuidos de vSphere.

Los conmutadores vSphere Distributed Switch asociados con un host ESXi requieren un campo para sus nombres. Esta etiqueta sirve como descriptor funcional del conmutador, al igual que el nombre de host asociado con un conmutador físico. La etiqueta de vSphere Distributed Switch indica la función o la subred IP del conmutador. Por ejemplo, puede etiquetar el conmutador como interno para indicar que sirve solo para las redes internas del conmutador virtual privado de una máquina virtual sin adaptadores de red físicos enlazados.

- 6 Deshabilite la comprobación de estado de la red en los conmutadores vSphere Distributed Switch si no la utiliza de forma activa.

La comprobación de estado de la red está deshabilitada de forma predeterminada. Una vez habilitados, los paquetes de comprobación de estado contienen información sobre el host, el conmutador y el puerto que un atacante podría utilizar. Utilice la comprobación de estado de la red solo para tareas de solución de problemas y desactívela al finalizar.

- 7 Puede proteger el tráfico virtual contra ataques de suplantación e interceptación de la Capa 2 si configura una directiva de seguridad en los puertos o grupos de puertos.

La directiva de seguridad en los puertos y grupos de puertos distribuidos incluye las siguientes opciones:

- Modo promiscuo (consulte [Operación en modo promiscuo](#)).
- Cambios en la dirección MAC (consulte [Cambios de dirección MAC](#)).
- Transmisiones falsificadas (consulte [Transmisiones falsificadas](#)).

Para ver y cambiar la configuración actual, seleccione **Administrar grupos de puertos distribuidos** en el menú contextual y, a continuación, seleccione **Seguridad** en el asistente. Consulte la documentación de *Redes de vSphere*.

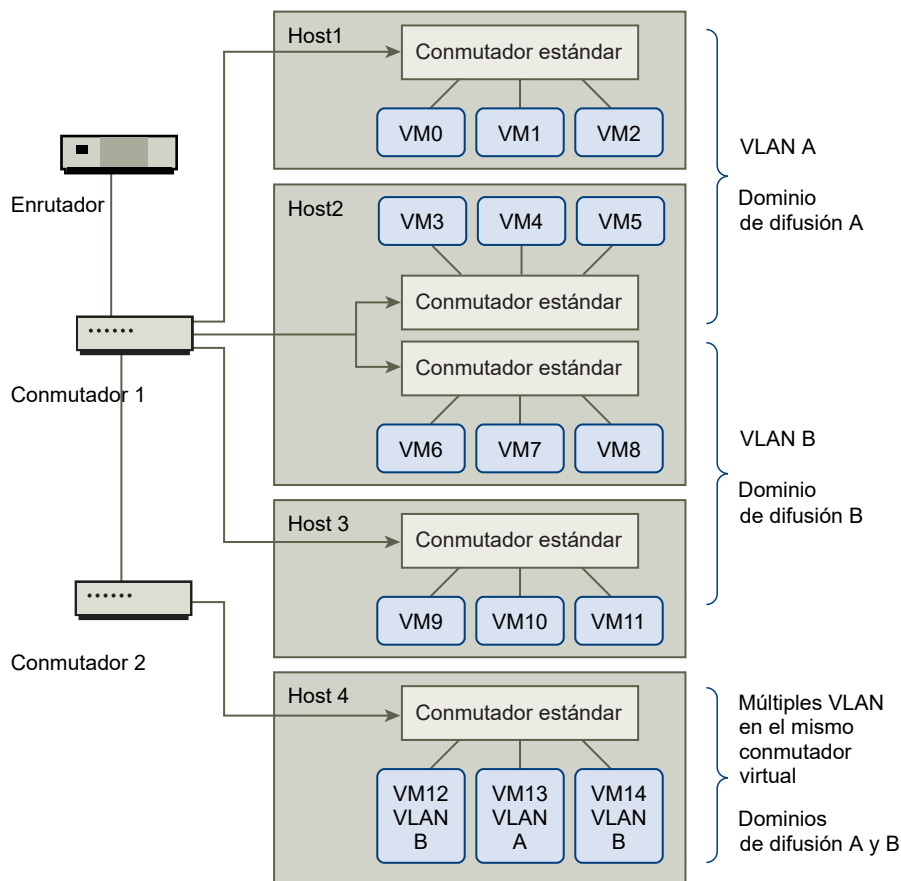
## Proteger las máquinas virtuales con VLAN

La red puede ser una de las partes más vulnerables de un sistema. La red de máquinas virtuales necesita tanta protección como una red física. La utilización de VLAN puede mejorar la seguridad de las redes del entorno.

Las VLAN se encuentran en un esquema de redes estándar IEEE, con métodos de etiquetado específicos que permiten el enrutamiento de los paquetes únicamente hacia los puertos que forman parte de la VLAN. Cuando se las configura correctamente, las VLAN constituyen un medio confiable para proteger un conjunto de máquinas virtuales contra intrusiones accidentales o maliciosas.

Las VLAN permiten segmentar una red física de modo que dos máquinas de la red no puedan transmitirse paquetes entre ellas a menos que formen parte de la misma VLAN. Por ejemplo, las transacciones y los registros contables son algunos de los datos internos más confidenciales de una empresa. En una empresa cuyos empleados de los departamentos de ventas, envíos y contabilidad utilizan máquinas virtuales en la misma red física, es posible proteger las máquinas virtuales del departamento contable mediante la configuración de las VLAN.

**Figura 8-1. Esquema de muestra de una VLAN**



En esta configuración, todos los empleados del departamento contable utilizan máquinas virtuales en la VLAN A y los empleados de ventas utilizan máquinas virtuales en la VLAN B.

El enrutador reenvía los paquetes que contienen los datos contables a los conmutadores. Estos paquetes se etiquetan para la distribución en la VLAN A únicamente. Por lo tanto, los datos quedan confinados al dominio de difusión A y no pueden enrutarse al dominio de difusión B a menos que se configure al enrutador para hacerlo.

Esta configuración de VLAN impide que los empleados de ventas intercepten los paquetes destinados al departamento contable. También evita que el departamento contable reciba paquetes destinados al grupo de ventas. Las máquinas virtuales atendidas por un único conmutador virtual pueden encontrarse en diferentes VLAN.

## Consideraciones de seguridad para VLAN

La forma de configurar VLAN para proteger partes de una red depende de factores tales como el sistema operativo invitado y el tipo de configuración del equipo de red.

ESXi cuenta con una implementación completa de VLAN compatibles con IEEE 802.1q VLAN. VMware no puede hacer recomendaciones específicas sobre el modo de configurar las VLAN, pero hay algunos factores que deben considerarse al usar la implementación de VLAN como parte de la directiva de cumplimiento de seguridad.

## Proteger las VLAN

Los administradores tienen varias opciones para proteger las VLAN en el entorno de vSphere.

### Procedimiento

- 1 Asegúrese de que los grupos de puertos no estén configurados con valores de la VLAN reservados para los conmutadores físicos ascendentes.

No establezca los identificadores de la VLAN con valores reservados para el conmutador físico.

- 2 Compruebe que los grupos de puertos no estén configurados en la VLAN 4095 a menos que esté utilizando el etiquetado de invitado virtual (VGT).

Hay tres tipos de etiquetado de VLAN en vSphere:

- Etiquetado de conmutador externo (EST)
- Etiquetado de conmutador virtual (VST): el conmutador virtual etiqueta con el identificador de VLAN configurado el tráfico que entra en las máquinas virtuales asociadas y quita la etiqueta de VLAN del tráfico saliente. Para configurar el modo VST, asigne un identificador de VLAN entre 1 y 4095.
- Etiquetado de invitado virtual (VGT): las máquinas virtuales controlan el tráfico de VLAN. Para activar el modo VGT, establezca el identificador de VLAN en 4095. En un conmutador distribuido, también puede permitir el tráfico de máquinas virtuales en función de su VLAN mediante la opción **Enlace troncal de VLAN**.

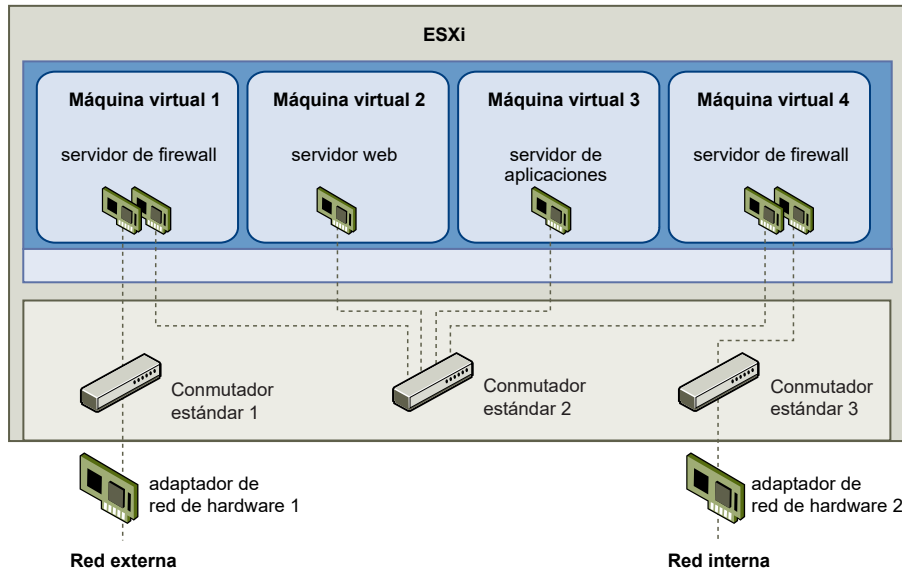
En un conmutador estándar, puede configurar el modo de redes de VLAN en el nivel del conmutador o del grupo de puertos. En un conmutador distribuido, puede hacerlo en el nivel del puerto o del grupo de puertos distribuidos.

- 3 Asegúrese de que todas las VLAN de cada conmutador virtual estén completamente documentadas y que cada conmutador virtual tenga todas las VLAN requeridas y solamente esas.

## Crear una DMZ de una red en un único host ESXi

Un ejemplo de cómo utilizar el aislamiento de ESXi y las características de redes virtuales para configurar un entorno seguro es la creación de una red perimetral de red (DMZ) en un único host.

Figura 8-2. DMZ configurada en un único host ESXi



En este ejemplo, se configuran cuatro máquinas virtuales para crear una DMZ virtual en el conmutador estándar 2:

- La máquina virtual 1 y la máquina virtual 4 ejecutan firewalls y están conectadas a adaptadores de red físicos mediante conmutadores estándar. Ambas máquinas virtuales utilizan varios conmutadores.
- La máquina virtual 2 ejecuta un servidor web, mientras que la máquina virtual 3 ejecuta un servidor de aplicaciones. Ambas máquinas virtuales están conectadas a un conmutador virtual.

El servidor web y el servidor de aplicaciones ocupan la DMZ entre los dos firewalls. El medio de transmisión entre estos elementos es el conmutador estándar 2, que conecta los firewalls con los servidores. Este conmutador no tiene conexión directa con ningún elemento fuera de la DMZ, y está aislado del tráfico externo mediante los dos firewalls.

Desde el punto de vista operativo, el tráfico externo de Internet entra a la máquina virtual 1 a través del adaptador de red de hardware 1 (enrutado con el conmutador estándar 1) y se somete a la comprobación del firewall instalado en esta máquina. Si el firewall autoriza el tráfico, este último se enruta al conmutador estándar de la DMZ, el conmutador estándar 2. Como el servidor web y el servidor de aplicaciones también están conectados a este conmutador, pueden atender solicitudes externas.

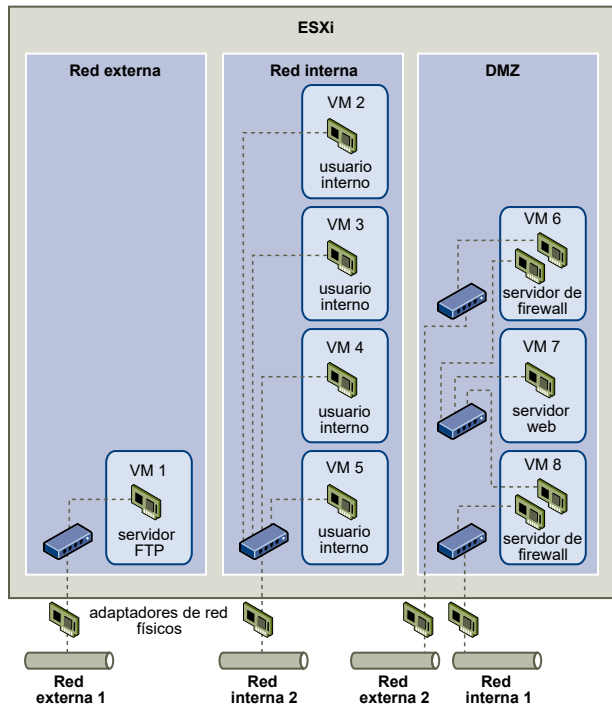
El conmutador estándar 2 también está conectado a la máquina virtual 4. Esta máquina virtual coloca un firewall entre la DMZ y la red interna de la empresa. Este firewall filtra los paquetes provenientes del servidor web y del servidor de aplicaciones. Si se comprueba un paquete, este se enruta al adaptador de red de hardware 2 a través del conmutador estándar 3. El adaptador de red de hardware 2 está conectado a la red interna de la empresa.

Al crear una DMZ en un único host, se pueden utilizar firewalls bastante ligeros. Aunque una máquina virtual en esta configuración no puede ejercer un control directo sobre otra máquina virtual ni acceder a su memoria, todas las máquinas virtuales siguen conectadas a través de una red virtual. Esta red se puede utilizar para propagar virus o como objetivo de otros tipos de ataques. La seguridad de las máquinas virtuales dentro de la DMZ es igual a la de distintas máquinas físicas conectadas a la misma red.

## Crear varias redes en un único host ESXi

El diseño del sistema ESXi permite conectar algunos grupos de máquinas virtuales a la red interna, otros a la red externa y otros a ambos, todos en el mismo host. Esta capacidad es una extensión del aislamiento básico de máquinas virtuales combinado con la utilización bien planificada de características de redes virtuales.

Figura 8-3. Redes externas, redes internas y una DMZ configuradas en un único host ESXi



En la figura, el administrador de sistema configuró un host en tres zonas de máquinas virtuales diferentes: servidor FTP, máquinas virtuales internas y DMZ. Cada zona tiene una función única.

### Servidor FTP



La máquina virtual 1 está configurada con el software FTP y actúa como área de retención de los datos enviados hacia los recursos externos y desde estos, como formularios y documentación localizados por un proveedor.

Esta máquina virtual solo está asociada con una red externa. Tiene su propio conmutador virtual y su propio adaptador de red físico que la conectan a la red externa 1. Esta red está dedicada a los servidores que usa la empresa para recibir datos de orígenes externos. Por ejemplo, la empresa utiliza la red externa 1 para recibir tráfico FTP de los proveedores, y permite a estos últimos acceder a los datos almacenados en servidores disponibles de forma externa a través de FTP. Además de atender a la máquina virtual 1, la red externa 1 se encarga de los servidores FTP configurados en diferentes hosts ESXi en todo el sitio.

Debido a que la máquina virtual 1 no comparte un conmutador virtual o un adaptador de red físico con ninguna máquina virtual del host, las otras máquinas virtuales residentes no pueden transmitir paquetes a la red de la máquina virtual 1 ni recibir paquetes de ella. Esta restricción evita los ataques por analizadores de protocolos (sniffer), que se basan en el envío de tráfico de red a la víctima. Otro factor más importante es que un atacante no puede utilizar la vulnerabilidad natural de FTP para acceder a ninguna de las otras máquinas virtuales del host.

### **Máquinas virtuales internas**

Las máquinas virtuales 2 a 5 están reservadas para la utilización interna. Estas máquinas virtuales procesan y almacenan datos privados de la empresa, como registros médicos, declaraciones legales e investigaciones de fraude. Por lo tanto, los administradores del sistema deben garantizar el nivel más alto de protección de estas máquinas virtuales.

Estas máquinas virtuales se conectan a la red interna 2 mediante un conmutador virtual y un adaptador de red propios. La red interna 2 está reservada para la utilización interna por parte del personal, por ejemplo, procesadores de reclamos, abogados internos o tasadores.

Las máquinas virtuales 2 a 5 pueden comunicarse entre sí mediante el conmutador virtual, y con máquinas internas de otros lugares de la red interna 2 mediante el adaptador de red físico. Sin embargo, no pueden comunicarse con máquinas externas. Al igual que con el servidor FTP, estas máquinas virtuales no pueden enviar paquetes a las redes de las otras máquinas virtuales ni recibir paquetes de ellas. De forma similar, las otras máquinas virtuales del host no pueden enviar paquetes a las máquinas virtuales 2 a 5 ni recibir paquetes de ellas.

### **DMZ**

Las máquinas virtuales 6 a 8 están configuradas como una DMZ que utiliza el grupo de comercialización para publicar el sitio web externo de la empresa.

Este grupo de máquinas virtuales está asociado con la red externa 2 y la red interna 1. La empresa utiliza la red externa 2 para admitir los servidores web que utilizan el departamento de comercialización y finanzas para alojar el sitio web de la empresa y otras características web para usuarios externos. La red interna 1 es el medio que utiliza el departamento de comercialización para publicar contenido en el sitio web de la empresa, publicar descargas y mantener servicios como los foros de usuarios.

Debido a que estas redes están separadas de la red externa 1 y la red interna 2, y las máquinas virtuales no tienen puntos de contacto compartidos (conmutadores o adaptadores), no existe riesgo de ataque hacia o desde el servidor FTP o el grupo de máquinas virtuales internas.

Al lograr el aislamiento de máquinas virtuales, configurar correctamente los conmutadores virtuales y mantener la separación de las redes, el administrador del sistema puede alojar las tres zonas de máquinas virtuales en el mismo host ESXi y estar seguro de que no se producirán infracciones de datos o recursos.

La empresa aplica el aislamiento en los grupos de máquinas virtuales mediante la utilización de varias redes internas y externas, y se asegura de que los conmutadores virtuales y los adaptadores de red físicos de cada grupo estén completamente separados de esos grupos o de otros.

Gracias a que ninguno de estos conmutadores virtuales favorece zonas de máquinas virtuales sobre las demás, el administrador del sistema logra eliminar el riesgo de pérdida de paquetes de una zona a la otra. Debido a su diseño, un conmutador virtual no puede perder paquetes directamente en otro conmutador virtual. La única forma de que los paquetes pasen de un conmutador virtual a otro es en estas circunstancias:

- Los conmutadores virtuales están conectados a la misma LAN física.
- Los conmutadores virtuales se conectan a una máquina virtual común, que se puede utilizar para transmitir paquetes.

Ninguna de estas condiciones se cumple en la configuración de ejemplo. Si los administradores del sistema quieren comprobar que no existen rutas de acceso a conmutadores virtuales comunes, pueden revisar la distribución de conmutadores de red de vSphere Web Client para buscar posibles puntos de contacto compartidos.

Para proteger los recursos de las máquinas virtuales, el administrador del sistema disminuye el riesgo de ataques DoS y DDoS mediante la configuración de una reserva de recursos y un límite para cada máquina virtual. El administrador del sistema protege aún más el host y las máquinas virtuales de ESXi mediante la instalación de firewalls de software en los extremos delanteros y traseros de la DMZ, que garantiza que el host esté detrás de un firewall físico, y la configuración de los recursos de almacenamiento en red para que cada uno de ellos tenga su propio conmutador virtual.

## Seguridad del protocolo de Internet

El protocolo Internet Protocol Security (IPsec) protege las comunicaciones de IP que recibe y envía un host. Los hosts ESXi admiten IPsec con IPv6.

Al configurar IPsec en un host, se habilita la autenticación y el cifrado de paquetes entrantes y salientes. El momento y el modo en que el tráfico de IP se cifra dependen de la configuración de las asociaciones de seguridad del sistema y de las directivas de seguridad.

Una asociación de seguridad determina el modo en que el sistema cifra el tráfico. Al crear una asociación de seguridad, se especifican el origen y el destino, los parámetros de cifrado y un nombre para la asociación de seguridad.

Una directiva de seguridad determina el momento en el que el sistema debe cifrar el tráfico. La directiva de seguridad incluye la información del origen y destino, el protocolo y la dirección del tráfico que se va a cifrar, el modo (transporte o túnel) y la asociación de seguridad que se deben utilizar.

## Lista de asociaciones de seguridad disponibles

ESXi puede proporcionar una lista de todas las asociaciones de seguridad disponibles que pueden usar las directivas de seguridad. La lista incluye tanto las asociaciones de seguridad creadas por el usuario como las asociaciones de seguridad que haya instalado el VMkernel con el intercambio de claves por red.

Puede obtener una lista de las asociaciones de seguridad disponibles mediante el comando de vSphere CLI `esxcli`.

### Procedimiento

- ◆ En el símbolo del sistema, introduzca el comando **`esxcli network ip ipsec sa list`**.

### Resultados

ESXi muestra una lista de todas las asociaciones de seguridad disponibles.

## Agregar una asociación de seguridad IPsec

Agregue una asociación de seguridad a fin de especificar parámetros de cifrado para el tráfico de IP asociado.

Puede agregar una asociación de seguridad mediante el comando `esxcli` de vSphere CLI.

### Procedimiento

- ◆ En el símbolo del sistema, introduzca el comando **`esxcli network ip ipsec sa add`** con una o más de las siguientes opciones.

Opción	Descripción
<code>--sa-source= <i>source address</i></code>	Requerido. Especifique la dirección de origen.
<code>--sa-destination= <i>destination address</i></code>	Requerido. Especifique la dirección de destino.
<code>--sa-mode= <i>mode</i></code>	Requerido. Especifique el modo, ya sea <code>transport</code> o <code>tunnel</code> .
<code>--sa-spi= <i>security parameter index</i></code>	Requerido. Especifique el índice de parámetros de seguridad. El índice de parámetros de seguridad identifica la asociación de seguridad con el host. Debe ser un número hexadecimal con un prefijo 0x. Cada asociación de seguridad que cree debe tener una combinación única de protocolo e índice de parámetros de seguridad.

Opción	Descripción
<code>--encryption-algorithm= <i>encryption algorithm</i></code>	Requerido. Especifique el algoritmo de cifrado mediante uno de los siguientes parámetros. <ul style="list-style-type: none"> <li>■ 3des-cbc</li> <li>■ aes128-cbc</li> <li>■ null (no proporciona cifrado)</li> </ul>
<code>--encryption-key= <i>encryption key</i></code>	Requerido al especificar un algoritmo de cifrado. Especifique la clave de cifrado. Puede introducir claves como texto ASCII o un número hexadecimal con un prefijo 0x.
<code>--integrity-algorithm= <i>authentication algorithm</i></code>	Requerido. Especifique el algoritmo de autenticación, ya sea <code>hmac-sha1</code> o <code>hmac-sha2-256</code> .
<code>--integrity-key= <i>authentication key</i></code>	Requerido. Especifique la clave de autenticación. Puede introducir claves como texto ASCII o un número hexadecimal con un prefijo 0x.
<code>--sa-name= <i>name</i></code>	Requerido. Proporcione un nombre para la asociación de seguridad.

## Ejemplo: Nuevo comando de asociación de seguridad

El siguiente ejemplo contiene saltos de línea adicionales para facilitar la lectura.

```
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 0x6970763672656164796c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sal
```

## Quitar una asociación de seguridad IPsec

Es posible eliminar una asociación de seguridad mediante el comando ESXCLI de vSphere CLI.

### Requisitos previos

Compruebe que la asociación de seguridad que desea utilizar no esté en uso. Si intenta eliminar una asociación de seguridad en uso, la operación de eliminación generará errores.

### Procedimiento

- ◆ En el símbolo del sistema, introduzca el comando **`esxcli network ip ipsec sa remove --sa-name security_association_name`**

## Lista de directivas de seguridad IPsec disponibles

Las directivas de seguridad disponibles se pueden enumerar mediante el comando ESXCLI de vSphere CLI.

## Procedimiento

- ◆ En el símbolo del sistema, introduzca el comando **esxcli network ip ipsec sp list**.

## Resultados

El host muestra una lista de todas las directivas de seguridad disponibles.

## Crear una directiva de seguridad IPsec

Cree una directiva de seguridad para determinar cuándo se debe utilizar el conjunto de parámetros de autenticación y cifrado en una asociación de seguridad. Puede agregar una directiva de seguridad mediante el comando ESXCLI de vSphere CLI.

## Requisitos previos

Antes de crear una directiva de seguridad, agregue una asociación de seguridad con los parámetros de autenticación y cifrado adecuados, tal como se describe en [Agregar una asociación de seguridad IPsec](#).

## Procedimiento

- ◆ En el símbolo del sistema, introduzca el comando **esxcli network ip ipsec sp add** con una o más de las siguientes opciones.

Opción	Descripción
<b>--sp-source= <i>source address</i></b>	Requerido. Especifique la dirección IP de origen y la longitud del prefijo.
<b>--sp-destination= <i>destination address</i></b>	Requerido. Especifique la dirección de destino y la longitud del prefijo.
<b>--source-port= <i>port</i></b>	Requerido. Especifique el puerto de origen. El puerto de origen debe ser un número entre 0 y 65535.
<b>--destination-port= <i>port</i></b>	Requerido. Especifique el puerto de destino. El puerto de origen debe ser un número entre 0 y 65535.
<b>--upper-layer-protocol= <i>protocol</i></b>	Especifique el protocolo de capa superior mediante uno de los siguientes parámetros. <ul style="list-style-type: none"> <li>■ tcp</li> <li>■ udp</li> <li>■ icmp6</li> <li>■ any</li> </ul>
<b>--flow-direction= <i>direction</i></b>	Especifique la dirección en la que desea supervisar el tráfico mediante <i>in</i> o <i>out</i> .
<b>--action= <i>action</i></b>	Utilice los siguientes parámetros para especificar la acción que se debe realizar cuando se encuentra tráfico con los parámetros especificados. <ul style="list-style-type: none"> <li>■ none: no realice ninguna acción.</li> <li>■ discard: no permita la entrada o salida de datos.</li> <li>■ ipsec: utilice la información de autenticación y cifrado proporcionada en la asociación de seguridad para determinar si los datos provienen de un origen confiable.</li> </ul>

Opción	Descripción
<code>--sp-mode= <i>mode</i></code>	Especifique el modo, ya sea <code>tunnel</code> o <code>transport</code> .
<code>--sa-name= <i>security association name</i></code>	Requerido. Proporcione el nombre de la asociación de seguridad para la directiva de seguridad que se va a utilizar.
<code>--sp-name= <i>name</i></code>	Requerido. Proporcione un nombre para la directiva de seguridad.

## Ejemplo: Nuevo comando de directiva de seguridad

En el siguiente ejemplo se incluyen saltos de línea adicionales para facilitar la lectura.

```
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
```

## Quitar una directiva de seguridad IPsec

Es posible eliminar una directiva de seguridad del host ESXi mediante el comando ESXCLI de vSphere CLI.

### Requisitos previos

Compruebe que la directiva de seguridad que desea utilizar no esté en uso. Si intenta eliminar una directiva de seguridad en uso, la operación de eliminación generará errores.

### Procedimiento

- ◆ En el símbolo del sistema, introduzca el comando **`esxcli network ip ipsec sp remove --sa-name security policy name`**.

Para eliminar todas las directivas de seguridad, introduzca el comando **`esxcli network ip ipsec sp remove --remove-all`**.

## Garantizar la correcta configuración de SNMP

Si SNMP no se configura correctamente, puede enviarse información de supervisión a un host malicioso. El host malicioso puede usar esta información para planificar un ataque.

### Procedimiento

- 1 Ejecute el comando **`esxcli system snmp get`** para determinar si SNMP se usa correctamente.

- 2 Si el sistema requiere SNMP, asegúrese de que SNMP funcione. Para ello, ejecute el comando `esxcli system snmp set --enable true`.
- 3 Si el sistema usa SNMP, consulte la publicación *Supervisión y rendimiento* para obtener la información de instalación de SNMP 3.

SNMP debe configurarse en cada host ESXi. Puede usar vCLI, PowerCLI o vSphere Web Services SDK para la configuración.

## Usar conmutadores virtuales con vSphere Network Appliance API solo cuando es necesario

Si no utiliza productos que usan vSphere Network Appliance API (DvFilter), no configure el host para enviar información de red a una máquina virtual. Si vSphere Network Appliance API está habilitado, un atacante puede intentar conectar una máquina virtual al filtro. Esta conexión puede abrir el acceso a la red de otras máquinas virtuales del host.

Si utiliza un producto que usa esta API, compruebe que el host esté configurado correctamente. Consulte las secciones sobre DvFilter en *Desarrollo e implementación de soluciones de vSphere*, *vServices y agentes de ESX*. Si el host está configurado para usar la API, compruebe que el valor del parámetro `Net.DVFilterBindIpAddress` coincida con el producto que usa la API.

### Procedimiento

- 1 Para asegurarse de que el parámetro del kernel `Net.DVFilterBindIpAddress` tenga el valor correcto, busque el parámetro mediante vSphere Web Client.
  - a Seleccione el host y haga clic en la pestaña **Administrar**.
  - b En Sistema, seleccione **Configuración avanzada del sistema**.
  - c Desplácese hacia abajo hasta `Net.DVFilterBindIpAddress` y compruebe que el parámetro tenga un valor vacío.
 

El orden de los parámetros no es estrictamente alfabético. Escriba **DVFilter** en el campo Filtrar para mostrar todos los parámetros relacionados.
- 2 Si no utiliza la configuración de DvFilter, asegúrese de que el valor esté en blanco.
- 3 Si utiliza la configuración de DvFilter, asegúrese de que el valor del parámetro coincida con el valor que usa el producto que DvFilter utiliza.

## Prácticas recomendadas de seguridad de redes de vSphere

Seguir las prácticas recomendadas de seguridad de redes permite garantizar la integridad de la implementación de vSphere.

## Recomendaciones generales sobre seguridad de redes

El primer paso para proteger el entorno de las redes es seguir las recomendaciones generales sobre seguridad de red. A continuación, puede pasar a áreas especiales, como la protección de la red con firewalls o IPsec.

- Asegúrese de que los puertos de conmutadores físicos estén configurados con Portfast si el árbol de expansión está habilitado. Debido a que los conmutadores virtuales de VMware no admiten STP, los puertos de conmutadores físicos conectados a un host ESXi deben tener Portfast configurado si el árbol de expansión está habilitado, a fin de evitar bucles en la red de conmutadores físicos. Si Portfast no está configurado, pueden producirse problemas de rendimiento y conectividad.
- Asegúrese de que el tráfico de Netflow de un conmutador virtual distribuido se envíe solamente a direcciones IP de recopiladores autorizados. Las exportaciones de Netflow no están cifradas y pueden contener información sobre la red virtual, lo que aumenta el riesgo de recibir un ataque de intermediario efectivo. Si se necesita una exportación de Netflow, compruebe que todas las direcciones IP de destino de Netflow sean correctas.
- Use los controles de acceso basado en funciones para asegurarse de que solo los administradores autorizados tengan acceso a los componentes de redes virtuales. Por ejemplo, los administradores de máquinas virtuales deben tener acceso solo a los grupos de puertos en los que residen sus máquinas virtuales. Los administradores de red deben tener permisos para todos los componentes de redes virtuales, pero no deben tener acceso a las máquinas virtuales. Si se limita el acceso, se reduce el riesgo de una configuración incorrecta, ya sea accidental o malintencionada, y se aplican los conceptos de seguridad clave de división de tareas y privilegios mínimos.
- Asegúrese de que los grupos de puertos no estén configurados con el valor de la VLAN nativa. Los conmutadores físicos usan la VLAN 1 como su VLAN nativa. Las tramas de una VLAN no están etiquetadas con un 1. ESXi no tiene una VLAN nativa. Las tramas con VLAN especificadas en el grupo de puertos tienen una etiqueta, pero las tramas con VLAN no especificadas en el grupo de puertos no están etiquetadas. Esto puede provocar un problema porque las máquinas virtuales etiquetadas con un 1 terminan perteneciendo a una VLAN nativa del conmutador físico.

Por ejemplo, las tramas de la VLAN 1 de un conmutador físico de Cisco no tienen etiquetas porque la VLAN 1 es la VLAN nativa de ese conmutador físico. Sin embargo, las tramas del host ESXi especificadas como VLAN 1 están etiquetadas con un 1; por lo tanto, el tráfico del host ESXi que está destinado a la VLAN nativa no está enrutado correctamente porque está etiquetado con un 1, cuando en realidad no debería tener etiquetas. El tráfico del conmutador físico que viene de la VLAN nativa no es visible porque no está etiquetado. Si el grupo de puertos del conmutador virtual de ESXi usa el identificador de la VLAN nativa, el tráfico proveniente de las máquinas virtuales de ese puerto no será visible para la VLAN nativa del conmutador, ya que este último espera tráfico sin etiquetas.



- Asegúrese de que los grupos de puertos no estén configurados con los valores de la VLAN reservados para los conmutadores físicos ascendentes. Los conmutadores físicos reservan ciertos identificadores de VLAN para fines internos y generalmente no permiten el tráfico configurado con estos valores. Por ejemplo, los conmutadores Cisco Catalyst generalmente reservan las VLAN 1001-1024 y 4094. El uso de una VLAN reservada puede provocar la denegación de servicio en la red.
- Asegúrese de que los grupos de puertos no estén configurados con la VLAN 4095, con excepción del etiquetado de invitado virtual (VGT). Al configurar un grupo de puertos con la VLAN 4095, se activa el modo de VGT. En este modo, el conmutador virtual pasa todas las tramas de red a la máquina virtual sin modificar las etiquetas de la VLAN, y deja que la máquina virtual se encargue de ellas.
- Restrinja las anulaciones de la configuración de nivel de puerto de un conmutador virtual distribuido. Las anulaciones de la configuración de nivel de puerto están deshabilitadas de forma predeterminada. Una vez habilitadas, las anulaciones permiten el uso de opciones de configuración de seguridad para una máquina virtual diferentes a las del nivel de grupo de puertos. Algunas máquinas virtuales requieren una configuración única, pero la supervisión es fundamental. Si las anulaciones no se supervisan, cualquiera que tenga acceso a una máquina virtual con una configuración de conmutador virtual distribuido poco segura puede intentar aprovecharse de dicho acceso.
- Asegúrese de que el tráfico reflejado del conmutador virtual distribuido se envíe solo a los puertos o las VLAN de recopiladores autorizados. vSphere Distributed Switch puede reflejar el tráfico de un puerto a otro para permitir que los dispositivos de captura de paquetes recopilen flujos de tráfico específicos. La funcionalidad de creación de reflejo de puertos envía una copia de todo el tráfico especificado en formato no cifrado. El tráfico reflejado contiene todos los datos en los paquetes capturados, por lo que tales datos pueden verse afectados por completo si se envían a una dirección incorrecta. Si se requiere la creación de reflejo del puerto, verifique que la VLAN de destino del puerto reflejado, el puerto y los identificadores de vínculo superior sean correctos.

## Etiquetar componentes de redes

La identificación de los diversos componentes de la arquitectura de redes es esencial y permite garantizar que no se introduzcan errores a medida que se expande la red.

Siga estas prácticas recomendadas:

- Asegúrese de que los grupos de puertos se configuren con una etiqueta de red clara. Estas etiquetas actúan como un descriptor de funciones del grupo de puertos y permiten identificar la función de cada grupo de puertos a medida que se incrementa la complejidad de la red.

- Asegúrese de que cada vSphere Distributed Switch contenga una etiqueta de red clara donde se indique la función o la subred IP de ese conmutador. Esta etiqueta actúa como un descriptor de funciones para el conmutador, al igual que el nombre de host requerido para los conmutadores físicos. Por ejemplo, se puede etiquetar el conmutador como interno para indicar que es para las redes internas. No se puede cambiar la etiqueta de un conmutador virtual estándar.

## Documentación y verificación del entorno VLAN de vSphere

Compruebe el entorno de VLAN regularmente para evitar futuros problemas. Documente en detalle el entorno de VLAN y asegúrese de que los identificadores de VLAN se utilicen una sola vez. La documentación puede ayudar a solucionar problemas y resulta fundamental para expandir el entorno.

### Procedimiento

- 1 Asegúrese de que todos los identificadores de vSwitch y VLAN estén documentados detalladamente.

Si utiliza un etiquetado de VLAN en un conmutador virtual, los identificadores deben coincidir con los identificadores de los conmutadores ascendentes con reconocimiento de VLAN.

Si no se hace un seguimiento completo de los identificadores de VLAN, la reutilización de identificadores por error puede producir tráfico entre las máquinas virtuales y físicas inadecuadas. De modo similar, si los identificadores de VLAN son incorrectos o faltan, puede bloquearse el tráfico entre las máquinas físicas y virtuales en los lugares donde el tráfico debiera circular.

- 2 Compruebe que los identificadores de VLAN de todos los grupos de puertos virtuales distribuidos (instancias dvPortgroup) estén documentados detalladamente.

Si utiliza un etiquetado de VLAN en un dvPortgroup, los identificadores deben coincidir con los identificadores de los conmutadores ascendentes externos con reconocimiento de VLAN.

Si no se hace un seguimiento completo de los identificadores de VLAN, la reutilización de identificadores por error puede producir tráfico entre las máquinas virtuales y físicas inadecuadas. De modo similar, si los identificadores de VLAN son incorrectos o faltan, puede bloquearse el tráfico entre las máquinas físicas y virtuales en los lugares donde el tráfico debiera circular.

- 3 Compruebe que los identificadores de VLAN privada de todos los conmutadores virtuales distribuidos estén documentados detalladamente.

Las VLAN privadas (PVLAN) de los conmutadores virtuales distribuidos requieren identificadores de VLAN principales y secundarios. Estos identificadores deben coincidir con los identificadores de los conmutadores ascendentes externos con reconocimiento de PVLAN. Si no se hace un seguimiento completo de los identificadores de VLAN, la reutilización

de identificadores por error puede producir tráfico entre las máquinas virtuales y físicas inadecuadas. De modo similar, si los identificadores de PVLAN son incorrectos o faltan, puede bloquearse el tráfico entre las máquinas físicas y virtuales en los lugares donde el tráfico debiera circular.

- 4 Compruebe que los enlaces troncales de VLAN estén conectados únicamente a los puertos de conmutadores físicos que funcionan como enlaces troncales.

Quando conecte un conmutador virtual a un puerto troncal de VLAN, debe configurar correctamente tanto el conmutador virtual como el físico en el puerto de vínculo superior. Si el conmutador físico no está configurado adecuadamente, se reenvían las tramas con el encabezado VLAN 802.1q a un conmutador que no espera esa llegada.

## Adoptar prácticas de aislamiento de red de sonido

La adopción de prácticas de aislamiento de red de sonido refuerza en gran medida el entorno de vSphere.

### Aislar la red de administración

La red de administración de vSphere proporciona acceso a la interfaz de administración de vSphere en cada componente. Los servicios que se ejecutan en la interfaz de administración ofrecen una oportunidad para que un atacante obtenga acceso con privilegios a los sistemas. Los ataques remotos suelen comenzar al obtener acceso a esta red. Si un atacante obtiene acceso a la red de administración, significa que ha dado un gran paso para seguir obteniendo acceso no autorizado.

Para lograr un control estricto del acceso a la red de administración, protéjalo con el nivel de seguridad de la máquina virtual más segura que se ejecuta en un host o clúster de ESXi. Más allá del nivel de restricción que tenga la red de administración, los administradores deben acceder a ella para configurar los hosts ESXi y el sistema vCenter Server.

Coloque el grupo de puertos de administración de vSphere en una VLAN dedicada de un vSwitch común. El vSwitch se puede compartir con el tráfico de producción (máquina virtual), siempre y cuando las máquinas virtuales de producción no utilicen la VLAN del grupo de puertos de administración de vSphere. Compruebe que el segmento de red no se encuentre enrutado, excepto si se enrutó a redes donde se alojan otras entidades de administración, por ejemplo, en conjunto con vSphere Replication. En particular, asegúrese de que el tráfico de las máquinas virtuales de producción no se pueda enrutar a esta red.

Utilice uno de los siguientes métodos para habilitar el acceso a la funcionalidad de administración de forma estrictamente controlada.

- Para entornos de extrema confidencialidad, configure una puerta de enlace controlada u otro método controlado para acceder a la red de administración. Por ejemplo, realice la configuración de modo tal que se requiera que los administradores se conecten a la red de administración a través de una VPN, y permita el acceso solo a los administradores de confianza.
- Configure JumpBoxes que ejecuten clientes de administración.

## Aislar el tráfico de almacenamiento

Compruebe que el tráfico de almacenamiento basado en IP esté aislado. El almacenamiento basado en IP incluye iSCSI y NFS. Las máquinas virtuales pueden compartir conmutadores virtuales y VLAN con configuraciones de almacenamiento basadas en IP. Este tipo de configuración puede exponer el tráfico de almacenamiento basado en IP a usuarios de máquinas virtuales no autorizados.

El almacenamiento basado en IP casi nunca está cifrado; cualquiera que tenga acceso a esta red puede verlo. Para impedir que usuarios no autorizados vean el tráfico de almacenamiento basado en IP, separe lógicamente el tráfico de red de almacenamiento basado en IP del tráfico de producción. Configure los adaptadores de almacenamiento basado en IP en VLAN distintas o segmentos de red de la red de administración VMkernel para restringir la visualización del tráfico a usuarios no autorizados.

## Aislar el tráfico de vMotion

La información de migración de vMotion se transmite en texto sin formato. Cualquiera que tenga acceso a la red puede ver la información que pasa por ella. Los posibles atacantes pueden interceptar el tráfico de vMotion para obtener el contenido de memoria de una máquina virtual. También pueden preparar un ataque de MiTM en el que el contenido se modifica durante la migración.

Separe el tráfico de vMotion del tráfico de producción en una red aislada. Configure la red para que no se pueda enrutar, es decir, asegúrese de que no haya un enrutador de Capa 3 expandiendo esta u otras redes, a fin de restringir el acceso exterior a esta red.

El grupo de puertos de vMotion debe estar en la VLAN dedicada de un vSwitch común. El vSwitch se puede compartir con el tráfico de producción (máquina virtual), siempre y cuando las máquinas virtuales de producción no utilicen la VLAN del grupo de puertos de vMotion.

# Prácticas recomendadas relacionadas con varios componentes de vSphere

## 9

Algunas prácticas recomendadas de seguridad, como la configuración de NTP en el entorno, tienen efecto en más de un componente de vSphere. Tenga en cuenta estas recomendaciones al configurar el entorno.

Consulte [Capítulo 5 Proteger hosts ESXi](#) y [Capítulo 7 Proteger máquinas virtuales](#) para obtener información relacionada.

Este capítulo incluye los siguientes temas:

- [Sincronizar los relojes en la red de vSphere](#)
- [Prácticas recomendadas de seguridad de almacenamiento](#)
- [Comprobar que está deshabilitado el envío de datos de rendimiento del host a los invitados](#)
- [Configurar tiempos de espera de ESXi Shell y vSphere Web Client](#)

## Sincronizar los relojes en la red de vSphere

Asegúrese de que todos los componentes de la red de vSphere tengan sus relojes sincronizados. Si los relojes de los equipos de la red de vSphere no están sincronizados, es posible que los certificados SSL, que están sujetos a limitación temporal, no se reconozcan como válidos en las comunicaciones entre equipos de la red.

Los relojes que no están sincronizados pueden ocasionar problemas de autenticación que, a su vez, pueden provocar que la instalación sea incorrecta o evitar que se inicie el servicio vpxd de vCenter Server Appliance.

Asegúrese de que los equipos host de Windows en los que se ejecuta un componente de vCenter estén sincronizados con el servidor NTP. Consulte el artículo de la base de conocimientos <http://kb.vmware.com/kb/1318>.

- [Sincronización de los relojes de ESXi con un servidor horario de red](#)  
Antes de instalar vCenter Server o de implementar vCenter Server Appliance, asegúrese de que todas las máquinas de la red de vSphere tengan los relojes sincronizados.
- [Configurar la sincronización de hora en vCenter Server Appliance](#)  
Puede cambiar la configuración de hora en vCenter Server Appliance tras la implementación.

## Sincronización de los relojes de ESXi con un servidor horario de red

Antes de instalar vCenter Server o de implementar vCenter Server Appliance, asegúrese de que todas las máquinas de la red de vSphere tengan los relojes sincronizados.

Esta tarea explica cómo configurar NTP desde vSphere Client. Se puede utilizar en su lugar el comando de vCLI `vicfg-ntp`. Consulte la *referencia de vSphere Command-Line Interface*.

### Procedimiento

- 1 Inicie vSphere Client y conéctese al host ESXi.
- 2 En la pestaña **Configuración**, haga clic en **Configuración de hora**.
- 3 Haga clic en **Propiedades** y en **Opciones**.
- 4 Seleccione **Configuración de NTP**.
- 5 Haga clic en **Agregar**.
- 6 En el cuadro de diálogo Agregar servidor NTP, introduzca la dirección IP o el nombre de dominio completo del servidor NTP para realizar la sincronización.
- 7 Haga clic en **Aceptar**.

La hora del host se sincroniza con el servidor NTP.

## Configurar la sincronización de hora en vCenter Server Appliance

Puede cambiar la configuración de hora en vCenter Server Appliance tras la implementación.

Cuando implementa vCenter Server Appliance, puede decidir que el método de sincronización de hora sea mediante un servidor NTP o a través de VMware Tools. En caso de que la configuración de hora de la red de vSphere cambie, puede editar vCenter Server Appliance y configurar la sincronización horaria mediante los comandos del shell del dispositivo.

Cuando habilita la sincronización horaria periódica, VMware Tools configura la hora del sistema operativo invitado para que sea la misma que la hora del host.

Una vez que se sincroniza la hora, VMware Tools comprueba cada un minuto si los relojes del sistema operativo invitado y el host aún coinciden. Si no lo hacen, el reloj del sistema operativo invitado se sincroniza para que coincida con el reloj del host.

El software de sincronización de hora nativo, como el protocolo de hora de red (NTP), suele ser más preciso que la sincronización horaria periódica de VMware Tools y, por lo tanto, es el método preferido. En vCenter Server Appliance, solo puede utilizar un modo de sincronización horaria periódica. Si decide utilizar software de sincronización de hora nativo, se desactiva la sincronización horaria periódica de VMware Tools en vCenter Server Appliance, y viceversa.

### Usar la sincronización de hora de VMware Tools

Puede configurar vCenter Server Appliance para utilizar la sincronización de hora de VMware Tools.

### Procedimiento

- 1 Acceda al shell del dispositivo e inicie sesión como usuario que tiene la función de administrador o superadministrador.

El usuario predeterminado con la función de superadministrador es root.

- 2 Ejecute el comando para habilitar la sincronización de hora de VMware Tools.

```
timesync.set --mode host
```

- 3 (opcional) Ejecute el comando para comprobar que la sincronización de hora de VMware Tools se aplicó correctamente.

```
timesync.get
```

El comando devuelve un mensaje donde se indica que la sincronización de hora se encuentra en el modo host.

### Resultados

La hora del dispositivo se sincroniza con la hora del host ESXi.

## Agregar o reemplazar servidores NTP en la configuración de vCenter Server Appliance

Para configurar vCenter Server Appliance de modo que utilice la sincronización de hora basada en NTP, debe agregar los servidores NTP a la configuración de vCenter Server Appliance.

### Procedimiento

- 1 Acceda al shell del dispositivo e inicie sesión como usuario que tiene la función de administrador o superadministrador.

El usuario predeterminado con la función de superadministrador es root.

- 2 Agregue servidores NTP a la configuración de vCenter Server Appliance mediante la ejecución del comando `ntp.server.add`.

Por ejemplo, ejecute el siguiente comando:

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

Aquí, *IP-addresses-or-host-names* es una lista separada por comas de direcciones IP o nombres de host de los servidores NTP.

Este comando agrega servidores NTP a la configuración. Si la sincronización de hora se basa en un servidor NTP, el daemon de NTP se reinicia para volver a cargar los nuevos servidores NTP. De lo contrario, este comando solo agrega los nuevos servidores NTP a la configuración de NTP existente.

- 3 (opcional) Para eliminar servidores NTP antiguos y agregar nuevos a la configuración de vCenter Server Appliance, ejecute el comando `ntp.server.set`.

Por ejemplo, ejecute el siguiente comando:

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

Aquí, *IP-addresses-or-host-names* es una lista separada por comas de direcciones IP o nombres de host de los servidores NTP.

Este comando elimina servidores NTP antiguos de la configuración y establece los servidores NTP de entrada. Si la sincronización de hora se basa en un servidor NTP, el daemon de NTP se reinicia para volver a cargar la nueva configuración de NTP. De lo contrario, este comando solo reemplaza los servidores de la configuración de NTP por los servidores que proporciona como entrada.

- 4 (opcional) Ejecute el comando para comprobar que se aplicó correctamente la nueva configuración de NTP.

```
ntp.get
```

El comando devuelve una lista separada con espacios de los servidores configurados para la sincronización de NTP. Si la sincronización de NTP está habilitada, el comando informa de que el estado de la configuración de NTP es Activado. Si la sincronización de NTP está deshabilitada, el comando informa de que el estado de la configuración de NTP es Desactivado.

### Pasos siguientes

Si la sincronización de NTP está deshabilitada, se puede configurar la sincronización de hora en vCenter Server Appliance para que se base en un servidor NTP. Consulte [Sincronizar la hora de vCenter Server Appliance con un servidor NTP](#).

## Sincronizar la hora de vCenter Server Appliance con un servidor NTP

Puede configurar la sincronización de hora en vCenter Server Appliance para que se base en un servidor NTP.

### Requisitos previos

Establezca uno o más servidores Network Time Protocol (NTP) en la configuración de vCenter Server Appliance. Consulte [Agregar o reemplazar servidores NTP en la configuración de vCenter Server Appliance](#).

### Procedimiento

- 1 Acceda al shell del dispositivo e inicie sesión como usuario que tiene la función de administrador o superadministrador.

El usuario predeterminado con la función de superadministrador es root.



- 2 Ejecute el comando para habilitar la sincronización de hora basada en NTP.

```
timesync.set --mode NTP
```

- 3 (opcional) Ejecute el comando para comprobar que se aplicó correctamente la sincronización de NTP.

```
timesync.get
```

El comando devuelve que la sincronización de hora se encuentra en el modo NTP.

## Prácticas recomendadas de seguridad de almacenamiento

Siga las prácticas recomendadas de seguridad de almacenamiento que indica su proveedor de seguridad de almacenamiento. También puede aprovechar CHAP y Mutual CHAP para proteger el almacenamiento iSCSI, crear máscaras para los recursos de SAN y dividirlos en zonas, y configurar credenciales Kerberos para NFS 4.1.

Consulte además la documentación de *Administración de VMware Virtual SAN*.

### Proteger almacenamiento iSCSI

El almacenamiento que se configura en un host puede incluir una o más redes de área de almacenamiento (SAN) que utilizan iSCSI. Cuando se configura iSCSI en un host, se pueden tomar varias medidas para minimizar los riesgos de seguridad.

iSCSI es un medio para acceder a los dispositivos SCSI e intercambiar registros de datos mediante TCP/IP en un puerto de red en lugar de hacerlo a través de una conexión directa con el dispositivo SCSI. En las transacciones de iSCSI, se encapsulan datos de SCSI sin procesar en registros de iSCSI que después se transmiten al usuario o al dispositivo solicitante.

Las SAN iSCSI permiten utilizar eficientemente las infraestructuras de Ethernet actuales con el fin de proporcionar acceso a los hosts para almacenar recursos que pueden compartir de forma dinámica. Las SAN iSCSI proporcionan una solución de almacenamiento económica para los entornos que dependen de un grupo de recursos comunes para atender a muchos usuarios. Al igual que con cualquier sistema en red, la seguridad de las SAN iSCSI puede verse comprometida debido a infracciones.

---

**Nota** Los requisitos y procedimientos para proteger la SAN iSCSI son similares para los adaptadores iSCSI de hardware que pueden utilizarse con los hosts y para iSCSI configurado directamente mediante el host.

---

### Proteger dispositivos de iSCSI

Una forma de proteger los dispositivos de iSCSI frente a una intromisión no deseada es exigir la autenticación por parte del dispositivo de iSCSI o del destino en el host o el iniciador, cada vez que el host intente acceder a los datos del LUN de destino.

El objetivo de la autenticación es probar que el iniciador tiene el derecho de acceder al destino, un derecho otorgado durante la configuración de la autenticación.

ESXi no admite el protocolo Secure Remote Protocol (SRP) o los métodos de autenticación de clave pública de iSCSI. Kerberos se puede utilizar solo con NFS 4.1.

ESXi admite la autenticación de CHAP y Mutual CHAP. En el documento *Almacenamiento de vSphere* se explica cómo seleccionar el mejor método de autenticación para el dispositivo de iSCSI y cómo configurar CHAP.

Asegúrese de que las contraseñas de CHAP sean únicas. La contraseña de autenticación mutua debe ser diferente para cada host; de ser posible, la contraseña también debe ser diferente para cada cliente que autentica el servidor. Esto garantiza que si un único host está comprometido, un atacante no pueda crear otro host arbitrario y autenticarse en el dispositivo de almacenamiento. Si hay una única contraseña compartida y un host comprometido, un atacante podría autenticarse en el dispositivo de almacenamiento.

## Proteger una SAN iSCSI

Al planificar la configuración de iSCSI, tome las medidas necesarias para mejorar la seguridad general de la SAN iSCSI. La configuración de iSCSI es tan segura como la red IP, por lo tanto, si aplica estándares de seguridad adecuados al configurar la red, ayuda a proteger el almacenamiento iSCSI.

A continuación, se presentan sugerencias específicas para aplicar estándares de seguridad adecuados.

### Proteger datos transmitidos

Uno de los principales riesgos en las SAN iSCSI es que un atacante puede capturar los datos de almacenamiento transmitidos.

Tome medidas adicionales para evitar que los atacantes vean datos de iSCSI con facilidad. Ni el adaptador de iSCSI de hardware ni el iniciador iSCSI de ESXi cifran los datos que transmiten hacia y desde los destinos, lo que hace que los datos sean más vulnerables a ataques de analizadores de protocolos (sniffer).

Si permite que las máquinas virtuales compartan conmutadores estándar y VLAN con la configuración de iSCSI, se corre el riesgo de que algún atacante de máquinas virtuales haga un uso incorrecto del tráfico iSCSI. Para ayudar a garantizar que los intrusos no puedan escuchar transmisiones de iSCSI, asegúrese de que ninguna de las máquinas virtuales pueda ver la red de almacenamiento iSCSI.

Si usa un adaptador de iSCSI de hardware, puede lograr esto comprobando que el adaptador de iSCSI y el adaptador físico de red de ESXi no se conecten accidentalmente fuera del host debido al uso compartido de un conmutador o a algún otro motivo. Si configura iSCSI directamente mediante el host ESXi, podrá lograr esto configurando el almacenamiento iSCSI con un conmutador estándar diferente al que se usa en las máquinas virtuales.

Además de proteger la SAN iSCSI con un conmutador estándar dedicado, puede configurar la SAN iSCSI en su propia VLAN para mejorar el rendimiento y la seguridad. Al colocar la configuración de iSCSI en una VLAN distinta, se garantiza que ningún dispositivo que no sea el adaptador de iSCSI pueda ver transmisiones dentro de la SAN iSCSI. Además, la congestión de la red desde otros orígenes no puede interferir en el tráfico iSCSI.

### Proteger los puertos de iSCSI

Al utilizar dispositivos de iSCSI, ESXi no abre ningún puerto que escuche conexiones de red. Esta medida reduce la posibilidad de que un intruso logre entrar a ESXi por los puertos de reserva y tome el control del host. De esta manera, la ejecución de iSCSI no presenta ningún riesgo adicional de seguridad al final de la conexión de ESXi.

Todos los dispositivos de destino iSCSI que se utilicen deben tener uno o más puertos TCP abiertos para escuchar las conexiones de iSCSI. Si existe alguna vulnerabilidad de seguridad en el software del dispositivo iSCSI, los datos pueden estar en riesgo incluso si ESXi funciona correctamente. Para reducir este riesgo, instale todas las revisiones de seguridad que le proporcione el fabricante del equipo de almacenamiento y limite los dispositivos conectados a la red de iSCSI.

## Crear máscaras y dividir en zonas para recursos de SAN

Puede utilizar la división en zonas y el enmascaramiento de LUN para segregar la actividad de SAN y restringir el acceso a los dispositivos de almacenamiento.

Puede proteger el acceso al almacenamiento en el entorno de vSphere mediante la división en zonas y el enmascaramiento de LUN con los recursos de SAN. Por ejemplo, puede administrar zonas definidas para pruebas de manera independiente en la SAN para que no interfieran con la actividad de las zonas de producción. De forma similar, puede configurar diferentes zonas para distintos departamentos.

Al configurar zonas, tenga en cuenta los grupos de hosts que estén configurados en el dispositivo SAN.

Las capacidades de división en zonas y de máscaras para cada conmutador SAN y matriz de disco, junto con las herramientas de administración de enmascaramiento de LUN, son específicas del proveedor.

Consulte la documentación del proveedor de SAN y la documentación de *Almacenamiento de vSphere*.

## Usar credenciales Kerberos para NFS 4.1

Con la versión 4.1 de NFS, ESXi admite el mecanismo de autenticación Kerberos.

Kerberos es un servicio de autenticación que permite instalar un cliente de NFS 4.1 en ESXi para probar su identidad en un servidor NFS antes de montar un recurso compartido de NFS. Kerberos utiliza criptografía para funcionar en una conexión de red no segura. La implementación de Kerberos de vSphere para NFS 4.1 solo permite la comprobación de identidad del cliente y servidor, y no proporciona servicios de integridad o confidencialidad de datos.

Al utilizar la autenticación Kerberos, se deben tener en cuenta las siguientes consideraciones:

- ESXi utiliza la versión 5 de Kerberos con un dominio de Active Directory y el centro de distribución de claves (KDC).
- Como administrador de vSphere, debe especificar credenciales de Active Directory para proporcionar acceso a un usuario de NFS a los almacenes de datos Kerberos de NFS 4.1. Se utiliza un único conjunto de credenciales para acceder a todos los almacenes de datos Kerberos montados en ese host.
- Cuando varios hosts ESXi comparten el mismo almacén de datos de NFS 4.1, se deben utilizar las mismas credenciales de Active Directory para todos los hosts que tienen acceso al almacén de datos compartido. Para automatizar esta tarea, configure el usuario en los perfiles de host y aplique el perfil a todos los hosts ESXi.
- NFS 4.1 no admite montajes de AUTH\_SYS y Kerberos simultáneos.
- NFS 4.1 con Kerberos no admite IPv6. Solo se admite IPv4.

## Comprobar que está deshabilitado el envío de datos de rendimiento del host a los invitados

vSphere incluye contadores de rendimiento de las máquinas virtuales en los sistemas operativos Windows con VMware Tools instalado. Los contadores de rendimiento permiten que los propietarios de las máquinas virtuales realicen análisis precisos del rendimiento en el sistema operativo invitado. De forma predeterminada, vSphere no expone la información del host a la máquina virtual invitada.

La capacidad para enviar los datos de rendimiento del host a una máquina virtual invitada está deshabilitada de forma predeterminada. Esta configuración predeterminada impide que la máquina virtual obtenga información detallada sobre el host físico. Por lo tanto, los datos del host no quedan disponibles si se produce una infracción a la seguridad de la máquina virtual.

---

**Nota** El procedimiento siguiente muestra el proceso básico. Utilice vSphere o una de las interfaces de línea de comandos de vSphere (vCLI, PowerCLI, entre otras) para realizar esta tarea simultáneamente en todos los hosts.

---

### Procedimiento

- 1 En el sistema ESXi que aloja a la máquina virtual, desplácese hasta el archivo VMX.  
 Los archivos de configuración de la máquina virtual están ubicados en el directorio / `vmfs/volumes/datastore`, donde *datastore* corresponde al nombre del dispositivo de almacenamiento en el que están almacenados los archivos de la máquina virtual.
- 2 En el archivo VMX, compruebe que se haya establecido el siguiente parámetro.  

```
tools.guestlib.enableHostInfo=FALSE
```
- 3 Guarde y cierre el archivo.

## Resultados

No se puede recuperar la información de rendimiento del host desde la máquina virtual invitada.

# Configurar tiempos de espera de ESXi Shell y vSphere Web Client

Para evitar que los intrusos utilicen una sesión inactiva, asegúrese de configurar tiempos de espera para ESXi Shell y vSphere Web Client.

## Tiempo de espera de ESXi Shell

Para ESXi Shell, puede establecer los siguientes tiempos de espera desde vSphere Web Client y la interfaz de usuario de la consola directa (DCUI).

### Tiempo de espera de disponibilidad

La configuración de tiempo de espera de disponibilidad corresponde a la cantidad de tiempo que puede transcurrir antes de que pueda iniciar sesión tras la habilitación de ESXi Shell. Una vez que transcurre el período de espera, el servicio se deshabilita y los usuarios no pueden iniciar sesión.

### Tiempo de espera de inactividad

El tiempo de espera de inactividad corresponde a la cantidad de tiempo que puede transcurrir antes de que se cierren las sesiones interactivas inactivas. Los cambios en el tiempo de espera de inactividad se aplican la próxima vez que un usuario inicia sesión en ESXi Shell y no afectan las sesiones actuales.

## Tiempo de espera de vSphere Web Client

De forma predeterminada, las sesiones de vSphere Web Client finalizan después de 120 minutos. Puede cambiar este valor predeterminado en el archivo `webclient.properties`, tal como se indica en la documentación de *Administración de vCenter Server y hosts*.

# Administrar la configuración del protocolo TLS con la utilidad de reconfiguración de TLS

# 10

Puede usar la utilidad de reconfiguración de TLS para habilitar o deshabilitar las versiones del protocolo TLS. Puede deshabilitar TLS 1.0 en el entorno de vSphere, o bien puede deshabilitar los protocolos TLS 1.0 y TLS 1.1. A partir de vSphere 6.5, las versiones del protocolo TLS 1.0, 1.1 y 1.2 están habilitadas de forma predeterminada.

Para la reconfiguración, los hosts vCenter Server, Platform Services Controller, vSphere Update Manager y ESXi del entorno deben ejecutar las versiones de software que permiten la deshabilitación. Consulte el artículo [2145796](#) de la base de conocimientos de VMware para obtener una lista de productos de VMware que admiten la deshabilitación de TLS 1.0.

Antes de deshabilitar TLS 1.0, también tendrá que asegurarse de que otros productos de VMware y productos de terceros admitan un protocolo TLS que esté habilitado. Según la configuración, puede ser TLS 1.2 o TLS 1.1 y TLS 1.2.

Este capítulo incluye los siguientes temas:

- [Puertos que permiten deshabilitar versiones de TLS](#)
- [Deshabilitar las versiones de TLS en vSphere](#)
- [Instalar la utilidad de configuración de TLS](#)
- [Realizar una copia de seguridad manual opcional](#)
- [Deshabilitar las versiones de TLS en los sistemas vCenter Server](#)
- [Deshabilitar las versiones de TLS en los hosts ESXi](#)
- [Deshabilitar las versiones de TLS en los sistemas Platform Services Controller](#)
- [Revertir los cambios de configuración de TLS](#)
- [Deshabilitar las versiones de TLS en vSphere Update Manager](#)

## Puertos que permiten deshabilitar versiones de TLS

Cuando se ejecuta la utilidad de configuración de TLS en el entorno de vSphere, se puede deshabilitar TLS en los puertos que usan TLS en los hosts vCenter Server, Platform Services Controller y ESXi. Es posible deshabilitar TLS 1.0, o bien TLS 1.0 y TLS 1.1.

En la siguiente tabla, se enumeran los puertos. Si un puerto no se incluye, la utilidad no lo afecta.

**Tabla 10-1. vCenter Server y Platform Services Controller afectados por la utilidad de configuración de TLS**

Servicio	Nombre en Windows	Nombre en Linux	Puerto
VMware HTTP Reverse Proxy	rhttpproxy	vmware-rhttpproxy	443
VMware Directory Service	VMWareDirectoryService	vmdird	636
VMware Syslog Collector (*)	vmwaresyslogcollector (*)	rsyslogd	1514
vSphere Auto Deploy Waiter	vmware-autodeploy-waiter	vmware-rbd-watchdog	6501 6502
Servicio de token seguro de VMware	VMwareSTS	vmware-stsd	7444
Servicio de vSphere Update Manager (**)	vmware-ufad-vci (**)	vmware-updatemgr	8084 9087
vSphere Web Client	vspherewebclientsvc	vsphere-client	9443
VMware Directory Service	VMWareDirectoryService	vmdird	11712

(\*) TLS se controla mediante la lista de cifrado para estos servicios. La administración granular no es posible. Solo se admiten TLS 1.2 o todas las versiones TLS 1.x.

(\*\*) En vCenter Server Appliance, vSphere Update Manager se encuentra en el mismo sistema que vCenter Server. En vCenter Server en Windows, TLS se configura mediante la edición de los archivos de configuración. Consulte [Deshabilitar las versiones de TLS en vSphere Update Manager](#).

**Tabla 10-2. Puertos ESXi afectados por la utilidad de configuración de TLS**

Servicio	Nombre del servicio	Puerto
VMware HTTP Reverse Proxy y daemon de host	Hostd	443
VMware vSAN VASA Vendor Provider	vSANVP	8080
VMware Fault Domain Manager	FDM	8182
VMware vSphere API para filtros de E/S	ioFilterVPServer	9080
Daemon de autorización de VMware	vmware-authd	902

## Notas y advertencias

- Asegúrese de que los hosts ESXi heredados que se administran mediante vCenter Server admitan una versión habilitada de TLS, ya sea TLS 1.1 y TLS 1.2 o solo TLS 1.2. Cuando se deshabilita una versión de TLS en vCenter Server 6.5, vCenter Server ya no puede administrar los hosts ESXi 5.x y 6.0 heredados. Actualice estos hosts a versiones compatibles con TLS 1.1 o TLS 1.2.

- No puede utilizar una conexión de solo TLS 1.2 para una instancia de Microsoft SQL Server externa o una base de datos de Oracle externa.
- No deshabilite TLS 1.0 en una instancia de vCenter Server o de Platform Services Controller que se ejecute en Windows Server 2008. Windows 2008 admite únicamente TLS 1.0. Consulte el artículo de Microsoft TechNet *Configuración de TLS/SSL* incluido en la *guía de tecnologías y funciones de servidor*.
- En las siguientes circunstancias, es necesario reiniciar los servicios del host después de aplicar cambios de configuración de TLS.
  - Si aplica los cambios en el host ESXi directamente.
  - Si aplica los cambios a través de la configuración del clúster mediante el uso de perfiles de host.

## Deshabilitar las versiones de TLS en vSphere

Deshabilitar las versiones de TLS es un proceso de varias etapas. Al deshabilitar las versiones de TLS en el orden correcto, se garantiza que el entorno permanezca activo y en ejecución durante el proceso.

- 1 Si el entorno incluye vSphere Update Manager en Windows y vSphere Update Manager se encuentra en un sistema independiente, deshabilite los protocolos explícitamente mediante la edición de los archivos de configuración. Consulte [Deshabilitar las versiones de TLS en vSphere Update Manager](#).

vSphere Update Manager en vCenter Server Appliance siempre se incluye con el sistema vCenter Server y el script actualiza el puerto correspondiente.

- 2 Instale la utilidad de configuración de TLS en vCenter Server y Platform Services Controller. Si el entorno utiliza una instancia integrada de Platform Services Controller, la utilidad solo se instala en vCenter Server.
- 3 Ejecute la utilidad en vCenter Server.
- 4 Ejecute la utilidad en cada host ESXi que se administra mediante vCenter Server. Puede realizar esta tarea para cada host o para todos los hosts de un clúster.
- 5 Si el entorno utiliza una o varias instancias de Platform Services Controller, ejecute la utilidad en cada instancia.

### Requisitos previos

Esta configuración se realiza en los sistemas que ejecutan vSphere 6.0 U3 y en los sistemas que ejecutan vSphere 6.5. Hay dos opciones disponibles.

- Deshabilite TLS 1.0 y habilite TLS 1.1 y TLS 1.2.
- Deshabilite TLS 1.0 y TLS 1.1, y habilite TLS 1.2.



## Instalar la utilidad de configuración de TLS

Puede descargar la utilidad de configuración de TLS desde MyVMware.com e instalarla en la máquina local. Después de la instalación, hay dos scripts disponibles. Un script es para la configuración de vCenter Server y Platform Services Controller, y el otro script es para la configuración de ESXi.

En vCenter Server Appliance, los puertos de vSphere Update Manager se actualizan mediante el script. En vCenter Server, puede editar los archivos de configuración de vSphere Update Manager. Consulte [Deshabilitar las versiones de TLS en vSphere Update Manager](#).

### Requisitos previos

Se necesita una cuenta de MyVMware para descargar el script.

### Procedimiento

- 1 Inicie sesión en la cuenta de MyVMware y vaya a vSphere.
- 2 Busque el producto y la versión del producto para los cuales tiene licencia, seleccione VMware vCenter Server y haga clic en **Ir a descargas**.
- 3 Seleccione VMware vSphere Configurador de TLS y descargue el archivo siguiente.

Sistema operativo	Archivo.
Windows	VMware-vSphereTlsReconfigurator-version-build_number.x86_64.msi
Linux	VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm

#### 4 Cargue el archivo en vCenter Server e instale los scripts.

En entornos con una instancia externa de Platform Services Controller, también se carga el archivo en Platform Services Controller.

Sistema operativo	Procedimiento
Windows	<ol style="list-style-type: none"> <li>Inicie sesión como usuario con privilegios de administrador.</li> <li>Copie el archivo <code>VMware-vSphereTlsReconfigurator-version-build_number.x86_64.msi</code> que acaba de descargar.</li> <li>Instale el archivo MSI.</li> </ol>
Linux	<ol style="list-style-type: none"> <li>Conéctese al dispositivo mediante SSH e inicie sesión como usuario con privilegios para ejecutar scripts.</li> <li>Copie el archivo <code>VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm</code> en el dispositivo mediante un cliente SCP.</li> <li>Si no está habilitado el shell de Bash, ejecute los siguientes comandos. <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <pre>shell.set --enabled true shell</pre> </div> </li> <li>Vaya al directorio donde se encuentra el archivo rpm cargado y ejecute el siguiente comando. <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <pre>rpm -Uvh VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm</pre> </div> </li> </ol>

#### Resultados

Una vez concluida la instalación, encontrará los scripts en las siguientes ubicaciones.

Sistema operativo	Ubicación
Windows	<ul style="list-style-type: none"> <li>■ <code>C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</code></li> <li>■ <code>C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\EsxTlsReconfigurator</code></li> </ul>
Linux	<ul style="list-style-type: none"> <li>■ <code>/usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</code></li> <li>■ <code>/usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator</code></li> </ul>

## Realizar una copia de seguridad manual opcional

La utilidad de configuración de TLS realiza una copia de seguridad cada vez que el script modifica vCenter Server, Platform Services Controller o vSphere Update Manager. Si necesita una copia de seguridad en un directorio específico, puede realizar una copia de seguridad manual.

El directorio predeterminado es diferente para Windows y el dispositivo.

Sistema operativo	Directorio de copia de seguridad
Windows	<code>c:\users\current_user\appdata\local\temp\yearmonthdayTtime</code>
Linux	<code>/tmp/yearmonthdayTtime</code>

## Procedimiento

- 1 Cambie el directorio a vSphereTlsReconfigurator y, a continuación, al subdirectorio VcTlsReconfigurator.

Sistema operativo	Comando
Windows	<pre>C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\ cd VcTlsReconfigurator</pre>
Linux	<pre>cd /usr/lib/vmware-vSphereTlsReconfigurator/ cd VcTlsReconfigurator</pre>

- 2 Ejecute el siguiente comando para realizar una copia de seguridad en un directorio específico.

Sistema operativo	Comando
Windows	<pre>directory_path\VcTlsReconfigurator&gt; reconfigureVc backup -d backup_directory_path</pre>
Linux	<pre>directory_path/VcTlsReconfigurator&gt; ./ reconfigureVc backup -d backup_directory_path</pre>

- 3 Compruebe que la copia de seguridad se haya realizado correctamente.

Una copia de seguridad correcta es similar al siguiente ejemplo.

```
vCenter Transport Layer Security reconfigurator, version=6.0.0, build=8482376
For more information, refer to the following article: https://kb.vmware.com/kb/2148819"
Log file: "C:\ProgramData\VMware\vCenterServer\logs\vmware\vSphere-
TlsReconfigurator\VcTlsReconfigurator.log".
===== Backing up vCenter Server TLS configuration =====
Using backup directory: c:\users\admini~1\appdata\local\temp\1\20170202T054311
Backing up: vmsyslogcollector
Backing up: vspherewebclientsvc
Backing up: vmware-autodeploy-waiter
Backing up: rhttpproxy
Backing up: VMwareSTS
Backing up: VMWareDirectoryService
```

- 4 (opcional) Si debe realizar una restauración más adelante, puede ejecutar el siguiente comando.

```
reconfigure restore -d tmp_directory_or_custom_backup_directory_path
```

# Deshabilitar las versiones de TLS en los sistemas vCenter Server

Puede usar la utilidad de configuración de TLS para deshabilitar las versiones de TLS en los sistemas vCenter Server. Como parte del proceso, puede habilitar TLS 1.1 y TLS 1.2, o bien habilitar únicamente TLS 1.2.

## Requisitos previos

Asegúrese de que los hosts y los servicios que administra vCenter Server puedan comunicarse con una versión de TLS que permanezca habilitada. Para los productos que se comunican solo mediante TLS 1.0, la conectividad deja de estar disponible.

## Procedimiento

- 1 Inicie sesión en el sistema vCenter Server como usuario que puede ejecutar scripts y vaya al directorio donde está ubicado el script.

Sistema operativo	Comando
Windows	<code>cd C:\Archivos de programa\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vmwareTlsReconfigurator/VcTlsReconfigurator</code>

- 2 Ejecute el comando, según su sistema operativo y la versión de TLS que desee utilizar.

- Para deshabilitar TLS 1.0 y habilitar TLS 1.1 y TLS 1.2, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	<code>directory_path\VcTlsReconfigurator&gt; reconfigureVc update -p TLSv1.1 TLSv1.2</code>
Linux	<code>directory_path/VcTlsReconfigurator&gt; ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>

- Para deshabilitar TLS 1.0 y TLS 1.1, y habilitar únicamente TLS 1.2, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	<code>directory_path\VcTlsReconfigurator&gt; reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path/VcTlsReconfigurator&gt; ./reconfigureVc update -p TLSv1.2</code>

- 3 Si el entorno incluye otros sistemas vCenter Server, repita el proceso en cada sistema vCenter Server.
- 4 Repita la configuración en cada host ESXi y en cada instancia de Platform Services Controller.

## Deshabilitar las versiones de TLS en los hosts ESXi

Puede usar la utilidad de configuración de TLS para deshabilitar las versiones de TLS en un host ESXi. Como parte del proceso, puede habilitar TLS 1.1 y TLS 1.2, o bien habilitar únicamente TLS 1.2.

Para los hosts ESXi, se usa un script diferente que para los demás componentes del entorno de vSphere.

---

**Nota** El script deshabilita tanto TLS 1.0 como TLS 1.1, a menos que especifique la opción `-p`.

---

### Requisitos previos

Asegúrese de que los productos o los servicios asociados con el host ESXi puedan comunicarse con TLS 1.1 o TLS 1.2. Para los productos que se comunican solo mediante TLS 1.0, se pierde la conectividad.

### Procedimiento

- 1 Inicie sesión en el host vCenter Server como usuario que puede ejecutar scripts y vaya al directorio donde está ubicado el script.

Sistema operativo	Comando
Windows	<code>C:\Program Files\VMware\CIS\vsphereTLSReconfigurator\EsxTlsReconfigurator</code>
Linux	<code>/usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator</code>

- 2 Para deshabilitar TLS en todos los hosts de un clúster, ejecute uno de los siguientes comandos.
  - Para deshabilitar TLS 1.0 y habilitar TLS 1.1 y TLS 1.2 en todos los hosts de un clúster, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	<code>reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- Para deshabilitar TLS 1.0 y TLS 1.1, y habilitar únicamente TLS 1.2 en todos los hosts de un clúster, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	<code>reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2</code>

### 3 Para deshabilitar TLS en un host individual, ejecute uno de los siguientes comandos.

- Para deshabilitar TLS 1.0 y habilitar TLS 1.1 y TLS 1.2 en un host individual, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	<code>reconfigureEsx vCenterHost -h &lt;ESXi_Host_Name&gt; -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h &lt;ESXi_Host_Name&gt; -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- Para deshabilitar TLS 1.0 y TLS 1.1, y habilitar únicamente TLS 1.2 en un host individual, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	<code>reconfigureEsx vCenterHost -h &lt;ESXi_Host_Name&gt; -u Administrative_User -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h &lt;ESXi_Host_Name&gt; -u Administrative_User -p TLSv1.2</code>

### 4 Reinicie el host ESXi para completar los cambios del protocolo TLS.

## Deshabilitar las versiones de TLS en los sistemas Platform Services Controller

Si el entorno incluye uno o varios sistemas Platform Services Controller, puede usar la utilidad de configuración de TLS para cambiar las versiones de TLS que deben admitirse.

Si el entorno solo utiliza una instancia integrada de Platform Services Controller, no es necesario realizar esta tarea.

**Nota** Continúe con esta tarea solo después de confirmar que cada sistema vCenter Server ejecuta una versión compatible de TLS. Si las instancias de vCenter Server 6.0.x o 5.5.x están conectadas a vCenter Server, esas instancias dejan de comunicarse con Platform Services Controller si se deshabilitan las versiones de TLS.

Puede deshabilitar TLS 1.0 y TLS 1.1, y dejar TLS 1.2 habilitado, o bien puede deshabilitar solo TLS 1.0 y dejar TLS 1.1 y TLS 1.2 habilitados.

### Requisitos previos

Asegúrese de que los hosts y los servicios a los que se conecta Platform Services Controller puedan comunicarse mediante un protocolo compatible. Debido a que la autenticación y la administración de certificados se controlan mediante Platform Services Controller, evalúe detenidamente qué servicios pueden verse afectados. Para los servicios que se comunican solamente mediante protocolos no compatibles, la conectividad deja de estar disponible.

### Procedimiento

- 1 Inicie sesión en Platform Services Controller como usuario que puede ejecutar scripts y vaya al directorio donde está ubicado el script.

Sistema operativo	Comando
Windows	<code>cd C:\Archivos de programa\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</code>

- 2 Puede realizar la tarea en Platform Services Controller en Windows o en el dispositivo de Platform Services Controller.

- Para deshabilitar TLS 1.0 y habilitar TLS 1.1 y TLS 1.2, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	<code>directory_path\VcTlsReconfigurator&gt; reconfigureVc update -p TLSv1.1 TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator&gt; ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>

- Para deshabilitar TLS 1.0 y TLS 1.1, y habilitar únicamente TLS 1.2, ejecute el siguiente comando.

Sistema operativo	Comando
Windows	<code>directory_path\VcTlsReconfigurator&gt; reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator&gt; ./reconfigureVc update -p TLSv1.2</code>

- 3 Si el entorno incluye otros sistemas Platform Services Controller, repita el proceso.

## Revertir los cambios de configuración de TLS

Puede usar la utilidad de configuración de TLS para revertir los cambios de configuración. Al revertir los cambios, el sistema habilita los protocolos que se deshabilitaron mediante la utilidad de configuración de TLS.

Solo se puede llevar a cabo una recuperación si anteriormente se realizó una copia de seguridad de la configuración. No es posible revertir los cambios en los hosts ESXi.

Realice la recuperación en este orden.

- 1 vSphere Update Manager.

Si el entorno ejecuta una instancia de vSphere Update Manager distinta en un sistema Windows, primero es necesario actualizar vSphere Update Manager.

- 2 vCenter Server
- 3 Platform Services Controller

### Procedimiento

- 1 Conéctese al equipo Windows o al dispositivo.



## 2 Inicie sesión en el sistema donde desee revertir los cambios.

Sistema operativo	Procedimiento
Windows	<ol style="list-style-type: none"> <li>1 Inicie sesión como usuario con privilegios de administrador.</li> <li>2 Vaya al directorio <code>VcTlsReconfigurator</code>. <div> <pre>cd C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</pre> </div> </li> </ol>
Linux	<ol style="list-style-type: none"> <li>1 Conéctese al dispositivo mediante SSH e inicie sesión como usuario con privilegios para ejecutar scripts.</li> <li>2 Si no está habilitado el shell de Bash, ejecute los siguientes comandos. <div> <pre>shell.set --enabled true shell</pre> </div> </li> <li>3 Vaya al directorio <code>VcTlsReconfigurator</code>. <div> <pre>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</pre> </div> </li> </ol>

## 3 Revise la copia de seguridad anterior.

Sistema operativo	Procedimiento
Windows	<div> <pre>C:\ProgramData\VMware\vCenterServer\logs\vsphere-TlsReconfigurator\VcTlsReconfigurator.log</pre> </div> <p>El resultado es similar al siguiente ejemplo.</p> <div> <pre>c:\users\username\AppData\Local\Temp\20161108T161539 c:\users\username\AppData\Local\Temp\20161108T171539</pre> </div>
Linux	<div> <pre>grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log</pre> </div> <p>El resultado es similar al siguiente ejemplo.</p> <div> <pre>2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920 2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259</pre> </div>

- 4 Ejecute uno de los siguientes comandos para realizar una restauración.

Sistema operativo	Procedimiento
Windows	<pre>reconfigureVc restore -d <i>Directory_path_from_previous_step</i></pre> <p>Por ejemplo</p> <pre>reconfigureVc restore -d c:\users\username\appdata\local\temp\20161108T171539</pre>
Linux	<pre>reconfigureVc restore -d <i>Directory_path_from_previous_step</i></pre> <p>Por ejemplo</p> <pre>reconfigureVc restore -d /tmp/20161117T172920</pre>

- 5 Repita el procedimiento en cualquier otra instancia de vCenter Server.
- 6 Repita el procedimiento en cualquier otra instancia de Platform Services Controller.

## Deshabilitar las versiones de TLS en vSphere Update Manager

En vSphere Update Manager 6.0 Update 3 y versiones posteriores, las versiones de protocolo TLS 1.0, 1.1 y 1.2 están habilitadas de forma predeterminada. Es posible deshabilitar TLS versión 1.0 y TLS versión 1.1, pero no se puede deshabilitar TLS versión 1.2.

Puede administrar la configuración del protocolo TLS para otros servicios con la utilidad de configuración de TLS. Sin embargo, para vSphere Update Manager, debe volver a configurar el protocolo TLS manualmente.

La modificación de la configuración del protocolo TLS podría implicar cualquiera de las siguientes tareas.

- Deshabilitar TLS versión 1.0 y dejar habilitados TLS versión 1.1 y TLS 1.2.
- Deshabilitar TLS versión 1.0 y TLS versión 1.1, y dejar habilitado TLS versión 1.2.
- Volver a habilitar una versión de protocolo TLS deshabilitada.

## Deshabilitar las versiones anteriores de TLS para Update Manager, puerto 9087

Para deshabilitar las versiones anteriores de TLS para el puerto 9087, modifique el archivo de configuración `jetty-vum-ssl.xml`. El proceso es diferente para el puerto 8084.

**Nota** Antes de deshabilitar una versión de TLS, asegúrese de que ninguno de los servicios que se comunican con vSphere Update Manager utilice esa versión.

## Requisitos previos

Detenga el servicio de vSphere Update Manager. Consulte la documentación de *Instalación y administración de VMware vSphere Update Manager*.

## Procedimiento

- 1 Detenga el servicio de vSphere Update Manager.
- 2 Desplácese hasta el directorio de instalación de Update Manager, que es diferente para vSphere 6.0 y vSphere 6.5.

Versión	Ubicación
vSphere 6.0	C:\Archivos de programa (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Archivos de programa\VMware\Infrastructure\Update Manager

- 3 Realice una copia de seguridad del archivo `jetty-vum-ssl.xml` y abra el archivo.
- 4 Para deshabilitar las versiones anteriores de TLS, cambie el archivo.

Opción	Descripción
<b>Deshabilite TLS 1.0. Deje TLS 1.1 y TLS 1.2 habilitados.</b>	<pre>&lt;Set name="ExcludeProtocols"&gt;   &lt;Array type="java.lang.String"&gt;     &lt;Item&gt;TLSv1&lt;/Item&gt;   &lt;/Array&gt; &lt;/Set&gt;</pre>
<b>Deshabilite TLS 1.0 y TLS 1.1. Deje TLS 1.2 habilitado.</b>	<pre>&lt;Set name="ExcludeProtocols"&gt;   &lt;Array type="java.lang.String"&gt;     &lt;Item&gt;TLSv1&lt;/Item&gt;     &lt;Item&gt;TLSv1.1&lt;/Item&gt;   &lt;/Array&gt; &lt;/Set&gt;</pre>

- 5 Guarde el archivo.
- 6 Reinicie el servicio de vSphere Update Manager.

## Deshabilitar las versiones anteriores de TLS para Update Manager, puerto 8084

Para deshabilitar las versiones anteriores de TLS del puerto 8084, modifique el archivo de configuración `vci-integrity.xml`. El proceso es diferente para el puerto 9087.

**Nota** Antes de deshabilitar una versión de TLS, asegúrese de que ninguno de los servicios que se comunican con vSphere Update Manager utilice esa versión.

## Requisitos previos

Detenga el servicio de vSphere Update Manager. Consulte la documentación de *Instalación y administración de VMware vSphere Update Manager*.

## Procedimiento

- 1 Detenga el servicio de vSphere Update Manager.
- 2 Desplácese hasta el directorio de instalación de Update Manager, que es diferente para 6.0 y 6.5.

Versión	Ubicación
vSphere 6.0	C:\Archivos de programa (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Archivos de programa\VMware\Infrastructure\Update Manager

- 3 Realice una copia de seguridad del archivo `vci-integrity.xml` y abra el archivo.
- 4 Agregue la etiqueta `<sslOptions>` en el archivo `vci-integrity.xml`.

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

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

- 5 Según la versión de TLS que desee deshabilitar, utilice uno de los siguientes valores decimales en la etiqueta `<sslOptions>`.
  - Para deshabilitar solo TLS v1.0, utilice el valor decimal 117587968.
  - Para deshabilitar TLS v1.0 y TLS v1.1, utilice el valor decimal 386023424.
- 6 Guarde el archivo.
- 7 Reinicie el servicio de vSphere Update Manager.

## Volver a habilitar las versiones de TLS deshabilitadas para el puerto 9087 de Update Manager

Si deshabilita una versión de TLS para el puerto 9087 de Update Manager y tiene problemas, puede volver a habilitar la versión. El proceso es diferente para volver a habilitar el puerto 8084.

Volver a habilitar una versión anterior de TLS tiene implicaciones de seguridad.

**Procedimiento**

- 1 Detenga el servicio de vSphere Update Manager.
- 2 Desplácese hasta el directorio de instalación de Update Manager, que es diferente para 6.0 y 6.5.

Versión	Ubicación
vSphere 6.0	C:\Archivos de programa (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Archivos de programa\VMware\Infrastructure\Update Manager

- 3 Realice una copia de seguridad del archivo `jetty-vum-ssl.xml` y abra el archivo.
- 4 Elimine la etiqueta de TLS que corresponde a la versión de protocolo TLS que desea habilitar. Por ejemplo, elimine `<Item>TLSv1.1</Item>` en el archivo `jetty-vum-ssl.xml` para habilitar TLS v1.1.
- 5 Guarde el archivo.
- 6 Reinicie el servicio de vSphere Update Manager.

## Volver a habilitar las versiones de TLS deshabilitadas para el puerto 8084 de Update Manager

Si deshabilita una versión de TLS para el puerto 8084 de Update Manager y tiene problemas, puede volver a habilitar la versión. El proceso es diferente para el puerto 9087.

Volver a habilitar una versión anterior de TLS tiene implicaciones de seguridad.

**Procedimiento**

- 1 Detenga el servicio de vSphere Update Manager.
- 2 Desplácese hasta el directorio de instalación de Update Manager, que es diferente para 6.0 y 6.5.

Versión	Ubicación
vSphere 6.0	C:\Archivos de programa (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Archivos de programa\VMware\Infrastructure\Update Manager

- 3 Realice una copia de seguridad del archivo `vci-integrity.xml` y abra el archivo.
- 4 Cambie el valor decimal que se utiliza en la etiqueta `<sslOptions>` o elimine la etiqueta para permitir todas las versiones de TLS.
  - Para habilitar TLS 1.1, pero dejar TLS 1.0 deshabilitado, utilice el valor decimal 117587968.
  - Para volver a habilitar TLS 1.1 y TLS 1.0, elimine la etiqueta.

- 5 Guarde el archivo.
- 6 Reinicie el servicio de vSphere Update Manager.

# Privilegios definidos

# 11

En las siguientes tablas se enumeran los privilegios predeterminados que, cuando se seleccionan para una función, pueden asignarse a un usuario y a un objeto. En las tablas de este apéndice se usa VC para indicar vCenter Server y HC para indicar cliente de host, un host ESXi o de Workstation independiente.

Al establecer permisos, verifique que todos los tipos de objetos estén configurados con los privilegios adecuados para cada acción en particular. Algunas operaciones requieren permiso de acceso en la carpeta raíz o la carpeta primaria además del acceso al objeto que se manipula. Algunas operaciones requieren permiso de acceso o ejecución en la carpeta primaria y un objeto relacionado.

Las extensiones de vCenter Server pueden definir privilegios adicionales que no están indicados aquí. Consulte la documentación relacionada con las extensiones para obtener más información sobre estos privilegios.

Este capítulo incluye los siguientes temas:

- [Privilegios de alarmas](#)
- [Privilegios de Auto Deploy y perfiles de imagen](#)
- [Privilegios de los certificados](#)
- [Privilegios de la biblioteca de contenido](#)
- [Privilegios de centro de datos](#)
- [Privilegios de almacenes de datos](#)
- [Privilegios de clústeres de almacenes de datos](#)
- [Privilegios de Distributed Switch](#)
- [Privilegios de ESX Agent Manager](#)
- [Privilegios de extensiones](#)
- [Privilegios de carpeta](#)
- [Privilegios globales](#)
- [Privilegios de CIM para hosts](#)
- [Privilegios de configuración de hosts](#)

- Inventario del host
- Privilegios de operaciones locales en hosts
- Privilegios de vSphere Replication de host
- Privilegios de perfiles de host
- Privilegios de proveedor de Inventory Service
- Privilegios de etiquetado de Inventory Service
- Privilegios de red
- Privilegios de rendimiento
- Privilegios de permisos
- Privilegios de almacenamiento basado en perfiles
- Privilegios de recursos
- Privilegios para tareas programadas
- Privilegios de sesiones
- Privilegios de vistas de almacenamiento
- Privilegios de tareas
- Privilegios del servicio de transferencia
- Privilegios de directivas de VRM
- Privilegios de configuración de máquinas virtuales
- Privilegios de operaciones de invitado de máquina virtual
- Privilegios para la interacción con máquinas virtuales
- Privilegios de inventario de máquinas virtuales
- Privilegios de aprovisionamiento de las máquinas virtuales
- Privilegios de configuración de servicios de la máquina virtual
- Privilegios de administración de snapshots de las máquinas virtuales
- Privilegios de vSphere Replication de máquinas virtuales
- Privilegios de grupo dvPort
- Privilegios de vApp
- Privilegios de vServices

## Privilegios de alarmas

Los privilegios de alarmas controlan la capacidad de crear alarmas, modificarlas y responder a ellas en objetos de inventario.



Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-1. Privilegios de alarmas**

Nombre del privilegio	Descripción	Necesario para
<b>Alarms.Acknowledge alarm</b>	Permite eliminar todas las acciones de todas las alarmas activadas.	Objeto en el que se define una alarma
<b>Alarms.Create alarm</b>	Permite crear una alarma nueva. Al crear alarmas con una acción personalizada, se comprueba el privilegio de realizar la acción cuando el usuario crea la alarma.	Objeto en el que se define una alarma
<b>Alarms.Disable alarm action</b>	Permite evitar que se produzca una acción de alarma después de que se activa la alarma. Esto no deshabilita la alarma.	Objeto en el que se define una alarma
<b>Alarms.Modify alarm</b>	Permite cambiar las propiedades de una alarma.	Objeto en el que se define una alarma
<b>Alarms.Remove alarm</b>	Permite eliminar una alarma.	Objeto en el que se define una alarma
<b>Alarms.Set alarm status</b>	Permite cambiar el estado de la alarma de evento configurada. El estado puede cambiar a <b>Normal</b> , <b>Advertencia</b> o <b>Alerta</b> .	Objeto en el que se define una alarma

## Privilegios de Auto Deploy y perfiles de imagen

Los privilegios de Auto Deploy determinan quién puede realizar ciertas tareas en las reglas de Auto Deploy, y quién puede asociar un host. Los privilegios de Auto Deploy también permiten controlar quién puede crear o editar un perfil de imagen.

En la tabla se describen los privilegios que determinan quién puede administrar las reglas y los conjuntos de reglas de Auto Deploy, y quién puede crear y editar perfiles de imagen. Consulte *Instalación y configuración de vSphere*.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-2. Privilegios de Auto Deploy

Nombre del privilegio	Descripción	Necesario para
Auto Deploy.Host.Equipo asociado	Permite a los usuarios asociar un host a una máquina.	vCenter Server
Auto Deploy.Perfil de imagen .Crear	Permite crear perfiles de imagen.	vCenter Server
Auto Deploy.Perfil de imagen .Editar	Permite editar perfiles de imagen.	vCenter Server
Auto Deploy.Regla .Crear	Permite crear reglas de Auto Deploy.	vCenter Server
Auto Deploy.Regla .Eliminar	Permite eliminar reglas de Auto Deploy.	vCenter Server
Auto Deploy.Regla.Editar	Permite editar reglas de Auto Deploy.	vCenter Server
Auto Deploy.Conjunto de reglas .Activar	Permite activar conjuntos de reglas de Auto Deploy.	vCenter Server
Auto Deploy.Conjunto de reglas .Editar	Permite editar conjuntos de reglas de Auto Deploy.	vCenter Server

## Privilegios de los certificados

Los privilegios de los certificados controlan qué usuarios pueden administrar los certificados de ESXi.

Este privilegio determina quién puede administrar los certificados de los hosts de ESXi.

Consulte [Privilegios necesarios para operaciones de administración de certificados](#) para obtener información sobre cómo administrar certificados de vCenter Server.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-3. Privilegios de los certificados de los hosts**

Nombre del privilegio	Descripción	Necesario para
<b>Certificados. Administrar certificados</b>	Permite administrar los certificados de los hosts de ESXi.	vCenter Server

## Privilegios de la biblioteca de contenido

Las bibliotecas de contenido ofrecen administración simple y efectiva de plantillas de máquinas virtuales y vApps. Los privilegios de bibliotecas de contenido determinan quién puede ver o administrar diferentes aspectos de las bibliotecas de contenido.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-4. Privilegios de la biblioteca de contenido**

Nombre del privilegio	Descripción	Necesario para
<b>Biblioteca de contenido. Agregar elemento de biblioteca</b>	Permite agregar elementos a una biblioteca.	Biblioteca
<b>Biblioteca de contenido. Crear biblioteca local</b>	Permite crear bibliotecas locales en el sistema vCenter Server especificado.	vCenter Server
<b>Biblioteca de contenido. Crear biblioteca suscrita</b>	Permite crear bibliotecas suscritas.	vCenter Server
<b>Biblioteca de contenido. Eliminar elemento de biblioteca</b>	Permite eliminar elementos de biblioteca.	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.
<b>Biblioteca de contenido. Eliminar biblioteca local</b>	Permite borrar una biblioteca local.	Biblioteca

Tabla 11-4. Privilegios de la biblioteca de contenido (continuación)

Nombre del privilegio	Descripción	Necesario para
<b>Biblioteca de contenido. Eliminar biblioteca suscrita</b>	Permite borrar una biblioteca suscrita.	Biblioteca
<b>Biblioteca de contenido. Descargar archivos</b>	Permite descargar archivos de la biblioteca de contenido.	Biblioteca
<b>Biblioteca de contenido. Desalojar elemento de biblioteca</b>	Permite expulsar elementos. El contenido de una biblioteca suscrita puede estar almacenado en caché o no. Si el contenido está almacenado en caché, puede expulsar un elemento de biblioteca para quitarlo (si tiene el privilegio correspondiente).	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.
<b>Biblioteca de contenido. Desalojar biblioteca suscrita</b>	Permite expulsar una biblioteca suscrita. El contenido de una biblioteca suscrita puede estar almacenado en caché o no. Si el contenido está almacenado en caché, puede expulsar una biblioteca para quitarla (si tiene el privilegio correspondiente).	Biblioteca
<b>Biblioteca de contenido. Importar almacenamiento</b>	Permite a un usuario importar un elemento de biblioteca si la dirección URL del archivo de origen empieza con ds:// o file://. De forma predeterminada, este privilegio está deshabilitado para el administrador de bibliotecas de contenido, ya que una importación desde una dirección URL de almacenamiento implica la importación de contenido. Habilite este privilegio solo si es necesario y si no hay riesgos de seguridad con el usuario que realizará la importación.	Biblioteca
<b>Biblioteca de contenido. Sondear información de suscripción</b>	Este privilegio permite a las API y los usuarios de soluciones sondear la información de suscripción de una biblioteca remota, como su dirección URL, certificado SSL y contraseña. La estructura que se obtiene describe si la configuración de suscripción es correcta o si hay problemas, como errores de SSL.	Biblioteca
<b>Biblioteca de contenido. Leer almacenamiento</b>	Permite leer el almacenamiento de una biblioteca de contenido.	Biblioteca
<b>Biblioteca de contenido. Sincronizar elemento de biblioteca</b>	Permite sincronizar elementos de biblioteca.	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.
<b>Biblioteca de contenido. Sincronizar biblioteca suscrita</b>	Permite sincronizar bibliotecas suscritas.	Biblioteca
<b>Biblioteca de contenido. Escribir introspección</b>	Permite a un usuario de solución o a una API revisar los complementos de compatibilidad de tipos del servicio de biblioteca de contenido.	Biblioteca
<b>Biblioteca de contenido. Actualizar parámetros de configuración</b>	Permite actualizar los valores de configuración. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	Biblioteca
<b>Biblioteca de contenido. Actualizar archivos</b>	Permite cargar contenido a la biblioteca de contenido. También permite eliminar archivos de un elemento de biblioteca.	Biblioteca

Tabla 11-4. Privilegios de la biblioteca de contenido (continuación)

Nombre del privilegio	Descripción	Necesario para
<b>Biblioteca de contenido. Actualizar biblioteca</b>	Permite actualizar la biblioteca de contenido.	Biblioteca
<b>Biblioteca de contenido. Actualizar elemento de biblioteca</b>	Permite actualizar elementos de biblioteca.	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.
<b>Biblioteca de contenido. Actualizar biblioteca local</b>	Permite actualizar bibliotecas locales.	Biblioteca
<b>Biblioteca de contenido. Actualizar biblioteca suscrita</b>	Permite actualizar las propiedades de una biblioteca suscrita.	Biblioteca
<b>Biblioteca de contenido. Ver parámetros de configuración</b>	Permite ver las opciones de configuración. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	Biblioteca

## Privilegios de centro de datos

Los privilegios de centro de datos controlan la habilidad para crear y editar centros de datos en el inventario vSphere Web Client.

Todos los privilegios de centros de datos se utilizan solamente en vCenter Server. El privilegio **Crear centro de datos** se define en carpetas del centro de datos o el objeto raíz. Todos los demás privilegios de centros de datos se emparejan con centros de datos, carpetas de centros de datos o el objeto raíz.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-5. Privilegios de centro de datos

Nombre del privilegio	Descripción	Necesario para
<b>Datacenter.Create datacenter</b>	Permite la creación de un nuevo centro de datos.	Carpeta de centro de datos u objeto raíz
<b>Datacenter.Move datacenter</b>	Permite mover un centro de datos. El privilegio debe estar presente tanto en el origen como en el destino.	Centro de datos, origen y destino
<b>Datacenter.Network protocol profile configuration</b>	Permite la configuración del perfil de red para un centro de datos.	Centro de datos
<b>Datacenter.Query IP pool allocation</b>	Permite la configuración de un grupo de direcciones IP.	Centro de datos

Tabla 11-5. Privilegios de centro de datos (continuación)

Nombre del privilegio	Descripción	Necesario para
<b>Datacenter.Reconfigure datacenter</b>	Permite la reconfiguración de un centro de datos.	Centro de datos
<b>Datacenter.Release IP allocation</b>	Permite liberar la asignación de IP asignada para un centro de datos.	Centro de datos
<b>Datacenter.Remove datacenter</b>	Permite la eliminación de un centro de datos. Para tener los permisos necesarios para realizar esta operación, debe tener este privilegio asignado tanto en el objeto como en su objeto primario.	Centro de datos más objeto primario
<b>Datacenter.Rename datacenter</b>	Permite cambiarle el nombre a un centro de datos.	Centro de datos

## Privilegios de almacenes de datos

Los privilegios de almacenes de datos controlan la capacidad para examinar y administrar almacenes de datos, así como para asignar espacios en ellos.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-6. Privilegios de almacenes de datos

Nombre del privilegio	Descripción	Necesario para
<b>Datastore.Allocate space</b>	Permite asignar un espacio en un almacén de datos de una máquina virtual, una instantánea, un clon o un disco virtual.	Almacenes de datos
<b>Datastore.Browse datastore</b>	Permite desplazarse hasta archivos de un almacén de datos.	Almacenes de datos
<b>Datastore.Configure datastore</b>	Permite configurar un almacén de datos.	Almacenes de datos
<b>Datastore.Low level file operations</b>	Permite realizar tareas de lectura, escritura, eliminación y cambio de nombre en el explorador del almacén de datos.	Almacenes de datos
<b>Datastore.Move datastore</b>	Permite mover un almacén de datos entre diferentes carpetas. Los privilegios deben estar presentes tanto en el origen como en el destino.	Almacén de datos, origen y destino
<b>Datastore.Remove datastore</b>	Permite quitar un almacén de datos. Este privilegio es obsoleto. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Almacenes de datos
<b>Datastore.Remove file</b>	Permite eliminar archivos del almacén de datos. Este privilegio es obsoleto. Asigne el privilegio <b>Operaciones de archivos de nivel bajo</b> .	Almacenes de datos

Tabla 11-6. Privilegios de almacenes de datos (continuación)

Nombre del privilegio	Descripción	Necesario para
<b>Datastore.Rename datastore</b>	Permite cambiar el nombre de un almacén de datos.	Almacenes de datos
<b>Datastore.Update virtual machine files</b>	Permite actualizar las rutas de acceso de los archivos de máquinas virtuales en un almacén de datos una vez que el almacén de datos se volvió a firmar.	Almacenes de datos
<b>Datastore.Update virtual machine metadata</b>	Permite actualizar los metadatos de máquina virtual asociados con un almacén de datos.	Almacenes de datos

## Privilegios de clústeres de almacenes de datos

Los privilegios de clústeres de almacenes de datos controlan la configuración de clústeres de almacenes de datos de Storage DRS.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-7. Privilegios de clústeres de almacenes de datos

Nombre del privilegio	Descripción	Necesario para
<b>Datastore cluster.Configure a datastore cluster</b>	Permite crear y configurar parámetros para los clústeres de almacenes de datos de Storage DRS.	Clústeres de almacenes de datos

## Privilegios de Distributed Switch

Los privilegios de Distributed Switch controlan la capacidad para realizar tareas relacionadas con la administración de las instancias de Distributed Switch.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-8. Privilegios de vSphere Distributed Switch

Nombre del privilegio	Descripción	Necesario para
<b>Distributed switch.Create</b>	Permite crear un conmutador distribuido.	Centros de datos, carpetas de red
<b>Distributed switch.Delete</b>	Permite quitar un conmutador distribuido. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Conmutadores distribuidos

Tabla 11-8. Privilegios de vSphere Distributed Switch (continuación)

Nombre del privilegio	Descripción	Necesario para
<b>Distributed switch.Host operation</b>	Permite cambiar los miembros de host de un conmutador distribuido.	Conmutadores distribuidos
<b>Distributed switch.Modify</b>	Permite cambiar la configuración de un conmutador distribuido.	Conmutadores distribuidos
<b>Distributed switch.Move</b>	Permite mover vSphere Distributed Switch a otra carpeta.	Conmutadores distribuidos
<b>Distributed switch.Network I/O control operation</b>	Permite cambiar la configuración de los recursos de vSphere Distributed Switch.	Conmutadores distribuidos
<b>Distributed switch.Policy operation</b>	Permite cambiar la directiva de vSphere Distributed Switch.	Conmutadores distribuidos
<b>Distributed switch .Port configuration operation</b>	Permite cambiar los parámetros de un puerto en vSphere Distributed Switch.	Conmutadores distribuidos
<b>Distributed switch.Port setting operation</b>	Permite cambiar la configuración de un puerto en vSphere Distributed Switch.	Conmutadores distribuidos
<b>Distributed switch.VSPAN operation</b>	Permite cambiar la configuración de VSPAN de vSphere Distributed Switch.	Conmutadores distribuidos

## Privilegios de ESX Agent Manager

Los privilegios de ESX Agent Manager controlan las operaciones relacionadas con ESX Agent Manager y las máquinas virtuales de agentes. ESX Agent Manager es un servicio que permite instalar máquinas virtuales de administración asociadas a un host que no se ven afectadas por VMware DRS u otros servicios de migración de máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-9. ESX Agent Manager

Nombre del privilegio	Descripción	Necesario para
<b>ESX Agent Manager.Config</b>	Permite implementar la máquina virtual de un agente en un host o un clúster.	Máquinas virtuales
<b>ESX Agent Manager.Modify</b>	Permite modificar la máquina virtual de un agente, por ejemplo, apagar o eliminar la máquina virtual.	Máquinas virtuales
<b>ESX Agent View.View</b>	Permite ver la máquina virtual de un agente.	Máquinas virtuales

## Privilegios de extensiones

Los privilegios de extensiones controlan la capacidad para instalar y administrar extensiones.



Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-10. Privilegios de extensiones**

Nombre del privilegio	Descripción	Necesario para
<b>Extension.Register extension</b>	Permite registrar una extensión (complemento).	vCenter Server raíz
<b>Extension.Unregister extension</b>	Permite anular el registro de una extensión (complemento).	vCenter Server raíz
<b>Extension.Update extension</b>	Permite actualizar una extensión (complemento).	vCenter Server raíz

## Privilegios de carpeta

Estos privilegios controlan la capacidad para crear y administrar carpetas.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-11. Privilegios de carpeta**

Nombre del privilegio	Descripción	Necesario para
<b>Folder.Create folder</b>	Permite crear una carpeta nueva.	Carpetas
<b>Folder.Delete folder</b>	Permite eliminar una carpeta. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Carpetas
<b>Folder.Move folder</b>	Permite mover una carpeta. El privilegio debe estar presente tanto en el origen como en el destino.	Carpetas
<b>Folder.Rename folder</b>	Permite cambiarle el nombre a una carpeta.	Carpetas

## Privilegios globales

Los privilegios globales controlan tareas globales relacionadas con tareas, scripts y extensiones.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-12. Privilegios globales

Nombre del privilegio	Descripción	Necesario para
<b>Global.Act as vCenter Server</b>	Permite preparar e iniciar una operación de envío o recepción de vMotion.	vCenter Server raíz
<b>Global.Cancel task</b>	Permite cancelar una tarea en cola o en ejecución.	Objeto de inventario relacionado con la tarea
<b>Global.Capacity planning</b>	Permite habilitar el uso de la planificación de capacidad para la consolidación de planificación de máquinas físicas en máquinas virtuales.	vCenter Server raíz
<b>Global.Diagnostics</b>	Permite recuperar una lista de archivos de diagnóstico, encabezados de registro, archivos binarios o paquetes de diagnóstico.  Para evitar infracciones de seguridad potenciales, limite este privilegio a la función de administrador de vCenter Server.	vCenter Server raíz
<b>Global.Disable methods</b>	Permite a los servidores de las extensiones de vCenter Server deshabilitar ciertas operaciones en objetos administrados con vCenter Server.	vCenter Server raíz
<b>Global.Enable methods</b>	Permite a los servidores de las extensiones de vCenter Server habilitar ciertas operaciones en objetos administrados con vCenter Server.	vCenter Server raíz
<b>Global.Global tag</b>	Permite agregar o quitar etiquetas globales.	Host raíz o vCenter Server
<b>Global.Health</b>	Permite ver el estado de los componentes de vCenter Server.	vCenter Server raíz
<b>Global.Licenses</b>	Permite ver las licencias instaladas y agregar o quitar licencias.	Host raíz o vCenter Server
<b>Global.Log event</b>	Permite registrar un evento definido por el usuario ante una entidad administrada en particular.	Cualquier objeto
<b>Global.Manage custom attributes</b>	Permite agregar y quitar definiciones de campo personalizadas, así como cambiar sus nombres.	vCenter Server raíz
<b>Global.Proxy</b>	Permite acceder a una interfaz interna para agregar o quitar puntos extremos en el proxy o desde él.	vCenter Server raíz
<b>Global.Script action</b>	Permite programar una acción generada por script junto con una alarma.	Cualquier objeto
<b>Global.Service managers</b>	Permite utilizar el comando <code>resxtop</code> en vSphere CLI.	Host raíz o vCenter Server
<b>Global.Set custom attribute</b>	Permite ver, crear o quitar atributos personalizados para un objeto administrado.	Cualquier objeto
<b>Global.Settings</b>	Permite leer y modificar las opciones de configuración de vCenter Server de tiempo de ejecución.	vCenter Server raíz
<b>Global.System tag</b>	Permite agregar o quitar etiquetas de sistema.	vCenter Server raíz

## Privilegios de CIM para hosts

Los privilegios de CIM para hosts controlan el uso de CIM para supervisar el estado de los hosts.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-13. Privilegios de CIM para hosts**

Nombre del privilegio	Descripción	Necesario para
Host.CIM.CIM Interaction	Permite que un cliente obtenga un vale para usar los servicios de CIM.	Hosts

## Privilegios de configuración de hosts

Los privilegios de configuración de hosts controlan la capacidad para configurar hosts.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-14. Privilegios de configuración de hosts**

Nombre del privilegio	Descripción	Necesario para
Host.Configuration.Advanced Settings	Permite establecer las opciones de configuración avanzada del host.	Hosts
Host.Configuration.Authentication Store	Permite configurar los almacenes de autenticación de Active Directory.	Hosts
Host.Configuration.Change PciPassthru settings	Permite cambiar la configuración de PciPassthru de un host.	Hosts
Host.Configuration.Change SNMP settings	Permite cambiar la configuración de SNMP de un host.	Hosts
Host.Configuration.Change date and time settings	Permite cambiar la configuración de fecha y hora de un host.	Hosts
Host.Configuration.Change settings	Permite configurar el modo de bloqueo de los hosts ESXi.	Hosts
Host.Configuration.Connection	Permite cambiar el estado de conexión de un host (conectado o desconectado).	Hosts
Host.Configuration.Firmware	Permite actualizar el firmware del host ESXi.	Hosts
Host.Configuration.Hyperthreading	Permite habilitar y deshabilitar la función de hiperproceso en el programador de la CPU del host.	Hosts
Host.Configuration.Image configuration	Permite cambiar la imagen asociada a un host.	

Tabla 11-14. Privilegios de configuración de hosts (continuación)

Nombre del privilegio	Descripción	Necesario para
Host.Configuration.Maintenance	Permite que el host entre y salga del modo de mantenimiento, y apagar y reiniciar el host.	Hosts
Host.Configuration.Memory configuration	Permite modificar la configuración del host.	Hosts
Host.Configuration.Network configuration	Permite configurar la red, el firewall y la red vMotion.	Hosts
Host.Configuration.Power	Permite configurar las opciones de administración de energía del host.	Hosts
Host.Configuration.Query patch	Permite consultar las revisiones instalables e instalar revisiones en el host.	Hosts
Host.Configuration.Security profile and firewall	Permite configurar los servicios de Internet, como SSH, Telnet, SNMP y del firewall del host.	Hosts
Host.Configuration.Storage partition configuration	Permite administrar la partición de diagnóstico y el almacén de datos de VMFS. Los usuarios con este privilegio pueden examinar dispositivos de almacenamiento nuevos y administrar iSCSI.	Hosts
Host.Configuration.System Management	Permite que las extensiones manipulen el sistema de archivos del host.	Hosts
Host.Configuration.System resources	Permite actualizar la configuración de la jerarquía de recursos del sistema.	Hosts
Host.Configuration.Virtual machine autostart configuration	Permite cambiar el orden de inicio e interrupción automáticos de las máquinas virtuales de un solo host.	Hosts

## Inventario del host

Los privilegios de inventario de host controlan las operaciones de agregar hosts al inventario y a los clústeres, y de mover los hosts en el inventario.

En la tabla se describen los privilegios necesarios para agregar y mover hosts y clústeres en el inventario.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-15. Privilegios de inventario de host

Nombre del privilegio	Descripción	Necesario para
Host.Inventory.Add host to cluster	Permite agregar un host a un clúster que ya existe.	Clústeres
Host.Inventory.Add standalone host	Permite agregar un host independiente.	Carpetas de hosts

Tabla 11-15. Privilegios de inventario de host (continuación)

Nombre del privilegio	Descripción	Necesario para
<b>Host.Inventory.Create cluster</b>	Permite crear un nuevo clúster.	Carpetas de hosts
<b>Host.Inventory.Modify cluster</b>	Permite cambiar las propiedades de un clúster.	Clústeres
<b>Host.Inventory.Move cluster or standalone host</b>	Permite mover un clúster o un host independiente entre carpetas. El privilegio debe estar presente tanto en el origen como en el destino.	Clústeres
<b>Host.Inventory.Move host</b>	Permite mover un conjunto de hosts existentes hacia adentro o afuera de un clúster. El privilegio debe estar presente tanto en el origen como en el destino.	Clústeres
<b>Host.Inventory.Remove cluster</b>	Permite eliminar un clúster o un host independiente. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Clústeres, hosts
<b>Host.Inventory.Remove host</b>	Permite quitar un host. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Hosts más objeto primario
<b>Host.Inventory.Rename cluster</b>	Permite cambiar el nombre de un clúster.	Clústeres

## Privilegios de operaciones locales en hosts

Los privilegios de operaciones locales en hosts controlan las acciones que se realizan cuando vSphere Client está conectado directamente a un host.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-16. Privilegios de operaciones locales en hosts

Nombre del privilegio	Descripción	Necesario para
<b>Host.Local operations.Add host to vCenter</b>	Permite instalar y quitar agentes de vCenter, como vpxa y aam, en un host.	Host raíz
<b>Host.Local operations.Create virtual machine</b>	Permite crear una máquina virtual nueva desde cero en un disco sin registrarla en el host.	Host raíz

Tabla 11-16. Privilegios de operaciones locales en hosts (continuación)

Nombre del privilegio	Descripción	Necesario para
Host.Local operations.Delete virtual machine	Permite eliminar una máquina virtual del disco. Esta operación se admite para máquinas virtuales registradas o no registradas.	Host raíz
Host.Local operations.Extract NVRAM content	Permite extraer el contenido de NVRAM de un host.	
Host.Local operations.Manage user groups	Permite administrar cuentas locales en un host.	Host raíz
Host.Local operations.Reconfigure virtual machine	Permite volver a configurar una máquina virtual.	Host raíz
Host.Local operations.Relayout snapshots	Permite cambiar el diseño de las instantáneas de una máquina virtual.	Host raíz

## Privilegios de vSphere Replication de host

Los privilegios de vSphere Replication de host controlan la utilización de la replicación de máquinas virtuales que realiza VMware vCenter Site Recovery Manager™ para un host.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-17. Privilegios de vSphere Replication de host

Nombre del privilegio	Descripción	Necesario para
Host.vSphere Replication.Manage Replication	Permite administrar la replicación de máquinas virtuales en este host.	Hosts

## Privilegios de perfiles de host

Los privilegios de perfiles de host controlan las operaciones relacionadas con la creación y la modificación de perfiles de host.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-18. Privilegios de perfiles de host

Nombre del privilegio	Descripción	Necesario para
<b>Host profile.Clear</b>	Permite borrar información relacionada con el perfil.	vCenter Server raíz
<b>Host profile.Create</b>	Permite crear un perfil de host.	vCenter Server raíz
<b>Host profile.Delete</b>	Permite eliminar un perfil de host.	vCenter Server raíz
<b>Host profile.Edit</b>	Permite editar un perfil de host.	vCenter Server raíz
<b>Host profile.Export</b>	Permite exportar un perfil de host.	vCenter Server raíz
<b>Host profile.View</b>	Permite ver un perfil de host.	vCenter Server raíz

## Privilegios de proveedor de Inventory Service

Los privilegios de proveedor de Inventory Service son únicamente internos. No los utilice.

## Privilegios de etiquetado de Inventory Service

Los privilegios de etiquetado de Inventory Service controlan la capacidad para crear y eliminar etiquetas y categorías de etiquetas, así como asignar y quitar etiquetas en los objetos de inventario de vSphere.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-19. Privilegios de vCenter Inventory Service

Nombre del privilegio	Descripción	Necesario para
<b>Inventory Service.vSphere Tagging.Assign or Unassign vSphere Tag</b>	Permite asignar o anular la asignación de una etiqueta de un objeto en el inventario de vCenter Server.	Cualquier objeto
<b>Inventory Service.vSphere Tagging.Create vSphere Tag</b>	Permite crear una etiqueta.	Cualquier objeto
<b>Inventory Service.vSphere Tagging.Create vSphere Tag Category</b>	Permite crear una categoría de etiqueta.	Cualquier objeto
<b>Inventory Service.vSphere Tagging.Create vSphere Tag Scope</b>	Permite crear un ámbito de etiqueta.	Cualquier objeto
<b>Inventory Service.vSphere Tagging.Delete vSphere Tag</b>	Permite eliminar una etiqueta.	Cualquier objeto
<b>Inventory Service.vSphere Tagging.Delete vSphere Tag Category</b>	Permite eliminar una categoría de etiqueta.	Cualquier objeto

Tabla 11-19. Privilegios de vCenter Inventory Service (continuación)

Nombre del privilegio	Descripción	Necesario para
Inventory Service.vSphere Tagging.Delete vSphere Tag Scope	Permite eliminar un ámbito de etiqueta.	Cualquier objeto
Inventory Service.vSphere Tagging.Edit vSphere Tag	Permite editar una etiqueta.	Cualquier objeto
Inventory Service.vSphere Tagging.Edit vSphere Tag Category	Permite editar una categoría de etiqueta.	Cualquier objeto
Inventory Service.vSphere Tagging.Edit vSphere Tag Scope	Permite editar un ámbito de etiqueta.	Cualquier objeto
Inventory Service.vSphere Tagging.Modify UsedBy Field for Category	Permite cambiar el campo Usado por en una categoría de etiqueta.	Cualquier objeto
Inventory Service.vSphere Tagging.Modify UsedBy Field for Tag	Permite cambiar el campo Usado por de una etiqueta.	Cualquier objeto

## Privilegios de red

Los privilegios de red controlan las tareas relacionadas con la administración de redes.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-20. Privilegios de red

Nombre del privilegio	Descripción	Necesario para
Network.Assign network	Permite asignar una red a una máquina virtual.	Redes, máquinas virtuales
Network.Configure	Permite configurar una red.	Redes, máquinas virtuales
Network.Move network	Permite mover una red entre carpetas. El privilegio debe estar presente tanto en el origen como en el destino.	Redes
Network.Remove	Permite eliminar una red. Este privilegio es obsoleto. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Redes

## Privilegios de rendimiento

Los privilegios de rendimiento controlan la modificación de la configuración de estadísticas de rendimiento.



Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-21. Privilegios de rendimiento**

Nombre del privilegio	Descripción	Necesario para
<b>Performance.Modify intervals</b>	Permite crear, quitar y actualizar intervalos de recopilación de datos de rendimiento.	vCenter Server raíz

## Privilegios de permisos

Los privilegios de permisos controlan la asignación de funciones y permisos.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-22. Privilegios de permisos**

Nombre del privilegio	Descripción	Necesario para
<b>Permissions.Modify permission</b>	Permite definir una o más reglas de permiso en una entidad, o actualizar reglas si estas ya están presentes para un usuario o grupo determinados en la entidad.  Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Cualquier objeto más objeto primario
<b>Permissions.Modify privilege</b>	Permite modificar un grupo o una descripción del privilegio. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	
<b>Permissions.Modify role</b>	Permite actualizar el nombre de una función y los privilegios asociados con esa función.	Cualquier objeto
<b>Permissions.Reassign role permissions</b>	Permite reasignar todos los permisos de una función a otra.	Cualquier objeto

## Privilegios de almacenamiento basado en perfiles

Los privilegios de almacenamiento basado en perfiles controlan las operaciones relacionadas con los perfiles de almacenamiento.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-23. Privilegios de almacenamiento basado en perfiles

Nombre del privilegio	Descripción	Necesario para
<b>Profile-driven storage.Profile-driven storage update</b>	Permite realizar cambios en los perfiles de almacenamiento, por ejemplo, crear y actualizar capacidades de almacenamiento y perfiles de almacenamiento de máquinas virtuales.	vCenter Server raíz
<b>Profile-driven storage.Profile-driven storage view</b>	Permite ver las capacidades de almacenamiento y los perfiles de almacenamiento definidos.	vCenter Server raíz

## Privilegios de recursos

Los privilegios de recursos controlan la creación y la administración de grupos de recursos, como también la migración de máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-24. Privilegios de recursos

Nombre del privilegio	Descripción	Necesario para
<b>Resource.Apply recommendation</b>	Permite aceptar una sugerencia del servidor para realizar una migración con vMotion.	Clústeres
<b>Resource.Assign vApp to resource pool</b>	Permite asignar una vApp a un grupo de recursos.	Grupos de recursos
<b>Resource.Assign virtual machine to resource pool</b>	Permite asignar una máquina virtual a un grupo de recursos.	Grupos de recursos
<b>Resource.Create resource pool</b>	Permite crear grupos de recursos.	Grupos de recursos, clústeres
<b>Resource.Migrate powered off virtual machine</b>	Permite migrar una máquina virtual apagada a un grupo de recursos o host diferentes.	Máquinas virtuales
<b>Resource.Migrate powered on virtual machine</b>	Permite migrar con vMotion una máquina virtual encendida a un grupo de recursos o host diferentes.	
<b>Resource.Modify resource pool</b>	Permite cambiar las asignaciones de un grupo de recursos.	Grupos de recursos
<b>Resource.Move resource pool</b>	Permite mover un grupo de recursos. El privilegio debe estar presente tanto en el origen como en el destino.	Grupos de recursos
<b>Resource.Query vMotion</b>	Permite consultar la compatibilidad general de vMotion de una máquina virtual con un conjunto de hosts.	vCenter Server raíz

Tabla 11-24. Privilegios de recursos (continuación)

Nombre del privilegio	Descripción	Necesario para
<b>Resource.Remove resource pool</b>	Permite eliminar un grupo de recursos. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Grupos de recursos
<b>Resource.Rename resource pool</b>	Permite cambiar el nombre a un grupo de recursos.	Grupos de recursos

## Privilegios para tareas programadas

Estos privilegios controlan la creación, la edición y la eliminación de tareas programadas.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-25. Privilegios para tareas programadas

Nombre del privilegio	Descripción	Necesario para
<b>Scheduled task.Create tasks</b>	Permite programar una tarea. Se lo requiere, junto con los privilegios, para realizar la acción programada en el momento de la programación.	Cualquier objeto
<b>Scheduled task.Modify task</b>	Permite volver a configurar las propiedades de la tarea programada.	Cualquier objeto
<b>Scheduled task.Remove task</b>	Permite quitar una tarea programada de la cola.	Cualquier objeto
<b>Scheduled task.Run task</b>	Permite ejecutar la tarea programada de inmediato. Para crear y ejecutar una tarea programada también se necesitan permisos para la acción asociada.	Cualquier objeto

## Privilegios de sesiones

Los privilegios de sesiones controlan la capacidad de las extensiones para abrir sesiones en el sistema vCenter Server.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-26. Privilegios de sesiones

Nombre del privilegio	Descripción	Necesario para
<b>Sessions.Impersonate user</b>	Permiten suplantar a otro usuario. Esta capacidad se utiliza con las extensiones.	vCenter Server raíz
<b>Sessions.Message</b>	Permiten configurar el registro global en el mensaje.	vCenter Server raíz
<b>Sessions.Validate session</b>	Permiten verificar la validez de la sesión.	vCenter Server raíz
<b>Sessions.View and stop sessions</b>	Permiten visualizar sesiones y forzar el cierre de sesión de uno o más usuarios conectados.	vCenter Server raíz

## Privilegios de vistas de almacenamiento

Los privilegios de vistas de almacenamiento controlan los privilegios de las API de servicio de supervisión de almacenamiento.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-27. Privilegios de vistas de almacenamiento

Nombre del privilegio	Descripción	Necesario para
<b>Storage views.Configure service</b>	Permite a los usuarios con privilegios utilizar todas las API del servicio de supervisión de almacenamiento. Utilice <b>Storage views.View</b> para los privilegios sobre las API de solo lectura del servicio de supervisión de almacenamiento.	vCenter Server raíz
<b>Storage views.View</b>	Permite a los usuarios con privilegios utilizar las API de solo lectura del servicio de supervisión de almacenamiento.	vCenter Server raíz

## Privilegios de tareas

Los privilegios de tareas controlan la capacidad de las extensiones de crear y actualizar tareas en vCenter Server.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-28. Privilegios de tareas

Nombre del privilegio	Descripción	Necesario para
<b>Tasks.Create task</b>	Permite que una extensión cree una tarea definida por el usuario. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	vCenter Server raíz
<b>Tasks.Update task</b>	Permite que una extensión actualice una tarea definida por el usuario. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	vCenter Server raíz

## Privilegios del servicio de transferencia

Los privilegios de servicio de transferencia son internos de VMware. No utilice estos privilegios.

## Privilegios de directivas de VRM

Los privilegios de directivas de VRM son internos de VMware. No utilice estos privilegios.

## Privilegios de configuración de máquinas virtuales

Los privilegios de configuración de máquinas virtuales controlan la capacidad de configurar opciones y dispositivos de máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-29. Privilegios de configuración de máquinas virtuales

Nombre del privilegio	Descripción	Necesario para
<b>Virtual machine.Configuration.Add existing disk</b>	Permite agregar un disco virtual existente a una máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Add new disk</b>	Permite crear un disco virtual nuevo para agregar a una máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Add or remove device</b>	Permite agregar o eliminar cualquier dispositivo que no sea un disco.	Máquinas virtuales
<b>Virtual machine.Configuration.Advanced</b>	Permite agregar o modificar parámetros avanzados en el archivo de configuración de la máquina virtual.	Máquinas virtuales

Tabla 11-29. Privilegios de configuración de máquinas virtuales (continuación)

Nombre del privilegio	Descripción	Necesario para
<b>Virtual machine.Configuration.Change CPU count</b>	Permite cambiar la cantidad de CPU virtuales.	Máquinas virtuales
<b>Virtual machine.Configuration.Change resource</b>	Permite cambiar la configuración de recursos de un conjunto de nodos de máquinas virtuales en un grupo de recursos determinado.	Máquinas virtuales
<b>Virtual machine.Configuration.Configure managedBy</b>	Permite que una extensión o solución marque una máquina virtual como administrada por ella.	Máquinas virtuales
<b>Virtual machine.Configuration.Disk change tracking</b>	Permite habilitar o deshabilitar el seguimiento de cambios para los discos de la máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Disk lease</b>	Permite realizar operaciones de concesión de discos para una máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Display connection settings</b>	Permite configurar opciones de consola remota de máquinas virtuales.	Máquinas virtuales
<b>Virtual machine.Configuration.Extend virtual disk</b>	Permite expandir el tamaño de un disco virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Host USB device</b>	Permite conectar un dispositivo USB basado en host a una máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Memory</b>	Permite cambiar la cantidad de memoria asignada a la máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Modify device settings</b>	Permite cambiar las propiedades de un dispositivo existente.	Máquinas virtuales
<b>Virtual machine.Configuration.Query Fault Tolerance compatibility</b>	Permite comprobar si una máquina virtual es compatible con Fault Tolerance.	Máquinas virtuales
<b>Virtual machine.Configuration.Query unowned files</b>	Permite consultar archivos sin propietario.	Máquinas virtuales
<b>Virtual machine.Configuration.Raw device</b>	Permite agregar y eliminar una asignación de discos sin formato o un dispositivo de acceso directo de SCSI. Al configurar este parámetro, se anula cualquier otro privilegio de modificación de dispositivos sin procesar, incluidos los estados de conexión.	Máquinas virtuales

Tabla 11-29. Privilegios de configuración de máquinas virtuales (continuación)

Nombre del privilegio	Descripción	Necesario para
<b>Virtual machine.Configuration.Reload from path</b>	Permite cambiar la ruta de acceso de configuración de una máquina virtual y, a la vez, preservar la identidad de esta última. Las soluciones como vCenter Site Recovery Manager de VMware usan esta operación para resguardar la identidad de la máquina virtual durante la conmutación por error y la conmutación por recuperación.	Máquinas virtuales
<b>Virtual machine.Configuration.Remove disk</b>	Permite extraer el dispositivo de disco virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Rename</b>	Permite cambiar el nombre de una máquina virtual o modificar las notas asociadas de una máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Reset guest information</b>	Permite editar la información de sistemas operativos invitados de una máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Set annotation</b>	Permite agregar o editar una anotación de máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Settings</b>	Permite cambiar la configuración general de la máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Swapfile placement</b>	Permite cambiar la directiva de selección del archivo de intercambio de una máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Unlock virtual machine</b>	Permite descifrar una máquina virtual.	Máquinas virtuales
<b>Virtual machine.Configuration.Upgrade virtual machine compatibility</b>	Permite actualizar la versión de compatibilidad de la máquina virtual.	Máquinas virtuales

## Privilegios de operaciones de invitado de máquina virtual

Los privilegios de operaciones de invitado de máquina virtual controlan la capacidad de interacción con los archivos y los programas que se encuentran en el sistema operativo invitado de una máquina virtual con la API.

Consulte la documentación sobre la *referencia de VMware vSphere API* para obtener más información sobre dichas operaciones.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-30. Operaciones de invitado de la máquina virtual

Nombre del privilegio	Descripción	Efectivo en el objeto
<b>Virtual machine.Guest Operations.Guest Operation Alias modification</b>	Permite las operaciones de invitado de máquina virtual que implican modificar el alias de la máquina virtual.	Máquinas virtuales
<b>Virtual machine.Guest Operations.Guest Operation Alias query</b>	Permite las operaciones de invitado de máquina virtual que implican consultar el alias de la máquina virtual.	Máquinas virtuales
<b>Virtual machine.Guest Operations.Guest Operation Modifications</b>	Permite las operaciones de invitado de máquina virtual que implican modificaciones en un sistema operativo invitado de una máquina virtual, como la transferencia de un archivo a la máquina virtual.  Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	Máquinas virtuales
<b>Virtual machine.Guest Operations.Guest Operation Program Execution</b>	Permite las operaciones de invitado de máquina virtual que implican ejecutar un programa en la máquina virtual.  Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	Máquinas virtuales
<b>Virtual machine.Guest Operations.Guest Operation Queries</b>	Permite las operaciones de invitado de máquina virtual que implican consultar el sistema operativo invitado, como enumerar archivos en el sistema operativo invitado.  Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	Máquinas virtuales

## Privilegios para la interacción con máquinas virtuales

Estos privilegios controlan la capacidad de interactuar con la consola de una máquina virtual, configurar soportes físicos, realizar operaciones de energía e instalar VMware Tools.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.



Tabla 11-31. Interacción con la máquina virtual

Nombre del privilegio	Descripción	Necesario para
Virtual machine.Interaction.Answer question	Permitir e solucionar problemas con las transiciones de estado de las máquinas virtuales o con errores de ejecución.	Máquinas virtuales
Virtual machine.Interaction.Backup operation on virtual machine	Permitir realizar operaciones de copia de seguridad en las máquinas virtuales.	Máquinas virtuales

Tabla 11-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Virtual machine.Interaction.Configure CD media	Permitir configurar un dispositivo virtual de DVD o CD-ROM.	Máquinas virtuales
Virtual machine.Interaction.Configure floppy media	Permitir configurar un dispositivo virtual de disquete.	Máquinas virtuales
Virtual machine.Interaction.Console interaction	Permitir interactuar con el mouse, el teclado y la pantalla virtual de las máquinas virtuales.	Máquinas virtuales

Tabla 11-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Virtual machine.Interaction.Create screenshot	Permitir crear una captura de pantalla de una máquina virtual.	Máquinas virtuales
Virtual machine.Interaction.Defragment all disks	Permitir realizar operaciones de desfragmentación en todos los discos de la máquina virtual.	Máquinas virtuales
Virtual machine.Interaction.Device connection	Permitir cambiar el estado conectado de los dispositivos virtuales desconnectables de una máquina virtual.	Máquinas virtuales

Tabla 11-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Virtual machine.Interaction.Disable Fault Tolerance	Permitir el deshabilitar la máquina virtual secundaria de una máquina virtual mediante Fault Tolerance.	Máquinas virtuales
Virtual machine.Interaction.Drag and Drop	Permitir arrastrar y soltar archivos entre una máquina virtual y un cliente remoto.	Máquinas virtuales

Tabla 11-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Virtual machine.Interaction.Enable Fault Tolerance	Permitir habilitar la máquina virtual secundaria de una máquina virtual mediante Fault Tolerance.	Máquinas virtuales
Virtual machine.Interaction.Guest operating system management by VIX API	Permitir administrar el sistema operativo de la máquina virtual mediante VIX API.	Máquinas virtuales
Virtual machine.Interaction.Inject USB HID scan codes	Permitir inyectar códigos de análisis de dispositivos USB HID.	Máquinas virtuales

Tabla 11-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Virtual machine.Interaction.Pause/Unpause	Permitir pausar la máquina virtual y anular la pausa.	Máquinas virtuales
Virtual machine.Interaction.Perform wipe or shrink operations	Permitir realizar operaciones de borrado o reducción en la máquina virtual.	Máquinas virtuales

Tabla 11-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Virtual machine.Interaction.Power Off	Permitir apagar una máquina virtual que se encuentra encendida. Esta operación apaga el sistema operativo invitado.	Máquinas virtuales
Virtual machine.Interaction.Power On	Permitir encender una máquina virtual que se encuentra apagada y reanudar una máquina virtual suspendida.	Máquinas virtuales

Tabla 11-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Virtual machine.Interaction.Record session on Virtual Machine	Permitir grabar una sesión en una máquina virtual.	Máquinas virtuales
Virtual machine.Interaction.Replay session on Virtual Machine	Permitir reproducir una sesión grabada en una máquina virtual.	Máquinas virtuales
Virtual machine.Interaction.Reset	Permitir restablecer una máquina virtual y reiniciar el sistema operativo.	Máquinas virtuales



Tabla 11-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Virtual machine.Interaction..Resume Fault Tolerance	Permitir reanudar la tolerancia a errores en una máquina virtual.	Máquinas virtuales
Virtual machine.Interaction.Suspend	Permitir suspender una máquina virtual que se encuentra en estado de espera.	Máquinas virtuales
Virtual machine.Interaction.Suspend Fault Tolerance	Permitir suspender la tolerancia a errores en una máquina virtual.	Máquinas virtuales

Tabla 11-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Virtual machine.Interaction.Test failover	Permitir probar la conmutación por error de Fault Tolerance al convertir la máquina virtual secundaria en la máquina virtual principal.	Máquinas virtuales
Virtual machine.Interaction.Test restart Secondary VM	Permitir finalizar la máquina virtual secundaria de una máquina virtual mediante Fault Tolerance.	Máquinas virtuales

Tabla 11-31. Interacción con la máquina virtual (continuación)

Nombre del privilegio	Descripción	Necesario para
Virtual machine.Interaction.Turn Off Fault Tolerance	Permitir apagar Fault Tolerance en una máquina virtual.	Máquinas virtuales
Virtual machine.Interaction.Turn On Fault Tolerance	Permitir encender Fault Tolerance en una máquina virtual.	Máquinas virtuales
Virtual machine.Interaction.VMware Tools install	Permitir montar y desmontar el CD instalador de VMware Tools como CD-ROM del sistema operativo invitado.	Máquinas virtuales

## Privilegios de inventario de máquinas virtuales

Los privilegios de inventario de máquinas virtuales controlan las operaciones de agregar, mover y eliminar máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-32. Privilegios de inventario de máquinas virtuales**

Nombre del privilegio	Descripción	Necesario para
<b>Virtual machine.Inventory.Create from existing</b>	Permite crear una máquina virtual a partir de una máquina virtual o plantilla existentes, mediante la clonación o la implementación desde una plantilla.	Clústeres, hosts, carpetas de máquina virtual
<b>Virtual machine.Inventory.Create new</b>	Permite crear una máquina virtual y asignar recursos para su ejecución.	Clústeres, hosts, carpetas de máquina virtual
<b>Virtual machine.Inventory.Move</b>	Permite mover de lugar una máquina virtual en la jerarquía. El privilegio debe estar presente tanto en el origen como en el destino.	Máquinas virtuales
<b>Virtual machine.Inventory.Register</b>	Permite agregar una máquina virtual existente a vCenter Server o al inventario de hosts.	Clústeres, hosts, carpetas de máquina virtual
<b>Virtual machine.Inventory.Remove</b>	Permite eliminar una máquina virtual. Esta acción elimina del disco los archivos subyacentes de la máquina virtual. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Máquinas virtuales
<b>Virtual machine.Inventory.Unregister</b>	Permite cancelar el registro de una máquina virtual de una instancia de vCenter Server o un inventario de host. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Máquinas virtuales

## Privilegios de aprovisionamiento de las máquinas virtuales

Los privilegios de aprovisionamiento de las máquinas virtuales controlan las actividades relacionadas con la implementación y la personalización de las máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-33. Privilegios de aprovisionamiento de las máquinas virtuales

Nombre del privilegio	Descripción	Necesario para
<b>Virtual machine.Provisioning.Allow disk access</b>	Permite abrir un disco en una máquina virtual con acceso aleatorio de lectura y escritura. Se utiliza sobre todo para el montaje de discos remotos.	Máquinas virtuales
<b>Virtual machine.Provisioning.Allow read-only disk access</b>	Permite abrir un disco en una máquina virtual con acceso aleatorio de lectura. Se utiliza sobre todo para el montaje de discos remotos.	Máquinas virtuales
<b>Virtual machine.Provisioning.Allow virtual machine download</b>	Permite leer operaciones en archivos asociados con una máquina virtual, incluido vmx, discos, registros y nvram.	Host raíz o vCenter Server
<b>Virtual machine.Provisioning.Allow virtual machine files upload</b>	Permite escribir operaciones en archivos asociados con una máquina virtual, incluido vmx, discos, registros y nvram.	Host raíz o vCenter Server
<b>Virtual machine.Provisioning.Clone template</b>	Permite clonar una plantilla.	Plantillas
<b>Virtual machine.Provisioning.Clone virtual machine</b>	Permite clonar una máquina virtual ya existente y asignar recursos.	Máquinas virtuales
<b>Virtual machine.Provisioning.Create template from virtual machine</b>	Permite crear una plantilla nueva desde una máquina virtual.	Máquinas virtuales
<b>Virtual machine.Provisioning.Customize</b>	Permite personalizar el sistema operativo invitado de una máquina virtual sin moverla.	Máquinas virtuales
<b>Virtual machine.Provisioning.Deploy template</b>	Permite implementar una máquina virtual desde una plantilla.	Plantillas
<b>Virtual machine.Provisioning.Mark as template</b>	Permite marcar como una plantilla a una máquina virtual ya existente que está apagada.	Máquinas virtuales
<b>Virtual machine.Provisioning.Mark as virtual machine</b>	Permite marcar una plantilla existente como una máquina virtual.	Plantillas
<b>Virtual machine.Provisioning.Modify customization specification</b>	Permite crear, modificar o eliminar especificaciones de personalización.	vCenter Server raíz
<b>Virtual machine.Provisioning.Promote disks</b>	Permite promover operaciones en los discos de una máquina virtual.	Máquinas virtuales
<b>Virtual machine.Provisioning.Read customization specifications</b>	Permite leer una especificación de personalización.	Máquinas virtuales

## Privilegios de configuración de servicios de la máquina virtual

Los privilegios de configuración de servicios de la máquina virtual controlan quién puede realizar tareas de supervisión y administración en la configuración de servicios.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Nota** En vSphere 6.0, no asigne ni quite este privilegio mediante vSphere Web Client.

**Tabla 11-34. Privilegios de configuración de servicios de la máquina virtual**

Nombre del privilegio	Descripción
Máquina virtual. Configuración de servicios. Permitir notificaciones	Permite generar y recibir notificaciones sobre el estado del servicio.
Máquina virtual. Configuración de servicios. Permitir medición de notificaciones de eventos globales	Permite consultar si hay notificaciones presentes.
Máquina virtual. Configuración de servicios. Administrar configuración de servicios	Permite crear, modificar y eliminar servicios de la máquina virtual.
Máquina virtual. Configuración de servicios. Modificar configuración de servicios	Permite modificar la configuración actual del servicio de la máquina virtual.
Máquina virtual. Configuración de servicios. Consultar configuración de servicios	Permite recuperar la lista de servicios de la máquina virtual.
Máquina virtual. Configuración de servicios. Leer configuración de servicios	Permite recuperar la configuración actual del servicio de la máquina virtual.

## Privilegios de administración de snapshots de las máquinas virtuales

Los privilegios de administración de snapshots de las máquinas virtuales controlan la capacidad para crear, eliminar, cambiar el nombre y restaurar snapshots.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-35. Privilegios del estado de las máquinas virtuales

Nombre del privilegio	Descripción	Necesario para
<b>Virtual machine.Snapshot management. Create snapshot</b>	Permite crear una snapshot a partir del estado actual de la máquina virtual.	Máquinas virtuales
<b>Virtual machine.Snapshot management.Remove Snapshot</b>	Permite quitar una snapshot del historial de snapshots.	Máquinas virtuales
<b>Virtual machine.Snapshot management.Rename Snapshot</b>	Permite cambiar el nombre de una snapshot con un nuevo nombre, una nueva descripción o ambos.	Máquinas virtuales
<b>Virtual machine.Snapshot management.Revert to snapshot</b>	Permite configurar la máquina virtual con el estado que tenía en una snapshot determinada.	Máquinas virtuales

## Privilegios de vSphere Replication de máquinas virtuales

Los privilegios de vSphere Replication de máquinas virtuales controlan la utilización de la replicación que hace VMware vCenter Site Recovery Manager™ en máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-36. vSphere Replication de máquinas virtuales

Nombre del privilegio	Descripción	Necesario para
<b>Virtual machine.vSphere Replication.Configure Replication</b>	Permite configurar la replicación de la máquina virtual.	Máquinas virtuales
<b>Virtual machine.vSphere Replication.Manage Replication</b>	Permite activar la sincronización completa, en línea o sin conexión de una replicación.	Máquinas virtuales
<b>Virtual machine.vSphere Replication.Monitor Replication</b>	Permite supervisar la replicación.	Máquinas virtuales

## Privilegios de grupo dvPort

Los privilegios de grupo de puertos virtuales distribuidos controlan la capacidad para crear, eliminar y modificar grupos de puertos virtuales distribuidos.

En la tabla se describen los privilegios necesarios para crear y configurar grupos de puertos virtuales distribuidos.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-37. Privilegios del grupo de puertos virtuales distribuidos**

Nombre del privilegio	Descripción	Necesario para
<b>dvPort group.Create</b>	Permite crear un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales
<b>dvPort group.Delete</b>	Permite eliminar un grupo de puertos virtuales distribuidos. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Grupos de puertos virtuales
<b>dvPort group.Modify</b>	Permite modificar la configuración de un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales
<b>dvPort group.Policy operation</b>	Permite configurar la directiva de un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales
<b>dvPort group.Scope operation</b>	Permite configurar el ámbito de un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales

## Privilegios de vApp

Los privilegios de vApp controlan las operaciones relacionadas con la implementación y la configuración de una vApp.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

**Tabla 11-38. Privilegios de vApp**

Nombre del privilegio	Descripción	Necesario para
<b>vApp.Add virtual machine</b>	Permite agregar una máquina virtual a una vApp.	vApps
<b>vApp.Assign resource pool</b>	Permite asignar un grupo de recursos a una vApp.	vApps
<b>vApp.Assign vApp</b>	Permite asignar una vApp a otra vApp.	vApps
<b>vApp.Clone</b>	Permite clonar una vApp.	vApps
<b>vApp.Crear</b>	Permite crear una vApp.	vApps



Tabla 11-38. Privilegios de vApp (continuación)

Nombre del privilegio	Descripción	Necesario para
<b>vApp.Delete</b>	Permite eliminar una vApp. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	vApps
<b>vApp.Export</b>	Permite exportar una vApp desde vSphere.	vApps
<b>vApp.Import</b>	Permite importar una vApp a vSphere.	vApps
<b>vApp.Move</b>	Permite mover una vApp a una nueva ubicación de inventario.	vApps
<b>vApp.Power Off</b>	Permite apagar las operaciones en una vApp.	vApps
<b>vApp.Power On</b>	Permite encender las operaciones en una vApp.	vApps
<b>vApp.Rename</b>	Permite cambiarle el nombre a una vApp.	vApps
<b>vApp.Suspend</b>	Permite suspender una vApp.	vApps
<b>vApp.Unregister</b>	Permite anular el registro de una vApp. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	vApps
<b>vApp.View OVF Environment</b>	Permite visualizar el entorno de OVF de una máquina virtual encendida dentro de una vApp.	vApps
<b>vApp.vApp application configuration</b>	Permite modificar la estructura interna de una vApp, como la información y las propiedades de un producto.	vApps
<b>vApp.vApp instance configuration</b>	Permite modificar la configuración de las instancias de una vApp, como sus directivas.	vApps
<b>vApp.vApp managedBy configuration</b>	Permite que una extensión o una solución marque una vApp como administrada por ella. Ninguno de los elementos de la interfaz de usuario de vSphere Web Client se asocia con este privilegio.	vApps
<b>vApp.vApp resource configuration</b>	Permite modificar la configuración de recursos de una vApp. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	vApps

## Privilegios de vServices

Los privilegios de vServices controlan la capacidad para crear, configurar y actualizar dependencias de vService para máquinas virtuales y vApps.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 11-39. vServices

Nombre del privilegio	Descripción	Necesario para
<b>vService.Create dependency</b>	Permite crear una dependencia de vService para una máquina virtual o vApp.	vApps y máquinas virtuales
<b>vService.Destroy dependency</b>	Permite quitar una dependencia de vService para una máquina virtual o vApp.	vApps y máquinas virtuales
<b>vService.Reconfigure dependency configuration</b>	Permite volver a configurar una dependencia para actualizar el proveedor o la unión.	vApps y máquinas virtuales
<b>vService.Update dependency</b>	Permite actualizar una dependencia para configurar el nombre o la descripción.	vApps y máquinas virtuales