

Instalar y configurar vSphere

Actualización 2

Modificado el 11 de agosto de 2020

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

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

Copyright © 2009-2020 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Acerca de la instalación y configuración de vSphere 9

Información actualizada 10

1 Introducción a la instalación y configuración de vSphere 12

Componentes y servicios de vCenter Server 12

Modelos de implementación de vCenter Server 15

Información general del proceso de instalación y configuración de vSphere 18

Descripción general de los certificados de seguridad de vSphere 21

Descripción general del reemplazo de certificados 21

Descripción general del modo vinculado mejorado 24

2 Requisitos del sistema 26

Requisitos de ESXi 26

Requisitos de hardware de ESXi 26

Modelos de servidores de administración remota compatibles y versiones de firmware 29

Recomendaciones para un rendimiento mejorado de ESXi 29

Puertos de firewall entrantes y salientes para hosts de ESXi 31

Requisitos de vCenter Server para Windows 34

Comprobaciones previas a la instalación de vCenter Server para Windows 35

Requisitos de hardware de vCenter Server para Windows 36

Requisitos de almacenamiento de vCenter Server para Windows 36

Requisitos de software de vCenter Server para Windows 37

Requisitos de base de datos de vCenter Server para Windows 37

Requisitos de vCenter Server Appliance 38

Requisitos de hardware de vCenter Server Appliance 38

Requisitos de almacenamiento de vCenter Server Appliance 38

Software incluido en vCenter Server Appliance 39

Requisitos de software de vCenter Server Appliance 39

Requisitos de base de datos de vCenter Server Appliance 40

Puertos necesarios para vCenter Server y Platform Services Controller 40

Requisitos de DNS de vSphere 46

Comprobar que el FQDN se puede resolver 47

Requisitos de software de vSphere Web Client 47

Requisitos de software del complemento de integración de clientes 48

Requisitos de vSphere Client 48

Requisitos de hardware de vSphere Client 48

Requisitos de software de vSphere Client 49

Puertos TCP y UDP para vSphere Client	49
Espacio libre necesario para registro del sistema	50

3 Antes de instalar ESXi 52

Opciones para instalar ESXi	52
Instalar ESXi de manera interactiva	52
Instalación de ESXi generada por script	52
Instalar Auto Deploy ESXi	53
Personalizar instalaciones con ESXi Image Builder CLI	54
Acerca de los modos de evaluación y con licencia de ESXi	55
Opciones de medios para arrancar el instalador de ESXi	55
Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi	56
Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi	56
Crear una unidad flash USB para almacenar el script de instalación o actualización de ESXi	58
Crear una imagen ISO de instalador con un script de instalación o actualización personalizado	60
Arranque PXE del instalador de ESXi	61
Instalar y arrancar ESXi con FCoE de software	70
Usar aplicaciones de administración remota	71
Información obligatoria para instalar ESXi	71
Descarga del instalador de ESXi	72

4 Instalación de ESXi 73

Instalar ESXi de forma interactiva	73
Instalar ESXi de forma interactiva	73
Instalar ESXi en un disco iSCSI de software	76
Instalar o actualizar hosts mediante un script	77
Enfoques para la instalación por script	78
Introducir las opciones de arranque para iniciar un script de instalación o actualización	78
Acerca de los scripts de instalación y actualización	81
Instalar o actualizar ESXi desde un CD o DVD con un script	93
Instalar o actualizar ESXi desde una unidad flash USB mediante un script	94
Realizar una instalación o actualización generada por script de ESXi a través de PXE para arrancar el instalador	95
Instalar ESXi con vSphere Auto Deploy	96
Información sobre vSphere Auto Deploy	96
Información general del cmdlet y el inicio rápido de Auto Deploy	105
Prepararse para vSphere Auto Deploy	109
Administrar Auto Deploy con los cmdlets de PowerCLI	117
Aprovisionar sistemas ESXi con vSphere Auto Deploy	122
Usar Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado	127

Configurar un host de referencia de Auto Deploy	137
Tareas de administración avanzadas	146
Prácticas recomendadas y consideración de seguridad de Auto Deploy	151
Solucionar problemas de Auto Deploy	160
Configurar prueba de concepto de Auto Deploy	167
Usar vSphere ESXi Image Builder	184
Información sobre vSphere ESXi Image Builder	185
Instalar y usar vSphere ESXi Image Builder	195
Tareas comunes de vSphere ESXi Image Builder	197
Flujos de trabajo de vSphere ESXi Image Builder	208

5 Configurar ESXi 216

Configurar ESXi automáticamente	217
Acerca de la interfaz de ESXi de la consola directa	217
Configuración de la distribución del teclado para la consola directa	218
Crear un mensaje emergente de seguridad para la consola directa	218
Redirigir la consola directa a un puerto serie	219
Configurar la contraseña de la cuenta de administrador	221
Configuración de arranque del BIOS	221
Cómo cambiar la configuración de arranque del BIOS para ESXi	222
Configuración de la opción de arranque para medios virtuales	222
El host no arranca después de instalar ESXi en modo UEFI	223
Acceso de red a un host ESXi	224
Configurar la red en un host que no se haya adjuntado a la red	224
Administrar ESXi de forma remota	225
Configuración de las opciones de red	225
Recomendaciones de seguridad para redes de ESXi	225
Selección de los adaptadores de red para la red de administración	226
Configurar el id. de VLAN	227
Configurar IP para ESXi	227
Configurar DNS para ESXi	228
Probar la red de administración	229
Reiniciar los agentes de administración	229
Reiniciar la red de administración	230
Restauración del conmutador estándar	230
Prueba de la conectividad con los dispositivos y las redes	231
Comportamiento de almacenamiento	231
Acerca de la partición desde cero	233
Habilitar el acceso a ESXi Shell y SSH con la interfaz de usuario de la consola directa	235
Ver registros del sistema	236
Configurar Syslog en hosts ESXi	236

- Configurar el filtrado de registros en hosts ESXi 237
- Configurar el nivel de aceptación del perfil de imagen de host 239
- Restablecer la configuración del sistema 240
- Quitar todos los paquetes personalizados en ESXi 241
- Deshabilitación de la compatibilidad con caracteres no ASCII en los nombres de directorios y archivos de máquinas virtuales 241
- Desinstalar un host ESXi 242

6 Después de instalar y configurar ESXi 243

- Administrar el host ESXi 243
- Licencias de hosts ESXi 243
 - Acerca de los modos de evaluación y con licencia de ESXi 244
 - Registro de la clave de licencia de un host ESXi 244
- Instalar vSphere Client 245

7 Antes de instalar vCenter Server o implementar vCenter Server Appliance 247

- Preparar las bases de datos de vCenter Server para la instalación 247
 - Notas sobre la configuración de la base de datos de vCenter Server 248
 - Configurar bases de datos de Microsoft SQL Server 249
 - Configurar bases de datos de Oracle 260
 - Requisitos de permisos de base de datos para vCenter Server 265
 - Comprobar que vCenter Server puede comunicarse con la base de datos local 268
 - Mantener una base de datos de vCenter Server 269
- Cómo influye vCenter Single Sign-On en la instalación 269
 - Componentes de vCenter Single Sign-On 270
 - Configurar el usuario administrador de vCenter Server 271
 - Autenticar con el entorno de vCenter Server 271
 - Cómo vCenter Single Sign-On afecta el comportamiento de inicio de sesión 272
 - Orígenes de identidad para vCenter Server con vCenter Single Sign-On 273
- Sincronizar los relojes en la red de vSphere 274
 - Sincronización de los relojes de ESXi con un servidor horario de red 274
- Usar una cuenta de usuario para ejecutar vCenter Server 275
- Instalar vCenter Server en máquinas IPv6 276
- Ejecutar el instalador de vCenter Server desde una unidad de red 276
- Información obligatoria para instalar vCenter Server 276
 - Información requerida para la instalación de vCenter Server con una instancia de Platform Services Controller integrada 276
 - Información obligatoria para instalar Platform Services Controller 278
 - Información obligatoria para instalar vCenter Server 280
- Información necesaria para la implementación de vCenter Server Appliance 282
 - Información necesaria para la implementación de vCenter Server Appliance con una instancia de Platform Services Controller integrada 282

	Información necesaria para la implementación de Platform Services Controller Appliance	287
	Información necesaria para la implementación de vCenter Server Appliance	290
8	Instalar vCenter Server en un servidor físico o una máquina virtual de Windows	294
	Descargar vCenter Server para Windows Installer	294
	Instalación de vCenter Server con una instancia de Platform Services Controller integrada	295
	Instalación de vCenter Server con un Platform Services Controller externo	299
	Instalar Platform Services Controller en una máquina con Windows	300
	Instalar vCenter Server y los componentes de vCenter Server	302
	Instalar vCenter Server en un entorno con varias NIC	305
9	Implementar vCenter Server Appliance	306
	Descargar el instalador de vCenter Server Appliance	307
	Instalar el complemento de integración de clientes	308
	Implementación de vCenter Server Appliance con una instancia de Platform Services Controller integrada	309
	Implementar vCenter Server Appliance con una instancia de Platform Services Controller externa	314
	Implementación de Platform Services Controller Appliance	315
	Implementación de vCenter Server Appliance	319
10	Solucionar problemas de instalación o implementación de vCenter Server	324
	Recopilar registros para solucionar problemas de una instalación o actualización de vCenter Server	324
	Recopilar registros de instalación mediante el asistente de instalación	325
	Recuperar registros de instalación de forma manual	325
	Recopilar archivos de registro de implementación para vCenter Server Appliance	325
	Exportar un paquete de soporte de vCenter Server para solución de problemas	326
	Instalar Platform Services Controller después de un error de instalación anterior	327
	Microsoft SQL Database configurado en modo de compatibilidad no admitido provoca errores en la instalación o actualización de vCenter Server	327
11	Después de instalar vCenter Server o implementar vCenter Server Appliance	329
	Iniciar sesión en vCenter Server con vSphere Web Client	329
	Recopilar archivos de registro de vCenter Server	330
	Instalar o actualizar vSphere Authentication Proxy	331
	Desinstalar vCenter Server	332
	Redirigir vCenter Server a otra instancia de Platform Services Controller externa	333
	Reconfigurar una instancia de vCenter Server independiente con una instancia de Platform Services Controller integrada en un vCenter Server con una instancia de Platform Services Controller externa	334

Reconfigurar varias instancias combinadas de vCenter Server con una instancia de Platform Services Controller integrada en vCenter Server con una instancia de Platform Services Controller externa 338

Comprobar que los servicios de las instancias de Platform Services Controller integradas estén en ejecución 341

Configurar el acuerdo de replicación entre todas las instancias de Platform Services Controller externas 342

Reconfigurar cada instancia de vCenter Server y redireccionarla de una instancia integrada de Platform Services Controller a una externa 344

12 Hacer copias de seguridad del entorno de vCenter Server y restaurar 348

Flujo de trabajo general de vSphere Data Protection 349

Implementación de la plantilla de OVF de vSphere Data Protection 350

Configuración de vSphere Data Protection 351

Crear un trabajo de copia de seguridad en vSphere Data Protection 353

Iniciar un trabajo de copia de seguridad de forma manual 354

Restaurar el entorno de vCenter Server 355

Hacer copias de seguridad de vCenter Server con una instancia de Platform Services Controller integrada y restaurar 360

Hacer copias de seguridad del entorno de vCenter Server con una instancia externa única de Platform Services Controller y restaurarlas 361

Hacer copias de seguridad de Platform Services Controller y restaurarlo 361

Copia de seguridad y restauración de vCenter Server 363

Hacer copias de seguridad del entorno de vCenter Server con varias instancias de Platform Services Controller y restaurarlo 364

Hacer copias de seguridad de una instancia única de Platform Services Controller y restaurar 365

Hacer copias de seguridad de varias instancias de Platform Services Controller y restaurar 368

Hacer copias de seguridad de todas las instancias de Platform Services Controller y restaurarlas 371

Copia de seguridad y restauración de vCenter Server 376

Acerca de la instalación y configuración de vSphere

En el tema sobre *instalación y configuración de vSphere* se describe cómo instalar y configurar VMware® vCenter Server y cómo implementar vCenter Server Appliance y ESXi.

Audiencia prevista

El tema sobre *instalación y configuración de vSphere* está pensado para administradores experimentados que desean instalar y configurar vCenter Server, implementar y configurar vCenter Server Appliance, e instalar y configurar ESXi.

Esta información está escrita para administradores del sistema de Windows y Linux expertos que están familiarizados con la tecnología de máquina virtual y las operaciones de centro de datos. La información sobre el uso de Image Builder y Auto Deploy está escrita para administradores que tienen experiencia con Microsoft PowerShell y PowerCLI.

Información actualizada

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

En esta tabla se muestra el historial de actualizaciones de *Instalación y configuración de vSphere*.

Revisión	Descripción
02 de abril de 2021	VMware ha cambiado el nombre del portal My VMware por VMware Customer Connect. Hemos actualizado la documentación <i>Instalación y configuración de vSphere</i> para reflejar este cambio de nombre.
11 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.
29 de octubre de 2019	Se actualizó Instalar el complemento de integración de clientes con las instrucciones corregidas para instalar el complemento de integración de clientes.
01 de diciembre de 2017	Se actualizó Descargar el instalador de vCenter Server Appliance para especificar que la imagen ISO de vCenter Server Appliance se debe descargar del sitio web de VMware.
ES-001986-05	<ul style="list-style-type: none">■ Se actualizó el tema Acerca del archivo boot.cfg para agregar una referencia a un ejemplo.■ Se revisaron los pasos de Descargar registros de Auto Deploy para descargar los archivos de registro mediante el botón Exportar paquete de soporte.■ Se actualizó el tema Puertos TCP y UDP para vSphere Client para quitar el puerto 903.■ Se ha actualizado el capítulo Preparar las bases de datos de vCenter Server para la instalación para mejorar la información sobre la configuración de las bases de datos externas.■ Se actualizó el tema Iniciar sesión en vCenter Server con vSphere Web Client para agregar la dirección URL de vSphere Web Client con el puerto HTTPS.■ Se ha actualizado el tema Redirigir vCenter Server a otra instancia de Platform Services Controller externa para mejorar el contexto y los requisitos previos de la tarea.
ES-001986-04	<ul style="list-style-type: none">■ Se actualizó Requisitos de hardware de vCenter Server para Windows y Requisitos de hardware de vCenter Server Appliance para indicar que los requisitos de hardware para vCenter Server con una instancia integrada de Platform Services Controller y vCenter Server con una instancia externa de Platform Services Controller son los mismos.■ Se actualizó Reconfigurar cada instancia de vCenter Server y redireccionarla de una instancia integrada de Platform Services Controller a una externa para agregar un paso en la creación de un acuerdo de replicación directo entre las instancias integrada y externa de Platform Services Controller si no existe uno.
ES-001986-03	<ul style="list-style-type: none">■ Se revisaron los requisitos previos y los pasos en Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.■ Se actualizó Instalar el complemento de integración de clientes para mejorar la información sobre la ubicación del archivo ejecutable.

Revisión	Descripción
ES-001986-02	<ul style="list-style-type: none"> ■ Se actualizó la información sobre los puertos 389, 636, 11711 y 11712 en Puertos necesarios para vCenter Server y Platform Services Controller. ■ Se realizaron revisiones menores en los ejemplos de Crear una imagen ISO de instalador con un script de instalación o actualización personalizado y Opciones de arranque. ■ Se actualizaron los temas Establecer la partición desde cero de vSphere Web Client y El host se detiene inesperadamente durante el arranque cuando comparte un disco de arranque con otro host para agregar un ejemplo de configuración de una ruta de acceso de directorio para la partición temporal. ■ Se actualizó el nombre del script <code>pvc_restore</code> en la sección Capítulo 12 Hacer copias de seguridad del entorno de vCenter Server y restaurar. ■ Se actualizó el tema Prácticas recomendadas de vSphere Auto Deploy para indicar que Auto Deploy se implementa junto con el sistema vCenter Server. ■ Se corrigió la URL en el tema Crear un trabajo de copia de seguridad en vSphere Data Protection.
ES-001986-01	<ul style="list-style-type: none"> ■ Se actualizó la información sobre la cantidad de instancias de vCenter Server en Cómo influye vCenter Single Sign-On en la instalación. ■ Se actualizó el tema Reconfigurar una instancia de vCenter Server independiente con una instancia de Platform Services Controller integrada en un vCenter Server con una instancia de Platform Services Controller externa y se añadió Reconfigurar varias instancias combinadas de vCenter Server con una instancia de Platform Services Controller integrada en vCenter Server con una instancia de Platform Services Controller externa para mejorar la información acerca de la reconfiguración de una instancia independiente o de varias instancias de vCenter Server con una instancia de Platform Services Controller integrada.
ES-001986-00	Versión inicial.

Introducción a la instalación y configuración de vSphere

1

vSphere 6.0 proporciona diferentes opciones para la instalación y configuración. Para garantizar una implementación correcta de vSphere, comprenda las opciones de instalación y configuración, y la secuencia de tareas.

Los dos componentes principales de vSphere son VMware ESXi[®] y VMware vCenter Server[®]. ESXi es la plataforma de virtualización en la que puede crear y ejecutar máquinas virtuales y aplicaciones virtuales. vCenter Server es un servicio que funciona como un administrador central para los hosts de ESXi conectados en una red. vCenter Server permite agrupar y administrar los recursos de varios hosts.

Puede instalar vCenter Server en una máquina virtual o servidor físico con Windows, o implementar vCenter Server Appliance. vCenter Server Appliance es una máquina virtual preconfigurada y basada en Linux optimizada para la ejecución de vCenter Server y los componentes de vCenter Server. Es posible implementar vCenter Server Appliance en hosts ESXi 5.0 o posteriores, o bien en instancias de vCenter Server 5.0 o posteriores.

A partir de vSphere 6.0, todos los servicios de requisito previo para la ejecución de vCenter Server y los componentes de vCenter Server están integrados en VMware Platform Services Controller. Puede implementar vCenter Server con un Platform Services Controller externo o integrado, pero deberá siempre instalar o implementar el Platform Services Controller antes de instalar o implementar vCenter Server.

Este capítulo incluye los siguientes temas:

- [Componentes y servicios de vCenter Server](#)
- [Modelos de implementación de vCenter Server](#)
- [Información general del proceso de instalación y configuración de vSphere](#)
- [Descripción general de los certificados de seguridad de vSphere](#)
- [Descripción general del modo vinculado mejorado](#)

Componentes y servicios de vCenter Server

vCenter Server proporciona una plataforma centralizada para la administración, el funcionamiento, el aprovisionamiento de recursos y la evaluación del rendimiento de las máquinas virtuales y los hosts.

Cuando instale vCenter Server con una instancia de Platform Services Controller integrada o implemente vCenter Server Appliance con una instancia de Platform Services Controller integrada, vCenter Server, los componentes de vCenter Server y los servicios incluidos en Platform Services Controller se implementan en el mismo sistema.

Cuando instale vCenter Server con una instancia de Platform Services Controller externa o implemente vCenter Server Appliance con una instancia de Platform Services Controller externa, vCenter Server y los componentes de vCenter Server se implementan en un sistema y los servicios incluidos en Platform Services Controller se implementan en otro sistema.

Los siguientes componentes se incluyen en las instalaciones de vCenter Server y vCenter Server Appliance:

- El grupo de servicios de infraestructura de VMware Platform Services Controller contiene vCenter Single Sign-On, el servicio de licencias, Lookup Service y VMware Certificate Authority.
- El grupo de servicios de vCenter Server contiene vCenter Server, vSphere Web Client, Inventory Service, vSphere Auto Deploy, vSphere ESXi Dump Collector, VMware vSphere Syslog Collector en Windows y VMware Sphere Syslog Service para vCenter Server Appliance.

Servicios instalados con VMware Platform Services Controller

vCenter Single Sign-On

El servicio de autenticación de vCenter Single Sign-On proporciona servicios de autenticación segura a los componentes de software de vSphere. Al utilizar vCenter Single Sign-On, los componentes de vSphere se comunican entre sí a través de un mecanismo de intercambio seguro de tokens, en lugar de requerir que cada componente autentique a un usuario por separado con un servicio de directorio como Active Directory. vCenter Single Sign-On implementa un dominio de seguridad interno (por ejemplo, vsphere.local), donde las soluciones y los componentes de vSphere se registran durante el proceso de instalación o actualización, lo que proporciona un recurso de infraestructura. vCenter Single Sign-On puede realizar la autenticación de los usuarios desde sus propios usuarios y grupos internos o puede conectarse a servicios de directorio externos de confianza, como Microsoft Active Directory. A continuación, los usuarios autenticados pueden recibir asignaciones de permisos o roles registrados y basados en soluciones dentro de un entorno de vSphere.

vCenter Single Sign-On está disponible y es un requisito con vCenter Server 5.1.x y versiones posteriores.

Servicio de licencias de vSphere

El servicio de licencias de vSphere proporciona funcionalidades comunes de administración e inventario de licencias a todos sistemas vCenter Server que estén conectados a Platform Services Controller o varias instancias de Platform Services Controller asociadas.

VMware Certificate Authority

VMware Certificate Authority (VMCA) aprovisiona cada host ESXi con un certificado firmado que tiene VMCA como la entidad de certificación raíz de forma predeterminada. El aprovisionamiento ocurre cuando el host ESXi se agrega a vCenter Server de forma explícita o como parte del proceso de instalación del host ESXi. Todos los certificados de ESXi se almacenan localmente en el host.

Servicios instalados con vCenter Server

Estos componentes adicionales se instalan de forma silenciosa cuando se instala vCenter Server. Los componentes no pueden instalarse por separado, puesto que no poseen sus propios instaladores.

vCenter Inventory Service

Inventory Service almacena los datos de configuración e inventario de vCenter Server, lo que permite buscar y acceder a objetos del inventario en instancias de vCenter Server.

PostgreSQL

Una versión integrada de la distribución de VMware de la base de datos de PostgreSQL para vSphere y vCloud Hybrid Services.

vSphere Web Client

vSphere Web Client permite conectarse a instancias de vCenter Server mediante un explorador web y, de esta forma, podrá administrar su infraestructura vSphere.

vSphere ESXi Dump Collector

Herramienta de soporte de vCenter Server. Puede configurar ESXi para guardar la memoria VMkernel en un servidor de red, en lugar de un disco, cuando el sistema detecta un error crítico. vSphere ESXi Dump Collector recopila los volcados de memoria en la red.

VMware vSphere Syslog Collector

La herramienta de soporte de vCenter Server en Windows que permite la generación de registros de la red y la combinación de registros de varios hosts. Puede utilizar vSphere Syslog Collector para dirigir los registros del sistema ESXi a un servidor de la red, en lugar de a un disco local. La cantidad máxima recomendada de hosts admitidos para la recopilación de registros es 30. Para obtener información sobre la configuración de vSphere Syslog Collector, consulte <http://kb.vmware.com/kb/2021652>.

Servicio de Syslog de VMware

La herramienta de soporte de vCenter Server Appliance que proporciona una arquitectura unificada para la generación de registros del sistema, la generación de registros de red y la recopilación de registros de los hosts. Puede utilizar el servicio de Syslog de VMware para dirigir los registros del sistema de ESXi a un servidor de la red, en lugar de a un disco local. La cantidad máxima recomendada de hosts admitidos para la recopilación de registros es 30.

Para obtener información sobre la configuración de servicio de Syslog de VMware, consulte *Configuración de vCenter Server Appliance*.

vSphere Auto Deploy

La herramienta de soporte de vCenter Server que puede aprovisionar cientos de hosts físicos con software ESXi. Se puede especificar la imagen que se implementará y los hosts que se aprovisionarán con esa imagen. O bien, puede especificar perfiles de host para aplicar a los hosts y una ubicación de vCenter Server (carpeta o clúster) para cada host.

Modelos de implementación de vCenter Server

Puede instalar vCenter Server en una máquina virtual o en un servidor físico con Microsoft Windows Server 2008 SP2 o versiones posteriores, o puede implementar el vCenter Server Appliance. vCenter Server Appliance es una máquina virtual basada en Linux preconfigurada y optimizada para ejecutar vCenter Server.

vSphere 6.0 incluye vCenter Server con un Platform Services Controller integrado vCenter Server con un Platform Services Controller externo.

Importante En esta documentación se proporciona información sobre los modelos de implementación básicos. Para obtener información sobre las topologías recomendadas, consulte la [lista de topologías recomendadas para vSphere 6.0.x](#).

vCenter Server con una instancia de Platform Services Controller integrada

Todos los servicios integrados con el Platform Services Controller se implementan en la misma máquina virtual o servidor físico que vCenter Server.

vCenter Server con una instancia de Platform Services Controller externa

Los servicios integrados con el Platform Services Controller y vCenter Server se implementan en máquinas virtuales o servidores físicos diferentes.

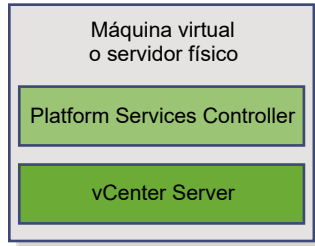
En primer lugar, deberá implementar el Platform Services Controller en una máquina virtual o servidor físico y, a continuación, implementar vCenter Server en otra máquina virtual o servidor físico.

Nota Después de implementar vCenter Server con una instancia de Platform Services Controller integrada, puede volver a configurar la topología y cambiar a vCenter Server con una instancia de Platform Services Controller externa. Este es un proceso unidireccional. Una vez realizado, no se puede volver a vCenter Server con una instancia de Platform Services Controller integrada. Puede redireccionar la instancia de vCenter Server solo a una instancia de Platform Services Controller externa configurada para replicar los datos de infraestructura dentro del mismo dominio.

vCenter Server con una instancia de Platform Services Controller integrada

vCenter Server y Platform Services Controller se implementan en una única máquina virtual o un único servidor físico.

Figura 1-1. vCenter Server con un Platform Services Controller integrado



La instalación de vCenter Server con un Platform Services Controller integrado posee las siguientes ventajas:

- La conexión entre vCenter Server y el Platform Services Controller no se realiza a través de la red, y vCenter Server no está propenso a interrupciones debido a problemas de conectividad y resolución de nombres entre vCenter Server y el Platform Services Controller.
- Si instala vCenter Server en máquinas virtuales o servidores físicos con Windows, necesitará menos licencias de Windows.
- Deberá administrar menos máquinas virtuales o servidores físicos.
- No necesitará un equilibrador de carga para distribuir la carga a través del Platform Services Controller.

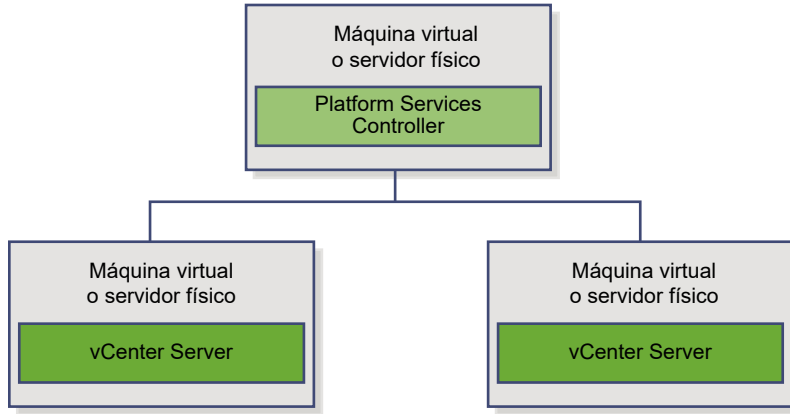
La instalación con un Platform Services Controller integrado posee las siguientes desventajas:

- Existe un Platform Services Controller para cada producto, lo que podría ser más que lo requerido. Esto consume más recursos.
- Este modelo es adecuado para entornos de pequeña escala.

vCenter Server con una instancia de Platform Services Controller externa

vCenter Server y el Platform Services Controller se implementan en una máquina virtual o servidor físico por separado. El Platform Services Controller puede compartirse en varias instancias de vCenter Server. Puede instalar un Platform Services Controller y, a continuación, instalar varias instancias de vCenter Server y registrarlas con el Platform Services Controller. A continuación, puede instalar otro Platform Services Controller, configurarlo para replicar los datos con el primer Platform Services Controller y, a continuación, instalar instancias de vCenter Server y registrarlas con el segundo Platform Services Controller.

Figura 1-2. vCenter Server con un Platform Services Controller externo



La instalación de vCenter Server con un Platform Services Controller externo posee las siguientes ventajas:

- La cantidad menor de recursos consumidos por los servicios combinados en las instancias de Platform Services Controller permite reducir el espacio y el mantenimiento requeridos.
- El entorno puede estar compuesto por más instancias de vCenter Server.

La instalación de vCenter Server con un Platform Services Controller externo posee las siguientes desventajas:

- La conexión entre vCenter Server y el Platform Services Controller se realiza a través de la red y está propensa a problemas de conectividad y resolución de nombres.
- Si instala vCenter Server en máquinas virtuales o servidores físicos con Windows, necesitará más licencias de Microsoft Windows.
- Deberá administrar más máquinas virtuales o servidores físicos.

Entorno de sistema operativo mixto

Una instancia de vCenter Server instalada en Windows puede registrarse con un Platform Services Controller instalado en Windows o una aplicación Platform Services Controller. Un vCenter Server Appliance puede registrarse con un Platform Services Controller instalado en Windows o una aplicación Platform Services Controller. Tanto vCenter Server como el vCenter Server Appliance puede registrarse con el mismo Platform Services Controller dentro de un dominio.

Figura 1-3. Ejemplo de un entorno de sistema operativo mixto con una instancia de Platform Services Controller externa en Windows

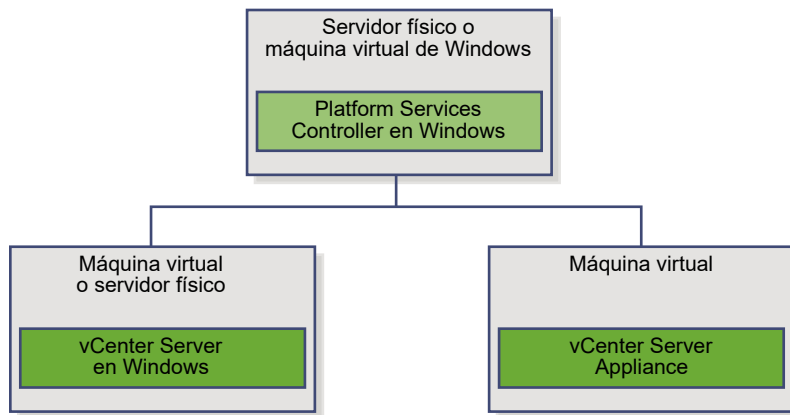
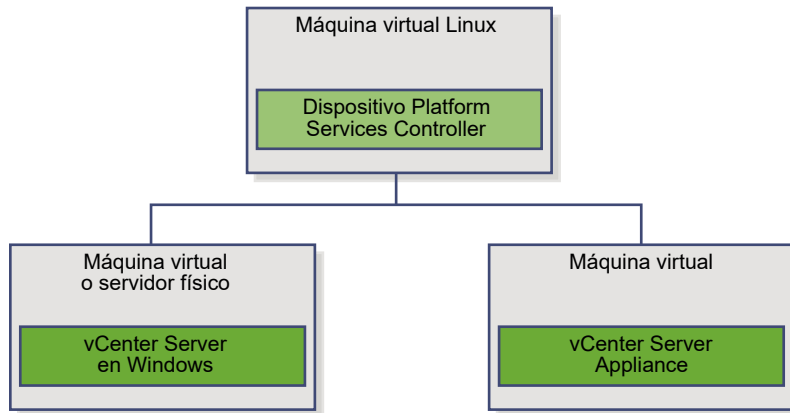


Figura 1-4. Ejemplo de un entorno de sistema operativo mixto con una aplicación de Platform Services Controller externa



Al tener varias instancias de Platform Services Controller que replican sus datos de infraestructura, puede garantizar una alta disponibilidad de su sistema.

Si un Platform Services Controller externo con el que se registró inicialmente su instancia de vCenter Server o vCenter Server Appliance deja de responder, puede redirigir su vCenter Server o vCenter Server Appliance a otro Platform Services Controller externo en el dominio. Para obtener más información, consulte [Redirigir vCenter Server a otra instancia de Platform Services Controller externa](#).

Información general del proceso de instalación y configuración de vSphere

vSphere es un producto sofisticado con varios componentes que puede instalar y configurar. A fin de garantizar una implementación correcta de vSphere, comprenda la secuencia de las tareas requeridas.

La instalación de vSphere incluye las siguientes tareas:

- 1 Lea las notas de la versión de vSphere.
- 2 Compruebe que el sistema cumpla los requisitos de software y hardware de vSphere. Consulte [Capítulo 2 Requisitos del sistema](#).
- 3 Instale ESXi.
 - a Compruebe que el sistema cumpla con los requisitos de hardware mínimos. Consulte [Requisitos de ESXi](#).
 - b Determine la opción de instalación de ESXi que desea utilizar. Consulte [Opciones para instalar ESXi](#).
 - c Determine dónde desea ubicar y arrancar el instalador de ESXi. Consulte [Opciones de medios para arrancar el instalador de ESXi](#). Si va a realizar un arranque PXE del instalador, compruebe que la infraestructura PXE de la red esté configurada correctamente. Consulte [Arranque PXE del instalador de ESXi](#).
 - d Cree una hoja de cálculo con la información que necesitará al instalar ESXi. Consulte [Información obligatoria para instalar ESXi](#).
 - e Instale ESXi.
 - [Instalar ESXi de forma interactiva](#)
 - [Instalar o actualizar hosts mediante un script](#)
 - [Instalar ESXi con vSphere Auto Deploy](#)

Importante En vSphere 6.0, Auto Deploy se instala junto con vCenter Server. A fin de aprovisionar hosts ESXi con Auto Deploy, deberá instalar vCenter Server o implementar vCenter Server Appliance.

- 4 Ajuste la configuración de red y arranque de ESXi, la consola directa y otra configuración. Consulte [Capítulo 5 Configurar ESXi](#) y [Capítulo 6 Después de instalar y configurar ESXi](#).
- 5 Considere la posibilidad de configurar un servidor de Syslog para inicio de sesión remoto, a fin de garantizar que haya almacenamiento de disco suficiente para los archivos de registro. La configuración del registro en un host remoto es especialmente importante para hosts con almacenamiento local limitado. Consulte [Espacio libre necesario para registro del sistema y Configurar Syslog en hosts ESXi](#).
- 6 Instale vCenter Server en una máquina virtual o un servidor físico con Windows, o implemente vCenter Server Appliance.

En vSphere 6.0, puede instalar vCenter Server o implementar vCenter Server Appliance y conectarlos en la configuración Enhanced Linked Mode registrando la instancia de vCenter Server y vCenter Server Appliance en las instancias de Platform Services Controller que replican sus datos de infraestructura.

No se admiten instalaciones simultáneas. Después de instalar o implementar Platform Services Controller, deberá instalar instancias de vCenter Server o implementar vCenter Server Appliance de forma secuencial.

- Instale vCenter Server en una máquina virtual o un servidor físico con Windows.

- 1 Compruebe que su sistema cumpla con los requisitos de hardware y software para la instalación de vCenter Server. Consulte [Requisitos de vCenter Server para Windows](#).
- 2 (Opcional) Configure una base de datos de vCenter Server externa. Consulte [Preparar las bases de datos de vCenter Server para la instalación](#).

Para un entorno con hasta 20 hosts y 200 máquinas virtuales, puede utilizar la base de datos PostgreSQL integrada. Para entornos de producción y gran escala, configure una base de datos externa, debido a que la migración desde la base de datos PostgreSQL integrada a una base de datos externa no es un proceso manual sencillo.

- 3 Cree una hoja de cálculo con la información que necesita para la instalación. Consulte [Información obligatoria para instalar vCenter Server](#).
- 4 Instale vCenter Server y Platform Services Controller. Consulte [Capítulo 8 Instalar vCenter Server en un servidor físico o una máquina virtual de Windows](#).

Puede instalar vCenter Server con una instancia de Platform Services Controller integrada o externa.

La implementación de vCenter Server con una instancia de Platform Services Controller integrada es adecuada para entornos de pequeña escala. La implementación de vCenter Server con una instancia de Platform Services Controller externa es adecuada para los entornos con varias instancias de vCenter Server. Consulte [Modelos de implementación de vCenter Server](#).

- Implemente vCenter Server Appliance.

- 1 Consulte los temas en [Requisitos de vCenter Server Appliance](#) y compruebe que su sistema cumpla con los requisitos de hardware y software para la implementación de vCenter Server Appliance.
- 2 (Opcional) Configure una base de datos de Oracle externa. vCenter Server Appliance solo admite una base de datos de Oracle como una base de datos externa. Consulte [Preparar las bases de datos de vCenter Server para la instalación](#).

También puede utilizar la base de datos PostgreSQL integrada, que es adecuada para entornos que contienen hasta 1.000 hosts y 10.000 máquinas virtuales.

- 3 Utilice el tema [Información necesaria para la implementación de vCenter Server Appliance](#) para crear una hoja de cálculo con la información que necesita para la instalación.
- 4 Implemente vCenter Server Appliance con una instancia de Platform Services Controller integrada o con una instancia de Platform Services Controller externa. Consulte [Capítulo 9 Implementar vCenter Server Appliance](#).

La implementación de vCenter Server con una instancia de Platform Services Controller integrada es adecuada para entornos de pequeña escala. La implementación de vCenter Server con una instancia de Platform Services Controller externa es adecuada para los entornos con varias instancias de vCenter Server. Consulte [Modelos de implementación de vCenter Server](#).

- 7 Conéctese a vCenter Server desde vSphere Web Client. Consulte [Capítulo 11 Después de instalar vCenter Server o implementar vCenter Server Appliance](#).
- 8 Configure vCenter Server y vCenter Server Appliance. Consulte *Administración de vCenter Server y hosts* y *Configuración de vCenter Server Appliance*.

Descripción general de los certificados de seguridad de vSphere

Los hosts ESXi y vCenter Server se comunican de forma segura a través de SSL para garantizar la confidencialidad, la integridad de los datos y la autenticación.

En vSphere 6.0, VMware Certificate Authority (VMCA) aprovisiona cada host ESXi con un certificado firmado que posee VMCA como la entidad de certificación raíz de forma predeterminada. El aprovisionamiento se realiza cuando el host ESXi se agrega a vCenter Server de forma explícita o como parte de la instalación del host ESXi. Todos los certificados de ESXi se almacenan localmente en el host.

Puede utilizar certificados personalizados con una entidad de certificación (CA) raíz diferente. Para obtener información sobre la administración de certificados para hosts ESXi, consulte la *Seguridad de vSphere* documentación.

Todos los certificados para vCenter Server y servicios de vCenter Server se almacenan en VMware Endpoint Certificate Store (VECS).

Puede reemplazar el certificado VMCA para vCenter Server por un certificado diferente firmado por una entidad de certificación (CA). Si desea utilizar un certificado de terceros, instale Platform Services Controller, agregue el certificado raíz firmado por la entidad de certificación (CA) nuevo a VMCA y, a continuación, instale vCenter Server. Para obtener información sobre la administración de certificados de vCenter Server, consulte la documentación de *Seguridad de vSphere*.

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.

VMCA se incluye en cada Platform Services Controller y en cada implementación integrada. VMCA aprovisiona cada nodo, cada usuario de la solución vCenter Server y cada host ESXi con un certificado firmado por VMCA en su calidad de entidad de certificación. Los usuarios de la solución vCenter Server son grupos de servicios de vCenter Server. Consulte *Seguridad de vSphere* para obtener una lista de los usuarios de la solución.

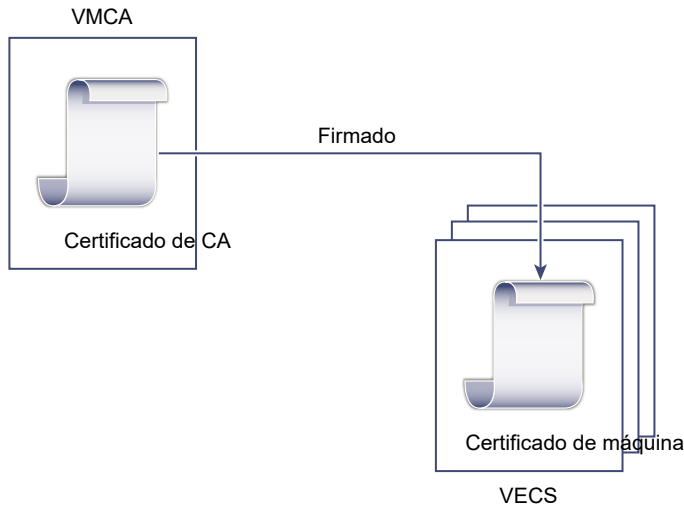
Es posible reemplazar los certificados predeterminados. Para los componentes de vCenter Server, puede usar un conjunto de herramientas de línea de comandos que se incluyen en la instalación. Existen varias opciones.

Consulte la publicación *Seguridad de vSphere* para obtener detalles sobre los flujos de trabajo de reemplazo y sobre la utilidad vSphere Certificate Manager.

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 1-5. Los certificados firmados por VMCA se almacenan en VECS

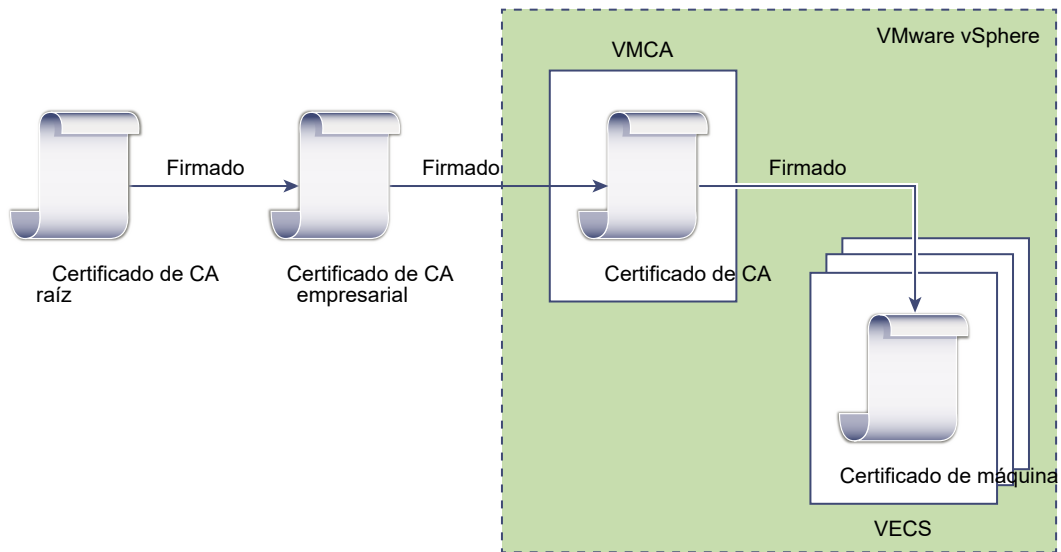


Conversión de VMCA en una CA intermediaria

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.

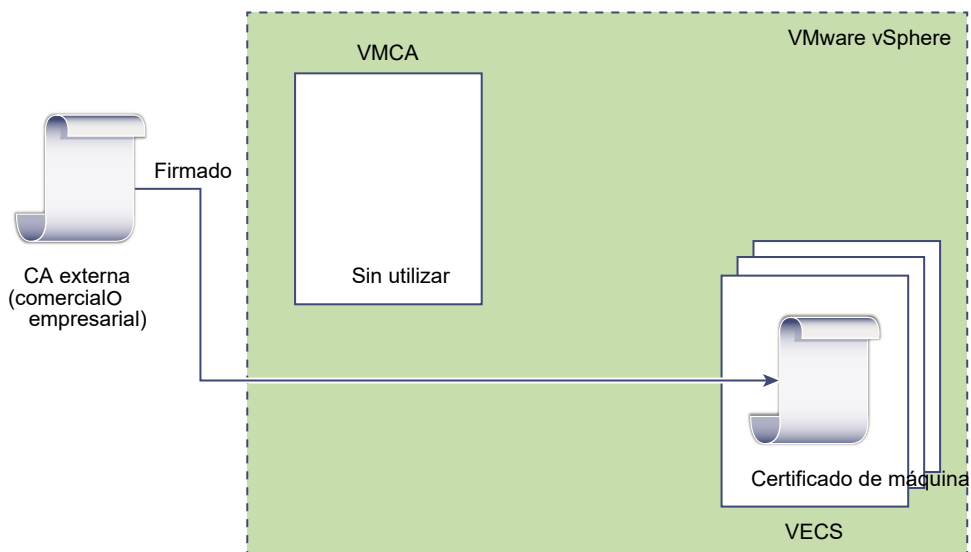
Figura 1-6. Los certificados firmados por una CA empresarial o externa usan VMCA como CA intermediaria



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 1-7. 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.

Descripción general del modo vinculado mejorado

El modo vinculado mejorado conecta varios sistemas vCenter Server por medio de una instancia de Platform Services Controller o más.

El modo vinculado mejorado permite ver y buscar contenido en todos los sistemas vCenter Server vinculados y replicar roles, permisos, licencias, directivas y etiquetas.

Quando instala vCenter Server o implementa vCenter Server Appliance con una instancia de Platform Services Controller externa, primero debe instalar Platform Services Controller. Durante la instalación de Platform Services Controller, puede determinar si desea crear un nuevo dominio de vCenter Single Sign-On o unirse a un dominio existente. Puede seleccionar unirse a un dominio existente de vCenter Single Sign-On si ya instaló o implementó una instancia de Platform Services Controller, y si creó un dominio de vCenter Single Sign-On. Al unirse a un dominio existente de vCenter Single Sign-On, se replican los datos entre la instancia de Platform Services Controller existente y la instancia de Platform Services Controller nueva, y los datos de infraestructura se replican entre las dos instancias de Platform Services Controller.

Con el modo vinculado mejorado, puede conectar no solo sistemas vCenter Server que ejecuten Windows, sino también una gran cantidad de instancias de vCenter Server Appliance. También puede tener un entorno en el que haya varios sistemas vCenter Server y vCenter Server Appliance vinculados juntos.

Si instala vCenter Server con una instancia de Platform Services Controller externa, primero debe implementar Platform Services Controller en una de las máquinas virtuales o en el servidor físico y, a continuación, debe implementar vCenter Server en otras máquinas virtuales o en otro servidor físico. Durante la instalación de vCenter Server, debe seleccionar la instancia de Platform Services Controller externa. Asegúrese de que la instancia de Platform Services Controller que seleccione sea una instancia de Platform Services Controller externa independiente. La selección de una instancia de Platform Services Controller existente que forme parte de una instalación integrada no es compatible y no se puede volver a configurar después de la implementación. Para obtener información sobre las topologías recomendadas, consulte <http://kb.vmware.com/kb/2108548>.

Requisitos del sistema

2

Los sistemas que ejecutan vCenter Server en Windows, vCenter Server Appliance y las instancias de ESXi deben cumplir con requisitos específicos de hardware y sistema operativo.

Si va a utilizar Auto Deploy para aprovisionar hosts ESXi, consulte también [Prepararse para vSphere Auto Deploy](#).

Este capítulo incluye los siguientes temas:

- [Requisitos de ESXi](#)
- [Requisitos de vCenter Server para Windows](#)
- [Requisitos de vCenter Server Appliance](#)
- [Puertos necesarios para vCenter Server y Platform Services Controller](#)
- [Requisitos de DNS de vSphere](#)
- [Requisitos de software de vSphere Web Client](#)
- [Requisitos de software del complemento de integración de clientes](#)
- [Requisitos de vSphere Client](#)
- [Espacio libre necesario para registro del sistema](#)

Requisitos de ESXi

Para instalar ESXi 6.0 o actualizar a ESXi 6.0, su sistema debe cumplir con requisitos de hardware y software específicos.

Requisitos de hardware de ESXi

Asegúrese de que el host cumpla los requisitos de hardware mínimos de ESXi 6.0.

Recursos de hardware y del sistema

Para instalar o actualizar ESXi 6.0, los recursos de hardware y del sistema deben cumplir con los siguientes requisitos:

- Plataforma de servidores compatible. Para obtener una lista de plataformas compatibles, consulte la *Guía de compatibilidad de VMware* en <http://www.vmware.com/resources/compatibility>.

- ESXi 6.0 requiere un equipo host con al menos dos núcleos de CPU.
- ESXi 6.0 admite procesadores x86 de 64 bits lanzados después de septiembre de 2006. Esto incluye una amplia gama de procesadores de varios núcleos. Para obtener una lista completa de procesadores compatibles, consulte la guía de compatibilidad de VMware en <http://www.vmware.com/resources/compatibility>.
- ESXi 6.0 requiere que el bit NX/XD esté habilitado para la CPU en el BIOS.
- ESXi requiere un mínimo de 4 GB de RAM física. Se recomienda proporcionar al menos 8 GB de RAM para ejecutar máquinas virtuales en entornos de producción típicos.
- Para admitir máquinas virtuales de 64 bits, se debe habilitar la compatibilidad para virtualización de (Intel VT-x o RVI AMD) en CPU x64.
- Una o más controladoras Gigabit o Ethernet más rápidas. Para obtener una lista de modelos de adaptadores de red compatibles, consulte la *Guía de compatibilidad de VMware* en <http://www.vmware.com/resources/compatibility>.
- Disco SCSI o un LUN RAID local que no sea de red con espacio sin particionar para las máquinas virtuales.
- Para la serie ATA (SATA), un disco conectado a través de controladoras SAS compatibles o controladoras SATA integradas compatibles. Los discos SATA se considerarán remotos, no locales. Estos discos no se usarán como una partición temporal de forma predeterminada, ya que se consideran remotos.

Nota No puede conectar un dispositivo CD-ROM SATA a una máquina virtual en un host ESXi 6.0. Para usar el dispositivo CD-ROM SATA, debe usar el modo de emulación IDE.

Sistemas de almacenamiento

Para obtener una lista de sistemas de almacenamiento compatibles, consulte la *Guía de compatibilidad de VMware* en <http://www.vmware.com/resources/compatibility>. Para obtener información sobre canal de fibra de software en Ethernet (FCoE), consulte [Instalar y arrancar ESXi con FCoE de software](#).

Requisitos de arranque de ESXi

vSphere 6.0 admite el arranque de hosts ESXi desde la Unified Extensible Firmware Interface (UEFI). Con la UEFI, puede arrancar sistemas desde unidades de disco duro, unidades de CD-ROM o medios USB. Para un arranque de red o aprovisionamiento de VMware Auto Deploy, se requiere el firmware del BIOS heredado y no está disponible con UEFI.

ESXi puede arrancar desde un disco con más de 2 TB siempre que el firmware del sistema y el firmware en cualquier tarjeta adicional que esté usando lo admitan. Consulte la documentación del proveedor.

Nota Si se cambia el tipo de arranque desde el BIOS heredado a UEFI después de instalar ESXi 6.0, es posible que el host no arranque. En este caso, el host muestra un mensaje de error similar a *No un banco de arranque de VMware*. No es posible cambiar el tipo de arranque de host entre el BIOS heredado y UEFI después de instalar ESXi 6.0.

Requisitos de almacenamiento para la instalación o actualización de ESXi 6.0

La instalación de ESXi 6.0 o actualización a ESXi 6.0 requiere un dispositivo de arranque cuyo tamaño sea de al menos 1 GB. Cuando se arranca desde un disco local, SAN o LUN iSCSI, se requiere un disco de 5,2 GB para permitir la creación del volumen de VMFS y la partición temporal de 4 GB en el dispositivo de arranque. Si se usa un disco o LUN de menor tamaño, el instalador intenta asignar una región temporal en un disco local separado. Si un disco local no se puede encontrar, la partición temporal, `/scratch`, se encuentra en el ramdisk de host ESXi, vinculado a `/tmp/scratch`. Puede volver a configurar `/scratch` para que use un disco o LUN separado. Para obtener el mejor rendimiento y optimización de la memoria, no deje `/scratch` en el ramdisk de host ESXi.

Para volver a configurar `/scratch`, consulte [Establecer la partición desde cero de vSphere Web Client](#).

Debido a la sensibilidad de E/S de los dispositivos USB y SD, el instalador no crea una partición temporal en estos dispositivos. Cuando se realiza una instalación o actualización en dispositivos USB o SD, el instalador intenta asignar una región desde cero en un disco o un almacén de datos local disponible. Si no se encuentra un disco o un almacén de datos local, `/scratch` está ubicado en el ramdisk. Después de la instalación o la actualización, debe volver a configurar `/scratch` para usar un almacén de datos persistente. Aunque es suficiente un dispositivo USB o SD de 1 GB para una instalación mínima, debe usar un dispositivo de 4 GB o más grande. El espacio adicional se utilizará para una partición de volcado de memoria del núcleo ampliada en el disco USB/SD. Use una unidad flash USB de alta calidad de 16 GB o mayor de manera que las celdas flash adicionales puedan prolongar la vida útil de los medios de arranque, pero es suficiente con unidades de alta calidad de 4 GB o mayores para mantener la partición de volcado del núcleo ampliada. Consulte el artículo de la base de conocimientos <http://kb.vmware.com/kb/2004784>.

En instalaciones de Auto Deploy, el instalador intenta asignar una región temporal en un disco o un almacén de datos local disponible. Si no se encuentra un disco o un almacén de datos local, `/scratch` está ubicado en ramdisk. Debe volver a configurar `/scratch` para usar un almacén de datos persistente después de la instalación.

Para entornos que arrancan desde un SAN o utilizan Auto Deploy, tiene que asignar un LUN separado para cada host ESXi. Puede localizar conjuntamente las regiones temporales para muchos hosts ESXi en un solo LUN. La cantidad de hosts asignados a un solo LUN deben sopesarse con respecto al tamaño del LUN y el comportamiento de E/S de las máquinas virtuales.

Modelos de servidores de administración remota compatibles y versiones de firmware

Puede utilizar aplicaciones de administración remota para instalar o actualizar ESXi o para administrar hosts de forma remota.

Tabla 2-1. Modelos de servidores de administración remota compatibles y versiones de firmware mínimas

Modelo de servidor de administración remota	Versión de firmware	Java
Dell DRAC 7	1.30.30 (compilación 43)	1.7.0_60-b19
Dell DRAC 6	1.54 (compilación 15), 1.70 (compilación 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20, 1.6.0_203
Dell DRAC 4	1.75	1.6.0_23
ILO HP	1.81, 1.92	1.6.0_22, 1.6.0_23
ILO HP 2	1.8, 1.81	1.6.0_20, 1.6.0_23
ILO HP 3	1.28	1.7.0_60-b19
ILO HP 4	1.13	1.7.0_60-b19
RSA IBM 2	1.03, 1.2	1.6.0_22

Recomendaciones para un rendimiento mejorado de ESXi

Para mejorar el rendimiento, instale o actualice ESXi en un sistema robusto con más RAM que el mínimo necesario y con varios discos físicos.

Para conocer los requisitos del sistema de ESXi, consulte [Requisitos de hardware de ESXi](#). Consulte también los documentos técnicos sobre el rendimiento de vSphere en <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-perfbest-practices-vsphere6-0-white-paper.pdf>.

Tabla 2-2. Recomendaciones para un mejor rendimiento

Elemento del sistema	Recomendación
RAM	<p>Los hosts ESXi requieren más RAM que los servidores típicos. Proporcione al menos 8 GB de RAM para aprovechar al máximo las características de ESXi y ejecutar máquinas virtuales en entornos de producción típicos. Un host ESXi debe tener suficiente RAM para que funcionen máquinas virtuales simultáneas. Se proporcionan los siguientes ejemplos para ayudar a calcular la RAM que necesitan las máquinas virtuales que se ejecutan en el host ESXi.</p> <p>Para operar cuatro máquinas virtuales con Red Hat Enterprise Linux o Windows XP se requiere al menos 3 GB de RAM para rendimiento línea base. Esta cifra incluye aproximadamente 1.024 MB para las máquinas virtuales, 256 MB como mínimo para cada sistema operativo, según lo que recomiendan los proveedores.</p> <p>Para que funcionen estas cuatro máquinas virtuales con 512 MB de RAM, es necesario que los hosts ESXi tengan aproximadamente 4 GB de RAM, lo que incluye 2048 MB para las máquinas virtuales.</p> <p>Estos cálculos no tienen en cuenta los posibles ahorros de memoria derivados de usar memoria con sobrecarga variable para cada máquina virtual. Consulte <i>Administración de recursos de vSphere</i>.</p>
Adaptadores Fast Ethernet dedicados para máquinas virtuales	<p>Coloque la red de administración y las redes de máquinas virtuales en tarjetas de red físicas distintas. Las tarjetas Gigabit Ethernet dedicadas para máquinas virtuales, como adaptadores Intel PRO 1000, mejoran el rendimiento para máquinas virtuales con gran tráfico de red.</p>
Ubicación del disco	<p>Coloque todos los datos que usan las máquinas virtuales en discos físicos asignados específicamente a máquinas virtuales. El rendimiento es mejor cuando no coloca las máquinas virtuales en el disco que contiene la imagen de arranque de ESXi. Use discos físicos que sean lo bastante grandes para mantener imágenes del disco que usan todas las máquinas virtuales.</p>
partición de VMFS5	<p>El instalador de ESXi crea los volúmenes iniciales de VMFS en el primer disco local en blanco que se encuentra. Para agregar discos o modificar la configuración original, use vSphere Web Client. Esta práctica asegura que los sectores de arranque de las particiones estén alineados con 64K, lo que mejora el rendimiento del almacenamiento.</p> <p>Nota Para entornos únicamente de SAS, es posible que el instalador no formatee los discos. Para algunos discos SAS, no es posible identificar si los discos son locales o remotos. Después de la instalación, se puede usar vSphere Web Client para configurar VMFS.</p>

Tabla 2-2. Recomendaciones para un mejor rendimiento (continuación)

Elemento del sistema	Recomendación
Procesadores	Los procesadores más rápidos mejoran el rendimiento de ESXi. Para ciertas cargas de trabajo, una mayor cantidad de memorias caché mejoran el rendimiento de ESXi.
Compatibilidad de hardware	Use dispositivos en el servidor que sean compatibles con controladores de ESXi 6.0. Consulte la <i>Guía de compatibilidad de hardware</i> en http://www.vmware.com/resources/compatibility .

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 2-3. 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.

Tabla 2-3. Conexiones de firewall entrantes (continuación)

Servicio	Puerto	Comentario
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).
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.

Tabla 2-4. 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.
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.

Tabla 2-4. Conexiones de firewall salientes (continuación)

Servicio	Puerto	Comentario
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.
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.

Requisitos de vCenter Server para Windows

Para instalar vCenter Server en una máquina virtual o servidor físico Windows, el sistema debe cumplir con requisitos específicos de hardware y software.

- Sincronice los relojes de las máquinas virtuales en las que tiene pensado instalar vCenter Server y Platform Services Controller. Consulte [Sincronizar los relojes en la red de vSphere](#).
- Compruebe que el nombre de DNS de la máquina virtual o del servidor físico coincida con el nombre completo del equipo.
- Compruebe que el nombre de host de la máquina virtual o del servidor físico donde va a instalar o actualizar vCenter Server cumpla con las directrices de RFC 1123.
- Compruebe que el sistema en el cual va a instalar vCenter Server no sea una controladora de dominio de Active Directory.
- Si el servicio de vCenter Server está ejecutándose en una cuenta de usuario diferente a la cuenta de Local System, compruebe que la cuenta de usuario en la cual se ejecuta el servicio de vCenter Server tenga los siguientes permisos:
 - **Miembro del grupo de administradores**
 - **Iniciar sesión como servicio**
 - **Actuar como parte del sistema operativo (si el usuario es un usuario de dominio)**

- Si el sistema que usa para su instalación de vCenter Server pertenece a un grupo de trabajo en lugar de a un dominio, algunas funcionalidades no estarán disponible para vCenter Server. Si se asigna a un grupo de trabajo, el sistema de vCenter Server no puede detectar todos los dominios y sistemas disponibles en la red cuando se usan algunas características. En caso de que se deseen agregar orígenes de identidad de Active Directory después de la instalación, el equipo host debe estar conectado a un dominio.
- Compruebe que la cuenta LOCAL SERVICE tenga permisos de lectura en la carpeta en la cual está instalado vCenter Server y en el registro HKLM.
- Compruebe que esté funcionando la conexión entre la máquina virtual o el servidor físico y la controladora de dominio.

Comprobaciones previas a la instalación de vCenter Server para Windows

Al instalar vCenter Server y Platform Services Controller, el instalador realiza una comprobación previa a la instalación; por ejemplo, para comprobar que haya espacio suficiente en la máquina virtual o el servidor físico donde va a instalar vCenter Server. También comprueba que se pueda acceder correctamente a la base de datos externa, si es que hay una.

Cuando implementa vCenter Server con una instancia integrada o externa de Platform Services Controller, vCenter Single Sign-On se instala como parte de Platform Services Controller. Durante la instalación, el instalador le brinda la opción de unirse a un dominio de servidor vCenter Single Sign-On existente. Cuando proporciona la información sobre el otro servicio de vCenter Single Sign-On, el instalador utiliza la cuenta de administrador para comprobar el nombre y la contraseña del host, para asegurarse de que los datos del servidor vCenter Single Sign-On que proporcionó puedan autenticarse antes de comenzar el proceso de instalación.

El comprobador previo a la instalación comprueba los siguientes aspectos del entorno:

- Versión de Windows
- Requisitos mínimos de procesador
- Requisitos mínimos de memoria
- Requisitos mínimos de espacio en disco
- Permisos del directorio de instalación y datos seleccionado
- Disponibilidad de puertos internos y externos
- Versión de base de datos externa
- Conectividad de base de datos externa
- Privilegios de administrador en el equipo Windows
- Las credenciales que introduce

Para obtener información sobre los requisitos mínimos de almacenamiento, consulte [Requisitos de almacenamiento de vCenter Server para Windows](#). Para obtener información sobre los requisitos mínimos de hardware, consulte [Requisitos de hardware de vCenter Server para Windows](#).

Requisitos de hardware de vCenter Server para Windows

Cuando instala vCenter Server en una máquina virtual o un servidor físico que ejecuta Microsoft Windows, su sistema debe cumplir con requisitos de hardware específicos.

Puede instalar vCenter Server y Platform Services Controller en la misma máquina virtual o un servidor físico o en máquinas virtuales o servidores físicos diferentes. Cuando instala vCenter Server con una instancia de Platform Services Controller integrada, instala vCenter Server y Platform Services Controller en la misma máquina virtual o servidor físico. Al instalar vCenter Server con una instancia de Platform Services Controller externa, primero instale Platform Services Controller que contiene todos los servicios requeridos en una máquina virtual o un servidor físico y, a continuación, instale vCenter Server y los componentes de vCenter Server en otra máquina virtual o servidor físico.

Nota No se admite la instalación de vCenter Server en una unidad de red o unidad flash USB.

Tabla 2-5. Requisitos de hardware mínimos recomendados para instalar vCenter Server y Platform Services Controller en Windows

	Platform Services Controller	vCenter Server con una instancia integrada o externa de Platform Services Controller para un entorno muy pequeño (hasta 10 hosts y 100 máquinas virtuales)	vCenter Server con una instancia integrada o externa de Platform Services Controller para un entorno pequeño (hasta 100 hosts y 1.000 máquinas virtuales)	vCenter Server con una instancia integrada o externa de Platform Services Controller para un entorno mediano (hasta 400 hosts y 4.000 máquinas virtuales)	vCenter Server con una instancia integrada o externa de Platform Services Controller para un entorno grande (hasta 1.000 hosts y 10.000 máquinas virtuales)
Cantidad de CPU	2	2	4	8	16
Memoria	2 GB de memoria RAM	8 GB de memoria RAM	16 GB de memoria RAM	24 GB de memoria RAM	32 GB de memoria RAM

Para ver los requisitos de hardware de su base de datos, consulte la documentación de la base de datos. Los requisitos de la base de datos son adicionales a los requisitos de vCenter Server en caso de que la base de datos y vCenter Server se ejecuten en la misma máquina.

Requisitos de almacenamiento de vCenter Server para Windows

Cuando se instala vCenter Server, el sistema debe cumplir unos requisitos de almacenamiento mínimos.

Los requisitos de almacenamiento por carpeta dependen del modelo de implementación que se decide instalar. Durante la instalación, se puede seleccionar una carpeta distinta a la predeterminada `C:\Archivos de programa\VMware` para instalar vCenter Server y Platform Services Controller. También es posible seleccionar una carpeta diferente a la predeterminada `C:\ProgramData\VMware\vCenterServer\` en la cual almacenar datos.

Tabla 2-6. Requisitos mínimos de almacenamiento de vCenter Server según el modelo de implementación

Carpeta predeterminada	vCenter Server con una instancia de Platform Services Controller integrada	vCenter Server con una instancia de Platform Services Controller externa	Instancia de Platform Services Controller externa
Archivos de programa	6 GB	6 GB	1 GB
ProgramData	8 GB	8 GB	2 GB
Carpeta de sistema (para almacenar en memoria caché el instalador de MSI)	3 GB	3 GB	1 GB

Requisitos de software de vCenter Server para Windows

Asegúrese de que su sistema operativo sea compatible con vCenter Server.

vCenter Server requiere un sistema operativo de 64 bits y se necesita el DSN de sistema de 64 bits para que vCenter Server pueda conectarse a la base de datos externa.

La versión más antigua de Windows Server admitida por vCenter Server es Windows Server 2008 SP2. Windows Server debe tener instaladas las actualizaciones y revisiones más recientes. Para obtener una lista completa de los sistemas operativos compatibles, consulte <http://kb.vmware.com/kb/2091273>.

Requisitos de base de datos de vCenter Server para Windows

vCenter Server requiere una base de datos para almacenar y organizar datos de servidor.

Cada instancia de vCenter Server debe tener su propia base de datos. En el caso de entornos con hasta 20 hosts y 200 máquinas virtuales, puede utilizar la base de datos de PostgreSQL incluida que el instalador de vCenter Server puede instalar y configurar durante la instalación de vCenter Server. Una instalación más grande requiere una base de datos externa compatible con el tamaño del entorno.

Durante la instalación o actualización de vCenter Server, debe elegir instalar la base de datos integrada o apuntar el sistema vCenter Server a cualquier base de datos compatible existente. vCenter Server admite bases de datos de Oracle y Microsoft SQL Server. Para obtener más información sobre las versiones de servidores de bases de datos compatibles, consulte la matriz de interoperabilidad de productos VMware en http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Requisitos de vCenter Server Appliance

Es posible implementar vCenter Server Appliance en un host ESXi 5.0 o posterior, o bien en una instancia de vCenter Server 5.0 o posterior. El sistema también debe cumplir con los requisitos específicos de software y hardware.

Al usar nombres de dominios completos, asegúrese de que la máquina que use para implementar vCenter Server Appliance y el host de ESXi residan en el mismo servidor DNS.

Antes de implementar vCenter Server Appliance, sincronice los relojes de todas las máquinas virtuales de la red de vSphere. Los relojes sin sincronizar pueden ocasionar problemas de autenticación y pueden producir un error en la instalación o impedir que se inicien los servicios de vCenter Server. Consulte [Sincronizar los relojes en la red de vSphere](#).

Requisitos de hardware de vCenter Server Appliance

Cuando implemente vCenter Server Appliance, puede seleccionar implementar un dispositivo que sea adecuado para el tamaño del entorno de vSphere. La opción que seleccione determina el número de CPU y la cantidad de memoria que tendrá el dispositivo.

Los requisitos de hardware, como la cantidad de CPU y memoria, dependen del tamaño del inventario de vSphere.

Tabla 2-7. Requisitos de hardware para VMware vCenter Server Appliance y el dispositivo de Platform Services Controller

Recursos	Platform Services Controller Appliance	vCenter Server Appliance con una instancia integrada o externa de Platform Services Controller para un entorno muy pequeño (hasta 10 hosts y 100 máquinas virtuales)	vCenter Server Appliance con una instancia integrada o externa de Platform Services Controller para un entorno pequeño (hasta 100 hosts y 1.000 máquinas virtuales)	vCenter Server Appliance con una instancia integrada o externa de Platform Services Controller para un entorno mediano (hasta 400 hosts y 4.000 máquinas virtuales)	vCenter Server Appliance con una instancia integrada o externa de Platform Services Controller para un entorno grande (hasta 1.000 hosts y 10.000 máquinas virtuales)
Cantidad de CPU	2	2	4	8	16
Memoria	2 GB de memoria RAM	8 GB de memoria RAM	16 GB de memoria RAM	24 GB de memoria RAM	32 GB de memoria RAM

Requisitos de almacenamiento de vCenter Server Appliance

Cuando se implementa vCenter Server Appliance, el host en el cual se implementa el dispositivo debe cumplir con requisitos mínimos de almacenamiento. El almacenamiento necesario depende no solo del tamaño del entorno de vSphere, sino también del modo de aprovisionamiento del disco.

Los requisitos de almacenamiento dependen del modelo de implementación que se escoja.

Tabla 2-8. Requisitos mínimos de almacenamiento de vCenter Server según el modelo de implementación

	vCenter Server Appliance con una instancia de Platform Services Controller integrada	vCenter Server Appliance con una instancia de Platform Services Controller externa	Dispositivo Platform Services Controller externo
Entorno muy pequeño (hasta 10 hosts y 100 máquinas virtuales)	120 GB	86 GB	30 GB
Entorno pequeño (hasta 100 hosts y 1.000 máquinas virtuales)	150 GB	108 GB	30 GB
Entorno mediano (hasta 400 hosts, 4.000 máquinas virtuales)	300 GB	220 GB	30 GB
Entorno grande (hasta 1.000 hosts y 10.000 máquinas virtuales)	450 GB	280 GB	30 GB

Software incluido en vCenter Server Appliance

vCenter Server Appliance es una máquina virtual preconfigurada basada en Linux y optimizada para ejecutar vCenter Server y los servicios asociados.

El paquete de vCenter Server Appliance contiene los siguientes componentes de software:

- SUSE Linux Enterprise Server 11, Update 3 para VMware, edición de 64 bits
- PostgreSQL
- Componentes vCenter Server 6.0 y vCenter Server 6.0.

Requisitos de software de vCenter Server Appliance

Es posible implementar VMware vCenter Server Appliance en hosts ESXi 5.0 o posteriores, o bien en instancias de vCenter Server 5.0 o posteriores.

Es posible implementar vCenter Server Appliance únicamente con el complemento de integración de clientes, que es un instalador HTML para Windows que puede utilizarse para conectarse al servidor de destino e implementar vCenter Server Appliance en el servidor. Es posible conectarse directamente a un host ESXi 5.0.x, ESXi 5.1.x, ESXi 5.5.x o ESXi 6.0.x para implementar el dispositivo allí. También es posible conectarse a una instancia de vCenter Server 5.0.x, vCenter Server 5.1.x, vCenter Server 5.5.x o vCenter Server 6.0.x para implementar el dispositivo en un host ESXi o clúster de DRS que resida en el inventario de vCenter Server.

Importante No puede implementarse vCenter Server Appliance mediante vSphere Client ni vSphere Web Client. Durante la implementación de vCenter Server Appliance, debe proporcionar varias entradas, como las contraseñas de vCenter Single Sign-On y del sistema operativo. Si intenta implementar la aplicación mediante vSphere Client o vSphere Web Client, el sistema no le solicita que proporcione estas entradas de datos y se produce un error en la implementación.

Requisitos de base de datos de vCenter Server Appliance

vCenter Server Appliance requiere una base de datos para almacenar y organizar datos de servidor.

Cada instancia de vCenter Server Appliance debe tener su propia base de datos. Puede utilizar la base de datos incluida de PostgreSQL que se incluye en vCenter Server Appliance, la cual admite hasta 1.000 hosts y 10.000 máquinas virtuales.

En el caso de bases de datos externas, vCenter Server Appliance admite solo bases de datos de Oracle. Estas bases de datos de Oracle tienen las mismas versiones que las que se indican en la matriz de interoperabilidad de productos VMware para la versión de vCenter Server que va a instalar. Consulte la matriz de interoperabilidad de productos de VMware en http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Si desea utilizar una base de datos externa, asegúrese de crear un DSN de 64 bits para que vCenter Server pueda conectarse con la base de datos de Oracle.

Puertos necesarios para vCenter Server y Platform Services Controller

El sistema vCenter Server, tanto en Windows como en el dispositivo, deben poder enviar datos a cada host administrado y recibir datos desde los servicios vSphere Web Client y Platform Services Controller. Para permitir las actividades de migración y aprovisionamiento entre los hosts administrados, los hosts de origen y de destino deben poder recibir datos de cada uno.

Si un puerto se encuentra en uso o está restringido, el instalador de vCenter Server mostrará un mensaje de error. Debe utilizar otro número de puerto para continuar con la instalación. Hay puertos internos que se utilizan solo para la comunicación entre los procesos.

VMware utiliza los puertos designados para la comunicación. Además, los hosts administrados supervisan los puertos designados para los datos desde vCenter Server. Si hay un firewall entre cualquiera de estos elementos, el instalador abre los puertos durante el proceso de instalación o actualización. En el caso de firewalls personalizados, debe abrir manualmente los puertos requeridos. Si posee un firewall entre dos hosts administrados y desea realizar actividades en el origen o destino, como la migración o clonación, debe configurar un medio para que los hosts administrados puedan recibir datos.

Nota En Microsoft Windows Server 2008 y versiones posteriores, el firewall está habilitado de manera predeterminada.

Tabla 2-9. Puertos requeridos para la comunicación entre componentes

Puerto	Protocolo	Descripción	Necesario para	Se utiliza para la comunicación entre nodos
22	TCP	Puerto del sistema para SSHD.	Implementaciones de dispositivos de <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	No
80	TCP	<p>vCenter Server requiere el puerto 80 para las conexiones HTTP directas. El puerto 80 redirecciona solicitudes al puerto HTTPS 443. Esta redirección es de suma utilidad si utiliza accidentalmente http://server en lugar de https://server.</p> <p>WS-Management (también requiere que el puerto 443 se encuentre abierto).</p> <p>Si utiliza una base de datos de Microsoft SQL que está almacenada en la misma máquina virtual o servidor físico que vCenter Server, SQL Reporting Service utiliza el puerto 80. Cuando instale o actualice vCenter Server, el instalador le solicitará que cambie el puerto HTTP de vCenter Server. Cambie el puerto HTTP de vCenter Server a un valor personalizado para garantizar una instalación o una actualización correctas.</p> <p>Importante Puede cambiar este número de puerto durante las instalaciones de vCenter Server y Platform Services Controller en Windows.</p>	Instalaciones en Windows e implementaciones de dispositivos de <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	No

Tabla 2-9. Puertos requeridos para la comunicación entre componentes (continuación)

Puerto	Protocolo	Descripción	Necesario para	Se utiliza para la comunicación entre nodos
88	TCP	Servidor de Active Directory. Este puerto debe estar abierto para que el host se una a Active Directory. Si utiliza Active Directory nativo, el puerto debe estar abierto en vCenter Server y Platform Services Controller.	Instalaciones en Windows e implementaciones de dispositivos de Platform Services Controller	No
389	TCP/UDP	<p>Este puerto debe estar abierto en la instancia local y en todas las instancias remotas de vCenter Server. Este es el número de puerto LDAP para Servicios de directorio del grupo vCenter Server. Si se está ejecutando otro servicio en este puerto, podría ser preferible eliminarlo o cambiar el puerto a uno diferente. Puede ejecutar el servicio LDAP en cualquier puerto del 1025 al 65535.</p> <p>Si esta instancia actúa como Microsoft Windows Active Directory, cambie el número de puerto de 389 a un puerto disponible de 1025 a 65535.</p>	Instalaciones en Windows e implementaciones de dispositivos de Platform Services Controller	<ul style="list-style-type: none"> ■ vCenter Server a Platform Services Controller ■ Platform Services Controller a Platform Services Controller

Tabla 2-9. Puertos requeridos para la comunicación entre componentes (continuación)

Puerto	Protocolo	Descripción	Necesario para	Se utiliza para la comunicación entre nodos
443	TCP	<p>El puerto predeterminado que utiliza el sistema vCenter Server para escuchar conexiones desde vSphere Web Client. Para habilitar el sistema vCenter Server para recibir datos desde vSphere Web Client, abra el puerto 443 en el firewall.</p> <p>El sistema vCenter Server también utiliza el puerto 443 para supervisar la transferencia de datos desde clientes de SDK.</p> <p>Este puerto también se utiliza para los siguientes servicios:</p> <ul style="list-style-type: none"> ■ WS-Management (también requiere que el puerto 80 se encuentre abierto) ■ Conexiones del cliente de administración de red de terceros con vCenter Server ■ Acceso de clientes de administración de red de terceros a los hosts <p>Importante Puede cambiar este número de puerto durante las instalaciones de vCenter Server y Platform Services Controller en Windows.</p>	<p>Instalaciones en Windows e implementaciones de dispositivos de</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	<ul style="list-style-type: none"> ■ vCenter Server a vCenter Server ■ vCenter Server a Platform Services Controller ■ Platform Services Controller a vCenter Server
514	TCP/UDP	<p>Puerto de vSphere Syslog Collector para vCenter Server en Windows y puerto de servicio de Syslog de vSphere para vCenter Server Appliance</p> <p>Importante Puede cambiar este número de puerto durante las instalaciones de vCenter Server y Platform Services Controller en Windows.</p>	<p>Instalaciones en Windows e implementaciones de dispositivos de</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	No
636	TCP	vCenter Single Sign-On LDAPS	<p>Instalaciones en Windows e implementaciones de dispositivos de Platform Services Controller</p>	vCenter Server a Platform Services Controller

Tabla 2-9. Puertos requeridos para la comunicación entre componentes (continuación)

Puerto	Protocolo	Descripción	Necesario para	Se utiliza para la comunicación entre nodos
902	TCP/UDP	<p>El puerto predeterminado que utiliza el sistema vCenter Server para enviar datos a los hosts administrados. Los hosts administrados también envían un latido normal a través del puerto UDP 902 al sistema vCenter Server. Este puerto no deberá estar bloqueado por firewalls entre el servidor y los hosts o entre los hosts.</p> <p>El puerto 902 no deberá estar bloqueado entre vSphere Client y los hosts. vSphere Client utiliza este puerto para mostrar las consolas de máquinas virtuales.</p> <p>Importante Puede cambiar este número de puerto durante las instalaciones de vCenter Server en Windows.</p>	Instalaciones en Windows e implementaciones de dispositivos de vCenter Server	No
1514	TCP/UDP	<p>Puerto TLS de vSphere Syslog Collector para vCenter Server en Windows y puerto de servicio de Syslog de vSphere para vCenter Server Appliance</p> <p>Importante Puede cambiar este número de puerto durante las instalaciones de vCenter Server y Platform Services Controller en Windows.</p>	<p>Instalaciones en Windows e implementaciones de dispositivos de</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	No
2012	TCP	Interfaz de control RPC para vCenter Single Sign-On	Instalaciones en Windows e implementaciones de dispositivos de Platform Services Controller	<ul style="list-style-type: none"> ■ vCenter Server a Platform Services Controller ■ Platform Services Controller a vCenter Server ■ Platform Services Controller a Platform Services Controller
2014	TCP	<p>Puerto RPC para todas las API de VMCA (VMware Certificate Authority)</p> <p>Importante Puede cambiar este número de puerto durante las instalaciones de Platform Services Controller en Windows.</p>	Instalaciones en Windows e implementaciones de dispositivos de Platform Services Controller	<ul style="list-style-type: none"> ■ vCenter Server a Platform Services Controller ■ Platform Services Controller a vCenter Server

Tabla 2-9. Puertos requeridos para la comunicación entre componentes (continuación)

Puerto	Protocolo	Descripción	Necesario para	Se utiliza para la comunicación entre nodos
2020	TCP/UDP	Administración del marco de autenticación Importante Puede cambiar este número de puerto durante las instalaciones de vCenter Server y Platform Services Controller en Windows.	Instalaciones en Windows e implementaciones de dispositivos de ■ vCenter Server ■ Platform Services Controller	■ vCenter Server a Platform Services Controller ■ Platform Services Controller a vCenter Server
5480	TCP	Interfaz de administración de dispositivos Abra el extremo que procesa todas las solicitudes HTTPS, XMLRPC y JSON-RPC a través de HTTPS.	Implementaciones de dispositivos de ■ vCenter Server ■ Platform Services Controller	No
6500	TCP/UDP	puerto de ESXi Dump Collector Importante Puede cambiar este número de puerto durante las instalaciones de vCenter Server en Windows.	Instalaciones en Windows e implementaciones de dispositivos de vCenter Server	No
6501	TCP	Servicio de Auto Deploy Importante Puede cambiar este número de puerto durante las instalaciones de vCenter Server en Windows.	Instalaciones en Windows e implementaciones de dispositivos de vCenter Server	No
6502	TCP	Administración de Auto Deploy Importante Puede cambiar este número de puerto durante las instalaciones de vCenter Server en Windows.	Instalaciones en Windows e implementaciones de dispositivos de vCenter Server	No
7444	TCP	Servicio de token seguro	Instalaciones en Windows e implementaciones de dispositivos de Platform Services Controller	■ vCenter Server a Platform Services Controller ■ Platform Services Controller a vCenter Server
9443	TCP	vSphere Web Client HTTPS	Instalaciones en Windows e implementaciones de dispositivos de vCenter Server	No

Tabla 2-9. Puertos requeridos para la comunicación entre componentes (continuación)

Puerto	Protocolo	Descripción	Necesario para	Se utiliza para la comunicación entre nodos
11711	TCP	vCenter Single Sign-On LDAP	-	Solo para compatibilidad con versiones anteriores de vSphere 5.5. De vCenter Single Sign-On 5.5 a Platform Services Controller 6.0
11712	TCP	vCenter Single Sign-On LDAPS	-	Solo para compatibilidad con versiones anteriores de vSphere 5.5. De vCenter Single Sign-On 5.5 a Platform Services Controller 6.0

Para configurar el sistema vCenter Server a fin de que utilice un puerto diferente donde recibir los datos de vSphere Web Client, consulte la documentación de *Administración de vCenter Server y hosts*.

Para obtener más información sobre la configuración del firewall, consulte la documentación de *Seguridad de vSphere*.

Requisitos de DNS de vSphere

vCenter Server, al igual que los demás servidores de red, se instala o se actualiza en un equipo host con una dirección IP fija y un nombre de DNS conocido, para que los clientes puedan acceder al servicio con confianza.

Asigne una dirección IP estática y un nombre de host al servidor de Windows que va a alojar el sistema vCenter Server. Esta dirección IP debe tener un registro de sistema de nombres de dominio (DNS) válido (interno). Al instalar vCenter Server y Platform Services Controller, debe proporcionar el nombre de dominio completo (FQDN) o la dirección IP estática del equipo host en el que va a realizar la instalación o actualización. Se recomienda utilizar el FQDN.

Al implementar vCenter Server Appliance, puede asignar una IP estática al dispositivo. De esta manera, se asegura de que, en caso de que se reinicie el sistema, la dirección IP de vCenter Server Appliance se mantenga igual.

Asegúrese de que la búsqueda inversa de DNS devuelva un FQDN cuando se consulta con la dirección IP del equipo host en el que está instalado vCenter Server. Al instalar o actualizar vCenter Server, se produce un error en la instalación o actualización del componente de servidor web compatible con vSphere Web Client si el instalador no puede buscar el nombre de dominio completo del equipo host vCenter Server a partir de su dirección IP. La búsqueda inversa se implementa mediante registros PTR.

Si utiliza DHCP en lugar de una dirección IP estática para vCenter Server, asegúrese de que el nombre de equipo de vCenter Server se actualice en el servicio de nombres de dominio (DNS). Si puede hacer ping al nombre de equipo, el nombre se actualiza en DNS.

Asegúrese de que la interfaz de administración del host ESXi tenga una resolución de DNS válida desde vCenter Server y todas las instancias de vSphere Web Client. Asegúrese de que vCenter Server tenga una resolución de DNS válida desde todos los hosts ESXi y todas las instancias de vSphere Web Client.

Comprobar que el FQDN se puede resolver

Se instala o actualiza vCenter Server, al igual que cualquier otro servidor de red, en una máquina virtual o un servidor físico con una dirección IP fija y nombre de DNS conocido, a fin de que los clientes puedan acceder con confianza al servicio.

Si tiene pensado utilizar un FQDN para la máquina virtual o servidor físico en el que desea instalar o actualizar vCenter Server, debe comprobar que el FQDN se pueda resolver.

Procedimiento

- ◆ En el símbolo del sistema de Windows, ejecute el comando `nslookup`.

```
nslookup -nosearch -nodefname your_vCenter_Server_FQDN
```

Resultados

Si el FQDN se puede resolver, el comando `nslookup` devuelve la dirección IP y el nombre de la máquina virtual o servidor físico de vCenter Server.

Requisitos de software de vSphere Web Client

Asegúrese de que su explorador sea compatible con vSphere Web Client.

vSphere Web Client 6.0 requiere Adobe Flash Player 16 o versiones posteriores. La última versión de Adobe Flash Player para sistemas Linux es la 11.2. Por lo tanto, vSphere Web Client no se puede ejecutar en plataformas Linux.

VMware ha probado y admite los siguientes sistemas operativos invitados y versiones de explorador para vSphere Web Client. Para obtener el mejor rendimiento, use Google Chrome.

Tabla 2-10. Sistemas operativos invitados compatibles y versiones de explorador mínimas para vSphere Web Client

Sistema operativo	Explorador
Windows	Microsoft Internet Explorer 10.0.19 y versiones posteriores. Mozilla Firefox 34 y versiones posteriores. Google Chrome 39 y versiones posteriores.
Mac OS	Mozilla Firefox 34 y versiones posteriores. Google Chrome 39 y versiones posteriores.

Requisitos de software del complemento de integración de clientes

Si planea instalar el complemento de integración de clientes separado de vSphere Web Client para conectarse a un host ESXi e implementar o actualizar vCenter Server Appliance, asegúrese de que su explorador admita el complemento de integración de clientes.

Para utilizar el complemento de integración de clientes, compruebe que tiene un explorador web compatible.

Tabla 2-11. Exploradores web compatibles

Explorador	Versiones compatibles
Microsoft Internet Explorer	Versión 10 y 11
Mozilla Firefox	Versión 30 y posterior
Google Chrome	Versión 35 y posterior

Requisitos de vSphere Client

Puede instalar vSphere Client para administrar un solo host ESXi. El sistema Windows en el cual instala vSphere Client debe cumplir con los requisitos específicos de hardware y software.

Requisitos de hardware de vSphere Client

Asegúrese de que el hardware de vSphere Client cumpla con los requisitos mínimos.

Requisitos mínimos de hardware y recomendaciones para vSphere Client

Tabla 2-12. Requisitos mínimos de hardware y recomendaciones para vSphere Client

Hardware de vSphere Client	Requisitos y recomendaciones
CPU	1 CPU
Procesador	Procesador Intel o AMD de 500 MHz o superior (1 GHz recomendado)

Tabla 2-12. Requisitos mínimos de hardware y recomendaciones para vSphere Client (continuación)

Hardware de vSphere Client	Requisitos y recomendaciones
Memoria	500 MB (1 GB recomendado)
Almacenamiento en disco	<p>1,5 GB de espacio disponible en disco para una instalación completa, que incluye los siguientes componentes:</p> <ul style="list-style-type: none"> ■ Microsoft .NET 2.0 SP2 ■ Microsoft .NET 3.0 SP2 ■ Microsoft .NET 3.5 SP1 ■ Microsoft Visual J# <p>Quite cualquier versión instalada anteriormente de Microsoft Visual J# en el sistema donde va a instalar vSphere Client.</p> <ul style="list-style-type: none"> ■ vSphere Client <p>Si aún no tiene alguno de estos componentes instalados, debe tener 400 MB libres en la unidad que tiene el directorio %temp%.</p> <p>Si ya tiene todos los componentes instalados, se requieren 300 MB de espacio disponible en la unidad que tiene el directorio %temp%, y 450 MB para vSphere Client.</p>
Redes	Conexión Gigabit recomendada

Requisitos de software de vSphere Client

Asegúrese de que el sistema operativo sea compatible con vSphere Client.

Para obtener una lista completa actualizada de los sistemas operativos compatibles con vSphere Client, consulte [“Sistemas operativos de host compatibles para la instalación de vSphere Client \(Windows\)”](#).

vSphere Client requiere Microsoft .NET Framework 3.5 SP1. Si no está instalado en el sistema, el instalador de vSphere Client lo instalará. Es posible que para la instalación de .NET 3.5 SP1 se requiera una conexión a Internet, para descargar más archivos.

Puertos TCP y UDP para vSphere Client

Se usan los puertos TCP y UDP predeterminados para acceder a los hosts ESXi y otros componentes de red. 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).

Tabla 2-13. Puertos TCP y UDP

Puerto	Propósito	Tipo de tráfico
443 (valor predeterminado)	Acceso HTTPS Acceso de vSphere Client a vCenter Server Acceso de vSphere Client a hosts ESXi Acceso de vSphere Client a vSphere Update Manager	TCP entrante al host ESXi
902 (valor predeterminado)	Acceso de vSphere Client a consolas de máquinas virtuales	TCP entrante al host ESXi, TCP saliente del host ESXi, UDP saliente del host ESXi

Espacio libre necesario para registro del sistema

Si utilizó Auto Deploy para instalar el host ESXi 6.0, o bien si configuró un directorio de registro separado de la ubicación predeterminada en un directorio totalmente nuevo en el volumen de VMFS, podría necesitar cambiar la configuración de tamaño y rotación de registro actual para garantizar que haya suficiente espacio disponible para el registro del sistema.

Todos los componentes de vSphere usan esta infraestructura. Los valores predeterminados para la capacidad de registros en esta infraestructura varían según la cantidad de almacenamiento disponible y cómo ha configurado el registro del sistema. Los hosts que se implementan con Auto Deploy almacenan registros en un disco RAM, lo que significa que hay poca cantidad de espacio disponible para registros.

Si su host se implementa con Auto Deploy, vuelva a configurar el almacenamiento de sus registros de una de estas formas:

- Redirija los registros a través de la red hacia un recopilador remoto.
- Redirija registros hacia un almacenamiento NAS o NFS.

Si redirige los registros hacia un almacenamiento no predeterminado, como NAS o NFS, es posible que también desee volver a configurar el dimensionamiento y las rotaciones de los registros para los hosts que están instalados en el disco.

No tiene que volver a configurar el almacenamiento de registros para hosts ESXi que utilizan la configuración predeterminada, que almacena registros en un directorio temporal en el volumen de VMFS. Para estos hosts, ESXi 6.0 configura registros para que se adecúen de la mejor manera a su instalación y proporciona suficiente espacio para alojar mensajes de registros.

Tabla 2-14. Configuración recomendada de tamaño y rotación mínima para registros hostd, vpxa y fdm

Registro	Tamaño máximo de archivo de registro	Cantidad de rotaciones que se debe mantener	Espacio de disco mínimo necesario
Agente de administración (hostd)	10 MB	10	100 MB
Agente VirtualCenter (vpxa)	5 MB	10	50 MB
Agente de vSphere HA (administrador de dominio de fallas, fdm)	5 MB	10	50 MB

Para obtener información sobre la configuración de un servidor de registro remoto, consulte [Configurar Syslog en hosts ESXi](#).

Antes de instalar ESXi

3

Antes de instalar ESXi, debe comprender el proceso y las opciones de instalación.

Este capítulo incluye los siguientes temas:

- [Opciones para instalar ESXi](#)
- [Opciones de medios para arrancar el instalador de ESXi](#)
- [Usar aplicaciones de administración remota](#)
- [Información obligatoria para instalar ESXi](#)
- [Descarga del instalador de ESXi](#)

Opciones para instalar ESXi

ESXi puede instalarse de varias maneras. Para garantizar que vSphere se implemente de la mejor manera, debe comprender las opciones en profundidad antes de comenzar la instalación.

Las instalaciones de ESXi están diseñadas para incluir distintos tamaños de implementación.

En base al método que elija, tendrá diferentes opciones disponibles para acceder a medios de instalación y arrancar el instalador.

Instalar ESXi de manera interactiva

Las instalaciones interactivas se recomiendan para las implementaciones pequeñas con menos de cinco hosts.

El instalador se arranca desde un CD o DVD, desde un dispositivo USB de arranque o mediante un arranque con PXE del instalador desde una ubicación de la red. Debe seguir las indicaciones del asistente de instalación para instalar ESXi en el disco. Consulte [Instalar ESXi de forma interactiva](#).

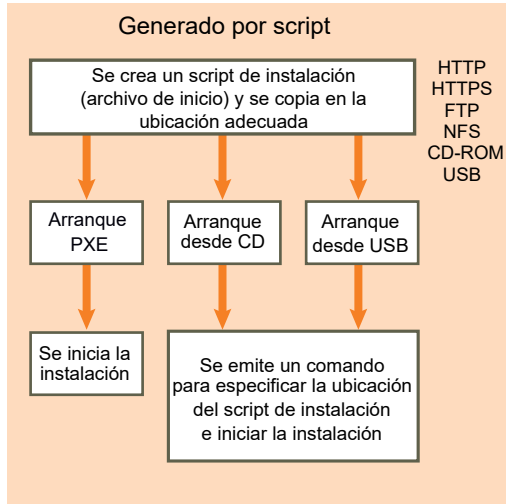
Instalación de ESXi generada por script

La ejecución de un script es una manera eficaz de implementar varios hosts ESXi mediante una instalación desatendida.

El script de instalación contiene los ajustes de configuración del host. Puede usar el script para configurar varios hosts con las mismas opciones. Consulte [Instalar o actualizar hosts mediante un script](#).

El script de instalación debe almacenarse en una ubicación a la que el host pueda acceder mediante HTTP, HTTPS, FTP, NFS, CD-ROM o USB. Puede arrancar el instalador de ESXi mediante PXE o desde una unidad USB o de CD/DVD.

Figura 3-1. Instalación generada por script



Instalar Auto Deploy ESXi

vSphere 5.x y vSphere 6.0 proporcionan varias formas para instalar ESXi con Auto Deploy.

Estos temas describen las opciones de Auto Deploy para la instalación de ESXi.

Aprovisionar hosts ESXi mediante vSphere Auto Deploy

Con la característica vSphere Auto Deploy ESXi, es posible aprovisionar y reaprovisionar grandes cantidades de hosts ESXi de manera eficaz con vCenter Server.

Al aprovisionar hosts mediante Auto Deploy, vCenter Server carga la imagen de ESXi directamente en la memoria del host. Auto Deploy no almacena el estado de ESXi en el disco host.

vCenter Server permite que las actualizaciones y las revisiones de ESXi estén disponibles para descarga a través de un perfil de imagen. De manera opcional, la configuración del host se proporciona a través de un perfil de host. Puede crear perfiles de host mediante vSphere Web Client. Puede crear perfiles de imagen personalizados mediante ESXi Image Builder CLI. Consulte [Usar vSphere ESXi Image Builder](#) y *Perfiles de host de vSphere*.

La primera vez que se aprovisiona un host mediante Auto Deploy, el PXE del host arranca el servidor Auto Deploy y establece contacto con él, lo que transmite el perfil de imagen y el perfil de host al host. El host comienza a usar el perfil de host y Auto Deploy asigna el host al sistema vCenter Server adecuado.

Cuando se reinicia el host, el servidor Auto Deploy sigue aprovisionando el host con el perfil de imagen y el perfil de host adecuados. Para aprovisionar el host con un perfil de imagen diferente, debe cambiar la regla que especifica el perfil de imagen y, posteriormente, realizar una operación de prueba y reparación de cumplimiento. Para propagar los cambios a todos los hosts que especifica la regla, cambie la regla y, a continuación, realice la operación de prueba y reparación. La capacidad de propagar cambios a varios hosts hace que Auto Deploy sea un mecanismo eficaz para aprovisionar y reaprovisionar grandes cantidades de hosts, y para aplicar el cumplimiento de normas en una imagen de ESXi.

Consulte [Información sobre vSphere Auto Deploy](#).

Usar vSphere Auto Deploy para instalaciones con estado

En algunas situaciones, puede resultar útil aprovisionar los hosts con Auto Deploy y realizar todos los arranques siguientes desde el disco.

Puede utilizar vSphere Auto Deploy para aprovisionar un host ESXi y configurar un perfil de host que haga que el host almacene la imagen y la configuración de ESXi en el disco local, un disco remoto o una unidad USB. Posteriormente, el host ESXi arrancará desde esta imagen local. Auto Deploy ya no realiza el aprovisionamiento del host. Este proceso es similar a realizar una instalación generada por scripts. Con una instalación generada por scripts, el script aprovisiona un host y el host arranca desde el disco. Para este caso, Auto Deploy aprovisiona un host y después el host arranca desde el disco.

Consulte [Usar Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado](#).

vSphere Auto Deploy y almacenamiento en caché sin estado

Puede utilizar vSphere Auto Deploy para aprovisionar un host ESXi y configurar un perfil de host que haga que el host almacene la imagen y la configuración de ESXi en el disco local, un disco remoto o una unidad USB.

Posteriormente, el servidor Auto Deploy sigue aprovisionando este host. Si el servidor Auto Deploy no está disponible, el host utiliza la imagen en el disco.

Consulte [Usar Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado](#).

Personalizar instalaciones con ESXi Image Builder CLI

Puede usar ESXi Image Builder CLI para crear imágenes de instalación de ESXi con un conjunto personalizado de actualizaciones, revisiones y controladores.

ESXi Image Builder CLI es un conjunto de comandos de PowerShell CLI que puede usarse para crear imágenes de instalación de ESXi con un conjunto personalizado de actualizaciones y revisiones de ESXi. También se pueden incluir controladores de almacenamiento o red de otros fabricantes que se lancen entre versiones de vSphere.

Se puede implementar una imagen de ESXi creada con Image Builder de cualquiera de las siguientes maneras:

- Grabando la imagen en un DVD de instalación.

- Mediante vCenter Server, utilizando la característica Auto Deploy.

Consulte [Usar vSphere ESXi Image Builder](#) y [Instalar ESXi con vSphere Auto Deploy](#).

Acerca de los modos de evaluación y con licencia de ESXi

Puede utilizar el modo de evaluación para explorar el conjunto completo de funciones para los hosts ESXi. El modo de evaluación proporciona un conjunto de funciones equivalente a una licencia de vSphere Enterprise Plus. Antes de que finalice el modo de evaluación, debe asignar a sus hosts una licencia que admita todas las funciones en uso.

Por ejemplo, en el modo de evaluación, puede utilizar la tecnología vSphere vMotion, la función vSphere HA, la característica vSphere DRS y otras características. Si desea continuar utilizando estas funciones, debe asignar una licencia que las admita.

La versión de los hosts ESXi Installable se instala siempre en el modo de evaluación. ESXi Embedded se ofrece preinstalado en el dispositivo de almacenamiento interno por parte de cada proveedor de hardware. Podría estar en el modo de evaluación o con licencia previa.

El período de evaluación es de 60 días y comienza cuando se enciende el host ESXi. En cualquier momento durante el período de evaluación de 60 días, se puede realizar la conversión de un modo con licencia a un modo de evaluación. El tiempo disponible en el modo de evaluación se resta del tiempo ya consumido.

Por ejemplo, supongamos que se utiliza un host ESXi en el modo de evaluación durante 20 días y, a continuación, se asigna una clave de licencia de vSphere Standard Edition al host. Si se vuelve a establecer el host en el modo de evaluación, se podrá explorar el conjunto completo de funciones para el host durante el período de evaluación restante de 40 días.

Para obtener información sobre la administración de licencias para los hosts ESXi, consulte la documentación *Administración de vCenter Server y hosts*.

Opciones de medios para arrancar el instalador de ESXi

El instalador de ESXi debe ser accesible para el sistema en el que se va a instalar ESXi.

Los siguientes medios de arranque son compatibles con el instalador de ESXi:

- Arranque desde un CD/DVD. Consulte [Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi](#).
- Arranque desde una unidad flash USB. Consulte [Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi](#).
- Arranque PXE desde la red. [Arranque PXE del instalador de ESXi](#)
- Arranque desde una ubicación remota mediante una aplicación de administración remota. Consulte [Usar aplicaciones de administración remota](#)

Descargar y grabar un CD o DVD de la imagen ISO del instalador de ESXi

Si no tiene un CD/DVD de instalación de ESXi, puede crear uno.

También puede crear una imagen ISO del instalador que incluya un script de instalación personalizado. Consulte [Crear una imagen ISO de instalador con un script de instalación o actualización personalizado](#).

Procedimiento

- 1 Descargue el instalador de ESXi desde el sitio web de VMware en <https://my.vmware.com/web/vmware/downloads>.
ESXi aparece en la sección Centro de datos e infraestructura de nube.
- 2 Confirme que el valor de md5sum sea correcto.
Consulte el tema del sitio web de VMware Uso de sumas de comprobación de MD5 en <http://www.vmware.com/download/md5.html>.
- 3 Grabe la imagen ISO en un CD o DVD.

Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi

Puede formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.

En las instrucciones de este procedimiento, se supone que la unidad flash USB se detecta como `/dev/sdb`.

Nota El archivo `ks.cfg` que contiene el script de instalación no puede estar ubicado en la misma unidad flash USB que se utiliza para arrancar la instalación o la actualización.

Requisitos previos

- Equipo Linux al que se acceda como superusuario
- Unidad flash USB que el equipo Linux pueda detectar
- Imagen ISO de ESXi, `VMware-VMvisor-Installer-número_versión-número_compilación.x86_64.iso`, que incluye el archivo `isolinux.cfg`
- Paquete Syslinux

Procedimiento

- 1 Si la unidad flash USB no se detecta como `/dev/sdb`, o si no conoce con certeza la forma en que se detecta la unidad flash USB, determine la manera en que se detecta.

- a En la línea de comandos, ejecute el comando para mostrar los mensajes de registro actuales.

```
tail -f /var/log/messages
```

- b Conecte la unidad flash USB.

Se mostrarán varios mensajes en los que se identifica la unidad flash USB con un formato similar al del siguiente mensaje.

```
Oct 25 13:25:23 ubuntu kernel: [ 712.447080] sd 3:0:0:0: [sdb] Attached SCSI removable disk
```

En este ejemplo, `sdb` identifica el dispositivo USB. Si el dispositivo se identifica de un modo diferente, use esa identificación en lugar de `sdb`.

- 2 Cree una tabla de particiones en el dispositivo flash USB.

```
/sbin/fdisk /dev/sdb
```

- a Introduzca `d` para eliminar las particiones hasta que no quede ninguna.
 - b Introduzca `n` para crear una partición principal 1 que se extienda a todo el disco.
 - c Introduzca `t` para configurar el tipo en una opción de configuración adecuada para el sistema de archivos FAT32, por ejemplo, `c`.
 - d Introduzca `a` para establecer la marca de activo en la partición 1.
 - e Introduzca `p` para imprimir la tabla de particiones.

El resultado debe ser similar al siguiente mensaje.

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes 255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes Device Boot Start End Blocks Id
System /dev/sdb1 1 243 1951866 c W95 FAT32 (LBA)
```

- f Introduzca `w` para escribir la tabla de particiones y salir del programa.

- 3 Formatee la unidad flash USB con el sistema de archivos Fat32.

```
/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
```

4 Instale el cargador de arranque de Syslinux en la unidad flash USB.

Las ubicaciones del archivo ejecutable de Syslinux y del archivo `mbr.bin` pueden variar según las versiones de Syslinux. Por ejemplo, si descargó Syslinux 6.02, ejecute los siguientes comandos.

```
/usr/bin/syslinux /dev/sdb1
cat /usr/lib/syslinux/mbr/mbr.bin > /dev/sdb
```

5 Cree un directorio de destino y monte la unidad flash USB allí.

```
mkdir /usbdisk
mount /dev/sdb1 /usbdisk
```

6 Cree un directorio de destino y monte la imagen ISO del instalador de ESXi allí.

```
mkdir /esxi_cdrom
mount -o loop VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso /esxi_cdrom
```

7 Copie el contenido de la imagen ISO en la unidad flash USB.

```
cp -r /esxi_cdrom/* /usbdisk
```

8 Cambie el nombre del archivo `isolinux.cfg` por `syslinux.cfg`.

```
mv /usbdisk/isolinux.cfg /usbdisk/syslinux.cfg
```

9 En el archivo `/usbdisk/syslinux.cfg`, cambie la línea `APPEND -c boot.cfg` por `APPEND -c boot.cfg -p 1`.

10 Desmonte la unidad flash USB.

```
umount /usbdisk
```

11 Desmonte la imagen ISO del instalador.

```
umount /esxi_cdrom
```

Resultados

La unidad flash USB puede arrancar el instalador de ESXi.

Crear una unidad flash USB para almacenar el script de instalación o actualización de ESXi

Puede utilizar una unidad flash USB para almacenar el script de instalación o actualización de ESXi que se va a utilizar para la instalación o actualización por script de ESXi.

Si existen varias unidades flash USB en el equipo de instalación, el software de instalación busca el script de instalación o actualización en todas las unidades flash USB que estén conectadas.

En las instrucciones de este procedimiento se supone que la unidad flash USB se detecta como `/dev/sdb`.

Nota El archivo `ks` que contiene el script de instalación o actualización no puede estar en la misma unidad flash USB que se utiliza para arrancar la instalación o actualización.

Requisitos previos

- Equipo Linux
- Script de instalación o actualización de ESXi, el archivo kickstart `ks.cfg`
- Unidad flash USB

Procedimiento

- 1 Conecte la unidad flash USB a un equipo Linux con acceso al script de instalación o actualización.

- 2 Cree una tabla de particiones.

```
/sbin/fdisk /dev/sdb
```

- a Escriba `d` para eliminar las particiones hasta que no quede ninguna.
- b Escriba `n` para crear la partición principal 1 que abarca todo el disco.
- c Escriba `t` para configurar el tipo para una configuración adecuada para el sistema de archivos FAT32, por ejemplo, `c`.
- d Escriba `p` para imprimir la tabla de particiones.

El resultado debe ser similar al texto siguiente:

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes
255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1             1           243        1951866   c   W95 FAT32 (LBA)
```

- e Escriba `w` para escribir la tabla de particiones y salir.

- 3 Formatee la unidad flash USB con el sistema de archivos Fat32.

```
/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
```

- 4 Monte la unidad flash USB.

```
mount /dev/sdb1 /usbdisk
```

- 5 Copie el script de instalación de ESXi en la unidad flash USB.

```
cp ks.cfg /usbdisk
```

- 6 Desmonte la unidad flash USB.

Resultados

La unidad flash USB contiene el script de instalación o actualización de ESXi.

Pasos siguientes

Al arrancar el instalador de ESXi, apunte a la ubicación de la unidad flash USB del script de instalación o actualización. Consulte [Introducir las opciones de arranque para iniciar un script de instalación o actualización](#) y [Acerca de los archivos de configuración de PXE](#).

Crear una imagen ISO de instalador con un script de instalación o actualización personalizado

Puede personalizar la imagen ISO del instalador de ESXi estándar con su propio script de instalación o actualización. Esta personalización permite realizar una instalación o actualización desatendida y generada por script cuando arranque la imagen ISO del instalador resultante.

Consulte también [Acerca de los scripts de instalación y actualización](#) y [Acerca del archivo boot.cfg](#).

Requisitos previos

- Equipo Linux
- La imagen ISO de ESXi `VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso`, donde `6.x.x` es la versión de ESXi que está instalando y `XXXXXX` es el número de compilación de la imagen ISO del instalador
- Su script de instalación o actualización personalizado, el archivo de inicio `ks_cust.cfg`

Procedimiento

1 Descargue la imagen ISO de ESXi desde el sitio web de VMware.

2 Monte la imagen ISO en una carpeta:

```
mount -o loop VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso /
esxi_cdrom_mount
```

`XXXXXX` es el número de versión de ESXi para la versión que está instalado o la versión a la que está actualizando.

3 Copie el contenido de `cdrom` a otra carpeta:

```
cp -r /esxi_cdrom_mount /esxi_cdrom
```

4 Copie el archivo de inicio a `/esxi_cdrom`.

```
cp ks_cust.cfg /esxi_cdrom
```

- 5 (opcional) Modifique el archivo `boot.cfg` para especificar la ubicación del script de instalación o actualización a través de la opción `kernelopt`.

Debe utilizar caracteres en mayúscula para proporcionar la ruta de acceso del script, por ejemplo,

```
kernelopt=runweasel ks=cdrom:/KS_CUST.CFG
```

Este paso automatiza la instalación o la actualización, sin la necesidad de especificar el archivo de inicio durante este proceso.

- 6 Recree la imagen ISO:

```
mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b isolinux.bin -c boot.cat -no-emul-boot -boot-load-size 4 -boot-info-table /esxi_cdrom
```

Resultados

La imagen ISO incluye su script de instalación o actualización personalizado.

Pasos siguientes

Instale ESXi desde la imagen ISO.

Arranque PXE del instalador de ESXi

Puede utilizar el entorno de ejecución previo al inicio (PXE) para arrancar un host e iniciar el instalador de ESXi desde una interfaz de red.

ESXi 6.0 se distribuye en un formato ISO que está diseñado para instalarse en la memoria flash o en un disco duro local. Puede extraer los archivos y arrancar con PXE.

PXE utiliza el protocolo de configuración dinámica de host (DHCP) y el protocolo trivial de transferencia de archivos (TFTP) para arrancar un sistema operativo a través de una red.

El arranque con PXE requiere determinada infraestructura de red y una máquina con un adaptador de red compatible con PXE. La mayoría de las máquinas que pueden ejecutar ESXi poseen adaptadores de red que pueden arrancar con PXE.

Nota Asegúrese de que el servidor vSphere Auto Deploy posea una dirección IPv4. El arranque PXE solo es compatible con IPv4.

Acerca del servidor TFTP, PXELINUX y gPXE

El protocolo trivial de transferencia de archivos (TFTP) es similar al servicio FTP y se utiliza generalmente solo para los sistemas de arranque de red o la carga de firmware en dispositivos de red, como los enrutadores.

La mayoría de las distribuciones de Linux incluyen una copia del servidor `tftp-hpa`. Si requiere una solución compatible, adquiera un servidor TFTP compatible de su proveedor de confianza.

Si su servidor TFTP va a funcionar en un host de Microsoft Windows, utilice tftpd32 versión 2.11 o posterior. Consulte <http://tftpd32.jounin.net/>. Las versiones anteriores de tftpd32 no eran compatibles con PXELINUX y gPXE.

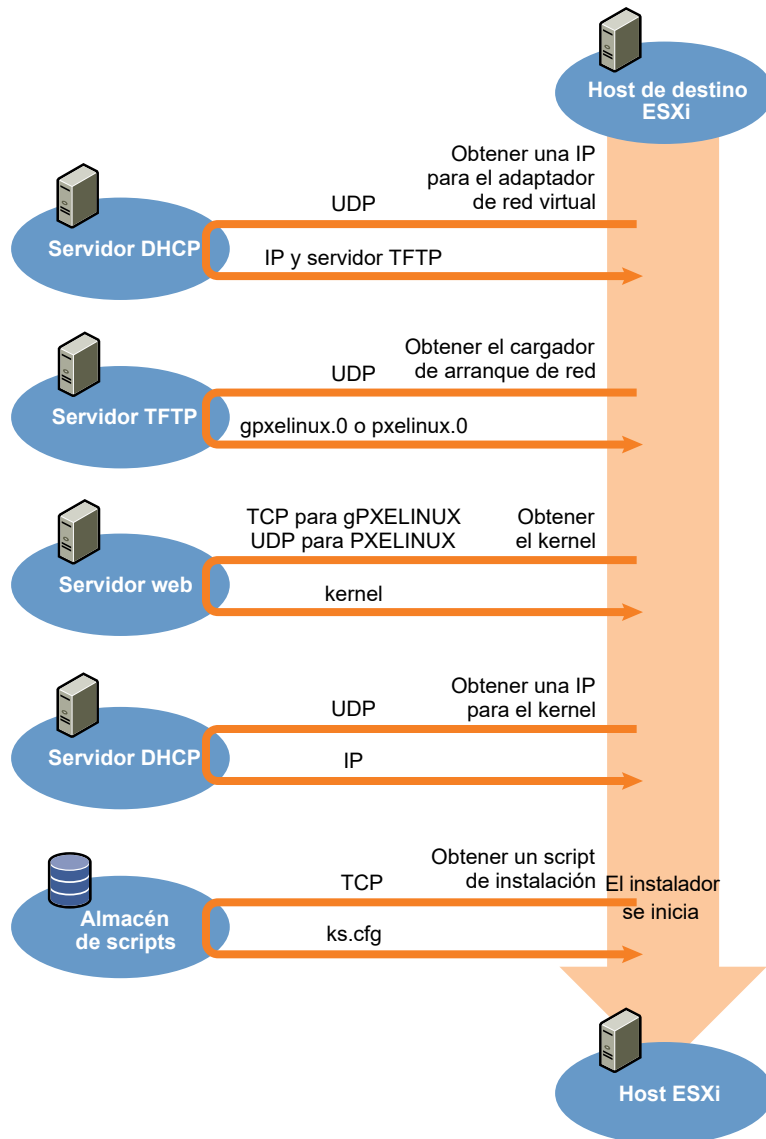
También puede adquirir un servidor TFTP desde uno de los dispositivos de paquete en VMware Marketplace.

Los entornos de PXELINUX y gPXE permiten que su máquina de destino arranque con el instalador de ESXi. PXELINUX es parte del paquete SYSLINUX, que puede encontrarse en <http://www.kernel.org/pub/linux/utils/boot/syslinux/>, aunque muchas distribuciones de Linux lo incluyen. Muchas versiones de PXELINUX también incluyen gPXE. Algunas distribuciones, como Red Hat Enterprise Linux versión 5.3, incluyen versiones anteriores de PXELINUX que no contienen gPXE.

Si no utiliza gPXE, podría sufrir problemas al arrancar con el instalador de ESXi en una red sumamente cargada y TFTP se vuelve algunas veces inestable para la transferencia de grandes cantidades de datos. Si utiliza PXELINUX sin gPXE, el archivo binario `pxelinux.0`, el archivo de configuración, el kernel y otros archivos se transfieren a través de TFTP. Si utiliza gPXE, solo el archivo binario `gpxelinux.0` y el archivo de configuración se transfieren a través de TFTP. Con gPXE, puede utilizar un servidor web para transferir el kernel y otros archivos requeridos para arrancar con el instalador de ESXi.

Nota VMware prueba el arranque PXE con la versión 3.86 de PXELINUX. Esta no es una declaración de compatibilidad limitada. En el caso de la compatibilidad de agentes de terceros que utilice para configurar su infraestructura de arranque PXE, póngase en contacto con el proveedor.

Figura 3-2. Descripción general de la instalación del arranque PXE



Configuración de DHCP de muestra

Para arrancar el instalador de ESXi mediante PXE, el servidor DHCP debe enviar la dirección al servidor TFTP y un puntero al directorio `pxelinux.0` o `gpxelinux.0`.

La máquina de destino usa el servidor DHCP para obtener una dirección IP. El servidor DHCP debe ser capaz de determinar si la máquina de destino puede arrancar y, asimismo, de determinar la ubicación del archivo binario de PXELINUX (que generalmente reside en un servidor TFTP). Cuando la máquina de destino se arranca por primera vez, transmite un paquete mediante la red para solicitar esta información a fin de realizar un arranque. El servidor DHCP responde.

Precaución No configure un nuevo servidor DHCP si la red ya tiene uno. Si varios servidores DHCP responden a las solicitudes de DHCP, las máquinas pueden obtener direcciones IP incorrectas o en conflicto, o no recibir la información de arranque correcta. Consulte a un administrador de red antes de configurar un servidor DHCP. Para obtener asistencia en relación con la configuración de DHCP, póngase en contacto con el proveedor del servidor DHCP.

Muchos servidores DHCP tienen hosts de arranque mediante PXE. Si usa una versión de DHCP para Microsoft Windows, consulte la documentación del servidor DHCP para determinar cómo transmitir los argumentos `next-server` y `filename` a la máquina de destino.

Ejemplo de gPXE

En este ejemplo se muestra cómo configurar un servidor DHCP de ISC versión 3.0 para habilitar gPXE.

```
allow booting;
allow bootp;
# gPXE options
option space gppe;
option gppe-encap-opts code 175 = encapsulate gppe;
option gppe.bus-id code 177 = string;
class "pexclients" {
    match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
    next-server TFTP server address;
    if not exists gppe.bus-id {
        filename "/gpxelinux.0";
    }
}
subnet Network address netmask Subnet Mask {
    range Starting IP AddressEnding IP Address;
}
```

Cuando una máquina intenta realizar un arranque mediante PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `gpxelinux.0` en el servidor TFTP. La dirección IP asignada se ubica en el rango definido en la sección de la subred del archivo de configuración.

Ejemplo de PXELINUX (sin gPXE)

En este ejemplo se muestra cómo configurar un servidor DHCP de ISC versión 3.0 para habilitar PXELINUX.

```
#
# DHCP Server Configuration file.
# see /usr/share/doc/dhcp*/dhcpd.conf.sample
```



```
#
ddns-update-style ad-hoc;
allow booting;
allow bootp;
class "pxeclients" {
    match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
    next-server xxx.xxx.xx.xx;
    filename = "pxelinux.0";
}
subnet 192.168.48.0 netmask 255.255.255.0 {
    range 192.168.48.100 192.168.48.250;
}
```

Cuando una máquina intenta realizar un arranque mediante PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `pxelinux.0` en el servidor TFTP. La dirección IP asignada se ubica en el rango definido en la sección de la subred del archivo de configuración.

Acerca de los archivos de configuración de PXE

El archivo de configuración de PXE define el menú visualizado en el host ESXi de destino a medida que arranca y entra en contacto con el servidor TFTP. Se necesita un archivo de configuración de PXE para que PXE arranque el instalador de ESXi.

El servidor TFTP se encuentra constantemente en el modo de escucha para la búsqueda de clientes PXE en la red. Cuando detecta que un cliente PXE está solicitando los servicios de PXE, envía al cliente un paquete de red que contiene un menú de arranque.

Archivos requeridos

En el archivo de configuración de PXE, debe incluir rutas de acceso a los siguientes archivos:

- `mboot.c32` es el cargador de arranque.
- `boot.cfg` es el archivo de configuración del cargador de arranque.

Consulte [Acerca del archivo boot.cfg](#)

Nombre del archivo de configuración de PXE

Para el nombre del archivo de configuración de PXE, seleccione una de las siguientes opciones:

- `01-mac_address_of_target_ESXi_host`. Por ejemplo, `01-23-45-67-89-0a-bc`
- La dirección IP del host ESXi de destino en anotación hexadecimal.
- `default`

El archivo de arranque inicial, `pxelinux.0` o `gpxelinux.0`, intenta cargar un archivo de configuración de PXE. Intenta con la dirección MAC del host ESXi de destino, con su código de tipo ARP, que es 01 para Ethernet, como prefijo. Si este intento genera un error, intenta con la anotación hexadecimal de la dirección IP del sistema ESXi de destino. Por último, intenta cargar un archivo con el nombre `default`.

Ubicación del archivo de configuración de PXE

Guarde el archivo en `var/lib/tftpboot/pxelinux.cfg/` en el servidor TFTP.

Por ejemplo, es posible guardar el archivo en el servidor TFTP en `/tftpboot/pxelinux.cfg/01-00-21-5a-ce-40-f6`. La dirección MAC del adaptador de red del host ESXi de destino es `00-21-5a-ce-40-f6`.

Realizar arranque PXE del instalador de ESXi con PXELINUX y un archivo de configuración de PXE

Puede utilizar un servidor TFTP para realizar un arranque PXE del instalador de ESXi, mediante PXELINUX y un archivo de configuración de PXE.

Consulte también [Acerca de los scripts de instalación y actualización](#) y [Acerca del archivo boot.cfg](#).

Requisitos previos

Compruebe que el entorno tenga los siguientes componentes:

- La imagen ISO del instalador de ESXi descargada desde el sitio web de VMware.
- Un servidor TFTP que admita el arranque PXE con gPXE. Consulte [Acerca del servidor TFTP, PXELINUX y gPXE](#).
- Un servidor DHCP configurado para el arranque PXE. Consulte [Configuración de DHCP de muestra](#).
- PXELINUX.
- Un servidor con una configuración de hardware compatible con la versión de ESXi. Consulte la guía de compatibilidad de VMware en <http://www.vmware.com/resources/compatibility/search.php>.
- Directivas de seguridad de red para permitir el tráfico TFTP (Puerto UDP 69).
- (Opcional) Un script de instalación, el archivo kickstart. Consulte [Acerca de los scripts de instalación y actualización](#).
- Un adaptador de red compatible con PXE en el host ESXi de destino.
- Redes IPv4. IPv6 no es compatible con el arranque PXE.

En la mayoría de los casos debe usar una VLAN nativa. Para especificar el identificador de VLAN que se va a utilizar con el arranque PXE, compruebe que su NIC admita la especificación del identificador de VLAN.

Procedimiento

- 1 Cree el directorio `/tftpboot/pxelinux.cfg` en el servidor TFTP.
- 2 En el equipo Linux, instale PXELINUX.

PXELINUX está incluido en el paquete Syslinux. Extraiga los archivos, busque el archivo `pxelinux.0` y cópielo en el directorio `/tftpboot` del servidor TFTP.

- 3 Configure el servidor DHCP para que envíe la siguiente información a cada host cliente:
 - El nombre o la dirección IP del servidor TFTP
 - El nombre del archivo de arranque inicial, `pxelinux.0`
- 4 Copie el contenido de la imagen del instalador de ESXi en el directorio `/var/lib/tftpboot` del servidor TFTP.
- 5 (opcional) En el caso de una instalación generada por script, en el archivo `boot.cfg`, agregue la opción `kernelopt` en la línea siguiente al comando del kernel, para especificar la ubicación del script de instalación.

Utilice el siguiente código como modelo, donde `xxx.xxx.xxx.xxx` es la dirección IP del servidor en el que reside el script de instalación y `esxi_ksFiles` es el directorio que contiene el archivo `ks.cfg`.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

- 6 Cree un archivo de configuración de PXE.

Este archivo define cómo se arranca el host cuando no hay ningún sistema operativo. El archivo de configuración de PXE hace referencia a los archivos de arranque. Utilice el siguiente código como modelo, donde `xxxxxxx` es el número de compilación de la imagen del instalador de ESXi.

```
DEFAULT menu.c32
MENU TITLE ESXi-6.x.x-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
    KERNEL mboot.c32
    APPEND -c location of boot.cfg
MENU LABEL ESXi-6.x.x-XXXXXX-full ^Installer
LABEL hddboot
    LOCALBOOT 0x80
MENU LABEL ^Boot from local disk
```

- 7 El nombre del archivo debe ser la dirección de Media Access Control (MAC) del equipo host de destino: `01-mac_address_of_target_ESXi_host`.
Por ejemplo, `01-23-45-67-89-0a-bc`.
- 8 Guarde el archivo de configuración de PXE en la ruta `/tftpboot/pxelinux.cfg` en el servidor TFTP.
- 9 Arranque el equipo con el adaptador de red.

Arranque PXE del instalador de ESXi a través de PXELINUX y un archivo de configuración de isolinux.cfg

Puede arrancar con PXE el instalador de ESXi a través de PXELINUX y puede utilizar el archivo isolinux.cfg como el archivo de configuración de PXE.

Consulte también [Acerca de los scripts de instalación y actualización](#) y [Acerca del archivo boot.cfg](#)

Requisitos previos

Compruebe que el entorno tenga los siguientes componentes:

- La imagen ISO del instalador de ESXi descargada desde el sitio web de VMware.
- Servidor TFTP que admita el arranque PXE con PXELINUX. Consulte [Acerca del servidor TFTP, PXELINUX y gPXE](#).
- Un servidor DHCP configurado para el arranque PXE. Consulte [Configuración de DHCP de muestra](#).
- PXELINUX.
- Un servidor con una configuración de hardware compatible con la versión de ESXi. Consulte la Guía de compatibilidad de VMware <http://www.vmware.com/resources/compatibility/search.php>.
- Directivas de seguridad de red para permitir el tráfico TFTP (Puerto UDP 69).
- (Opcional) Un script de instalación, el archivo kickstart. Consulte [Acerca de los scripts de instalación y actualización](#).
- Un adaptador de red compatible con PXE en el host ESXi de destino.
- Redes IPv4. IPv6 no es compatible con el arranque PXE.

En la mayoría de los casos debe usar una VLAN nativa. Para especificar el identificador de VLAN que se va a utilizar con el arranque PXE, compruebe que su NIC admita la especificación del identificador de VLAN.

Procedimiento

- 1 Cree el directorio `/tftpboot/pxelinux.cfg` en el servidor TFTP.
- 2 En el equipo Linux, instale PXELINUX.

PXELINUX está incluido en el paquete Syslinux. Extraiga los archivos, busque el archivo `pxelinux.0` y cópielo en el directorio `/tftpboot` del servidor TFTP.

- 3 Configure el servidor DHCP.

El servidor DHCP envía la siguiente información a los hosts de su cliente:

- El nombre o la dirección IP del servidor TFTP
- El nombre del archivo de arranque inicial, `pxelinux.0`

- 4 Copie el contenido de la imagen del instalador de ESXi en el directorio `/var/lib/tftpboot` del servidor TFTP.
- 5 (opcional) Para una instalación generada por script, en el archivo `boot.cfg`, agregue la opción `kernelopt` en la línea después del comando `kernel` para especificar la ubicación del script de instalación.

En el siguiente ejemplo, `XXX.XXX.XXX.XXX` es la dirección IP del servidor en el que reside el script de instalación.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

- 6 Copie el archivo `isolinux.cfg` desde la imagen ISO del instalador de ESXi al directorio `/tftpboot/pxelinux.cfg`.

El archivo `isolinux.cfg` contiene el siguiente código, donde `XXXXXX` es el número de versión de la imagen del instalador de ESXi:

```
DEFAULT menu.c32
MENU TITLE ESXi-6.x.x-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
    KERNEL mboot.c32
    APPEND -c location of boot.cfg
MENU LABEL ESXi-6.x.x-XXXXXX-full ^Installer
LABEL hddboot
    LOCALBOOT 0x80
MENU LABEL ^Boot from local disk
```

- 7 Cambie el nombre del archivo `isolinux.cfg` con la dirección MAC del equipo host de destino: `01-mac_address_of_target_ESXi_host`. Por ejemplo, `01-23-45-67-89-0a-bc`
- 8 Arranque el equipo con el adaptador de red.

Arranque PXE del instalador de ESXi mediante gPXE

Puede realizar un arranque PXE del instalador de ESXi mediante gPXE.

Consulte también [Acerca de los scripts de instalación y actualización](#) y [Acerca del archivo boot.cfg](#)

Requisitos previos

Compruebe que el entorno tenga los siguientes componentes:

- La imagen ISO del instalador de ESXi descargada desde el sitio web de VMware
- Un servidor web HTTP al que puedan acceder los hosts ESXi de destino
- Un servidor DHCP configurado para el arranque PXE: `/etc/dhcpd.conf` se configura para hosts de cliente con un servidor TFTP y el archivo de arranque inicial establecido como `gpxelinux.0/undionly.kpxe`. Consulte [Configuración de DHCP de muestra](#).

- Un servidor con una configuración de hardware compatible con la versión de ESXi. Consulte la guía de compatibilidad de hardware en <http://www.vmware.com/resources/compatibility/search.php>.
- gPXELINUX
- (Opcional) Un script de instalación de ESXi. Consulte [Acerca de los scripts de instalación y actualización](#).

En la mayoría de los casos debe usar una VLAN nativa. Si desea especificar el identificador de la VLAN que se va a utilizar con el arranque PXE, compruebe que su NIC admita la especificación de identificador de la VLAN.

Procedimiento

- 1 Copie el contenido de la imagen ISO del instalador de ESXi en el directorio `/var/www/html` del servidor HTTP.
- 2 Modifique el archivo `boot.cfg` con la información para el servidor HTTP.

Utilice el siguiente código como modelo, donde `XXX.XXX.XXX.XXX` es la dirección IP del servidor HTTP. La línea `kernelopt` es opcional. Incluya esa opción para especificar la ubicación del script de instalación en el caso de una instalación por script.

```
title=Loading ESX installer
kernel=http://XXX.XXX.XXX.XXX/tboot.b00
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
modules=http://XXX.XXX.XXX.XXX/b.b00 --- http://XXX.XXX.XXX.XXX/useropts.gz --- http://
XXX.XXX.XXX.XXX/k.b00 --- http://XXX.XXX.XXX.XXX/a.b00 --- http://XXX.XXX.XXX.XXX/s.v00
--- http://XXX.XXX.XXX.XXX/weaselin.t00 --- http://XXX.XXX.XXX.XXX/tools.t00 --- http://
XXX.XXX.XXX.XXX/imgdb.tgz --- http://XXX.XXX.XXX.XXX/imgpayld.tgz
```

- 3 Realice un arranque gPXE del host y presione Ctrl+B para acceder al menú GPT.
- 4 Escriba los siguientes comandos para arrancar con el instalador de ESXi, donde `XXX.XXX.XXX.XXX` es la dirección IP del servidor HTTP.

```
dhcp net0 ( if dhcp is not set)
kernel -n mboot.c32 http://XXX.XXX.XXX.XXX/mboot.c32
imgargs mboot.c32 -c http://XXX.XXX.XXX.XXX/boot.cfg
boot mboot.c32
```

Instalar y arrancar ESXi con FCoE de software

Puede instalar y arrancar ESXi desde un LUN FCoE utilizando los adaptadores FCoE de software VMware y los adaptadores de red con capacidades de descarga FCoE. Su host no requiere un HBA FCoE dedicado.

Consulte la documentación de *Almacenamiento de vSphere* para obtener información sobre la instalación y el arranque de ESXi con FCoE para software.

Usar aplicaciones de administración remota

Las aplicaciones de administración remota permiten instalar ESXi en servidores que se encuentran en ubicaciones remotas.

Las aplicaciones de administración remota compatibles para la instalación incluyen HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM management module (MM) y Remote Supervisor Adapter II (RSA II). Para obtener una lista de modelos de servidores compatibles y versiones de firmware de administración remota, consulte [Modelos de servidores de administración remota compatibles y versiones de firmware](#). Para obtener soporte técnico para las aplicaciones de administración remota, póngase en contacto con el proveedor.

Puede usar aplicaciones de administración remota para realizar instalaciones interactivas y por script de ESXi de forma remota.

Si utiliza aplicaciones de administración remota para instalar ESXi, el CD virtual podría encontrarse con daños en sistemas o redes que operan a capacidad máxima. Si se produce un error en una instalación remota de una imagen ISO, complete la instalación desde el CD físico.

Información obligatoria para instalar ESXi

En una instalación interactiva, el sistema le solicita la información del sistema necesaria. En una instalación por script, debe suministrar esta información en el script de instalación.

Para su uso en el futuro, anote los valores que utilice durante la instalación. Estas anotaciones son útiles si debe reinstalar ESXi y volver a entrar los valores que eligió inicialmente.

Tabla 3-1. Información obligatoria para instalar ESXi

Información	Obligatorio u opcional	Predeterminado	Comentarios
Distribución del teclado	Obligatorio	Inglés (EE. UU.)	
identificador de VLAN	Opcional	Ninguna	Rango: de 0 a 4094
Dirección IP	Opcional	DHCP	Puede permitir que DHCP configure la red durante la instalación. Después de la instalación, puede cambiar la configuración de red.
Máscara de subred	Opcional	Se calcula en base a la dirección IP	
Puerta de enlace	Opcional	En función de la dirección IP y la máscara de subred configuradas	
DNS principal	Opcional	En función de la dirección IP y la máscara de subred configuradas	
DNS secundario	Opcional	Ninguna	

Tabla 3-1. Información obligatoria para instalar ESXi (continuación)

Información	Obligatorio u opcional	Predeterminado	Comentarios
Nombre de host	Obligatorio para la configuración de IP estática	Ninguna	vSphere Web Client puede utilizar el nombre de host o la dirección IP para acceder al host ESXi.
Ubicación de instalación	Obligatorio	Ninguna	Debe tener al menos 5 GB si va a instalar los componentes en un único disco.
Migrar la configuración de ESXi existente. Conservar el almacén de datos de VMFS existente.	Obligatorio si va a instalar ESXi en una unidad con una instalación de ESXi existente.	Ninguna	Si ya existe una instalación de ESXi 5.x, el instalador de ESXi permite elegir entre conservar o sobrescribir el almacén de datos de VMFS durante la instalación
Contraseña raíz	Obligatorio	Ninguna	La contraseña raíz debe contener entre 8 y 40 caracteres. Para obtener información sobre las contraseñas, consulte la documentación sobre la <i>seguridad de vSphere</i> .

Descarga del instalador de ESXi

Descargue el instalador de ESXi.

Requisitos previos

Cree una cuenta de Customer Connect en <https://my.vmware.com/web/vmware/>.

Procedimiento

- 1 Descargue el instalador de ESXi desde el sitio web de VMware en <https://my.vmware.com/web/vmware/downloads>.

ESXi aparece en la sección Centro de datos e infraestructura de nube.

- 2 Confirme que el valor de md5sum sea correcto.

Consulte el tema del sitio web de VMware Uso de sumas de comprobación de MD5 en <http://www.vmware.com/download/md5.html>.

Instalación de ESXi

4

Puede instalar ESXi de forma interactiva, con una instalación generada por script o con vSphere Auto Deploy.

Este capítulo incluye los siguientes temas:

- [Instalar ESXi de forma interactiva](#)
- [Instalar o actualizar hosts mediante un script](#)
- [Instalar ESXi con vSphere Auto Deploy](#)
- [Usar vSphere ESXi Image Builder](#)

Instalar ESXi de forma interactiva

Utilice la opción de instalación interactiva para implementaciones pequeñas con menos de cinco hosts.

En una instalación interactiva típica, debe arrancar el instalador de ESXi y responder las solicitudes para instalar ESXi en el disco host local. El instalador vuelve a formatear y particiona el disco de destino y, a continuación, instala la imagen de arranque de ESXi. Si no instaló ESXi en el disco de destino anteriormente, se sobrescribirán todos los datos ubicados en la unidad. Esto incluye las particiones de proveedores de hardware, las particiones de sistemas operativos y los datos asociados.

Nota Para asegurarse de no perder datos, mígrelos a otro equipo antes de instalar ESXi.

Si va a instalar ESXi en un disco que contiene una instalación anterior de ESXi o ESX, o bien un almacén de datos de VMFS, el instalador le brindará opciones para actualización. Consulte la documentación sobre la *actualización de vSphere*.

Instalar ESXi de forma interactiva

Utilice el CD/DVD o una unidad flash USB de ESXi para instalar el software ESXi en un disco duro SAS, SATA o SCSI, o bien en una unidad USB.

Requisitos previos

- Debe tener el archivo ISO del instalador de ESXi en una de las siguientes ubicaciones:
 - Un CD o DVD. Si no posee el CD/DVD de instalación, puede crear uno. Consulte [Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi](#)
 - Una unidad flash USB. Consulte [Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi](#).

Nota También puede realizar un arranque PXE del instalador de ESXi para iniciar una instalación interactiva o por script. Consulte [Arranque PXE del instalador de ESXi](#).

- Compruebe que el reloj de hardware del servidor esté configurado como UTC. Esta configuración se encuentra en el BIOS del sistema.
- Compruebe que haya un teclado y un monitor conectados al equipo en el que se va a instalar el software ESXi. Como alternativa, utilice una aplicación de administración remota. Consulte [Usar aplicaciones de administración remota](#).
- Considere la posibilidad de desconectar el almacenamiento de red. Esta acción disminuye el tiempo que tarda el instalador en buscar unidades de disco disponibles. Tenga en cuenta que cuando desconecta el almacenamiento de red, los archivos de los discos desconectados no estarán disponibles en el momento de la instalación.

No desconecte un LUN que contenga una instalación de ESX o ESXi. No desconecte un almacén de datos de VMFS que contenga una consola de servicios de una instalación de ESX existente. Estas acciones podrían afectar el resultado de la instalación.

- Recopile la información que necesita el asistente de instalación de ESXi. Consulte [Información obligatoria para instalar ESXi](#).
- Compruebe que ESXi Embedded no esté presente en el equipo host. ESXi Installable y ESXi Embedded no pueden estar en el mismo host.

Procedimiento

- 1 Inserte el CD/DVD del instalador de ESXi en la unidad de CD/DVD-ROM, o bien conecte la unidad flash USB del instalador, y reinicie el equipo.
- 2 Configure el BIOS para que arranque desde el dispositivo de CD-ROM o la unidad flash USB.

Consulte la documentación del proveedor de hardware para obtener información sobre el cambio del orden de arranque.

- 3 En la página Seleccionar un disco, seleccione la unidad en la que va a instalar ESXi y presione Intro.

Presione F1 para obtener más información sobre el disco seleccionado.

Nota No se base en el orden de discos de la lista para seleccionar un disco. El BIOS determina el orden de discos y podría estar desordenado. Esto puede ocurrir en sistemas en los que se agregan y eliminan unidades continuamente.

Si selecciona un disco que contiene datos, aparece la página Confirmar selección de disco.

Si va a realizar la instalación en un disco que tiene una instalación anterior de ESXi o ESX, o bien en un almacén de datos de VMFS, el instalador proporciona varias alternativas.

Importante Si va a actualizar o migrar una instalación de ESX/ESXi existente, consulte la documentación sobre *Actualización de vSphere*. Las instrucciones de la documentación sobre *Instalación y configuración de vSphere* son para una instalación nueva de ESXi nueva.

Si selecciona un disco del grupo de discos de Virtual SAN, la instalación que se obtenga dependerá del tipo de disco y del tamaño del grupo:

- Si selecciona una SSD, esta y todas las HDD subyacentes del mismo grupo de discos se borrarán.
- Si selecciona una HDD, y el tamaño del grupo de discos es mayor que 2, solo se borrarán las HDD seleccionadas.
- Si selecciona una HDD y el tamaño del grupo de discos es 2 o menos, se borrarán la SSD y las HDD seleccionadas.

Para obtener más información acerca de la administración de grupos de discos de Virtual SAN, consulte la documentación de *Almacenamiento de vSphere*.

- 4 Seleccione el tipo de teclado para el host.

Después de la instalación, puede cambiar el tipo de teclado en la consola directa.

- 5 Escriba la contraseña raíz para el host.

Después de la instalación, puede cambiar la contraseña en la consola directa.

- 6 Presione Intro para iniciar la instalación.

- 7 Una vez que esta finaliza, quite el CD, el DVD o la unidad flash USB de instalación.

- 8 Presione Intro para reiniciar el host.

Cuando realiza una nueva instalación o decide sobrescribir un almacén de datos de VMFS existente, durante la operación de reinicio, se crean particiones VFAT desde cero y VMFS en el disco host.

- 9 Configure el dispositivo de primer arranque como la unidad en la que instaló ESXi en [Paso 3](#).

Para obtener más información sobre cómo cambiar el orden de arranque, consulte la documentación del proveedor de hardware.

Nota Es posible que se necesiten pasos adicionales para configurar el dispositivo de arranque en sistemas UEFI. Consulte [El host no arranca después de instalar ESXi en modo UEFI](#)

Resultados

Una vez finalizada la instalación, puede migrar los datos de VMFS existentes al host ESXi.

Puede arrancar un único equipo desde cada imagen de ESXi. No se permite arrancar varios dispositivos desde una única imagen compartida de ESXi.

Pasos siguientes

Establezca la configuración básica de administración y red para ESXi. Consulte [Capítulo 6 Después de instalar y configurar ESXi](#).

Instalar ESXi en un disco iSCSI de software

Al instalar ESXi en un disco iSCSI de software, debe configurar el nombre calificado iSCSI (IQN) de destino.

Durante el arranque del sistema, se realiza una prueba automática de encendido (POST) y se comienzan a iniciar los adaptadores en el orden especificado en el BIOS del sistema. Cuando el orden de arranque llega al adaptador de la tabla de firmware de arranque de iSCSI (iBFT), el adaptador intenta conectarse al destino, pero no arranca desde el destino. Consulte los requisitos previos.

Si la conexión con el destino de iSCSI se establece correctamente, el firmware de arranque de iSCSI guarda la configuración de arranque de iSCSI en iBFT. El próximo adaptador en arrancar debe ser el medio de instalación de ESXi, que puede ser una imagen ISO montada o un CD-ROM físico.

Requisitos previos

- Compruebe que el IQN de destino esté establecido en la configuración de parámetros de destino del BIOS de iBFT. Esta configuración se encuentra en la opción ROM de la tarjeta de interfaz de red (NIC) que se debe usar para el LUN de iSCSI. Consulte la documentación del proveedor de su sistema.
- Deshabilite la opción del adaptador de iBFT para arrancar en el destino de iSCSI. Esta acción es necesaria para garantizar el arranque del instalador de ESXi, en lugar del destino de iSCSI. Al iniciar el sistema, siga el aviso para iniciar sesión en el adaptador de iBFT y deshabilite la opción para arrancar en el destino de iSCSI. Consulte la documentación del proveedor de su sistema y su adaptador de iBFT. Después de finalizar la instalación de ESXi, puede volver a habilitar la opción para arrancar desde el LUN en el que instaló ESXi.

Procedimiento

- 1 Inicie la instalación interactiva desde la imagen ISO montada o el CD/DVD de instalación de ESXi.
- 2 En la pantalla Seleccionar un disco, seleccione el destino de iSCSI que especificó en la configuración de parámetros de destino del BIOS de iBFT.

Si el destino no aparece en este menú, asegúrese de que la configuración de TCP/IP e IQN iSCSI del iniciador sea la correcta. Compruebe la lista de control de acceso (ACL) de la red y confirme que el adaptador cuenta con los permisos necesarios para acceder al destino.
- 3 Siga las indicaciones para completar la instalación.
- 4 Reinicie el host.
- 5 En la configuración del BIOS del host, especifique la configuración del BIOS para el adaptador de iBFT y cambie el parámetro del adaptador para que arranque desde el destino de iSCSI.

Consulte la documentación del proveedor de su sistema.

Pasos siguientes

En el adaptador de iBFT, habilite nuevamente la opción para arrancar en el destino de iSCSI, de modo que el sistema arranque desde el LUN en el que instaló ESXi.

Instalar o actualizar hosts mediante un script

Puede implementar hosts de ESXi rápidamente mediante instalaciones o actualizaciones desatendidas generadas por script. Las instalaciones o las actualizaciones generadas por script proporcionan un mecanismo eficaz para la implementación de varios hosts.

El script de instalación o actualización contiene la configuración de instalación para ESXi. Puede aplicar el script a todos los que desee que tengan una configuración similar.

Para una instalación o una actualización generada por script, debe usar los comandos compatibles para crear un script. Puede editar el script con la finalidad de cambiar ajustes de configuración que sean exclusivos para cada host.

El script de instalación o actualización puede residir en una de las ubicaciones siguientes:

- Servidor FTP
- Servidor HTTP/HTTPS
- servidor NFS
- Unidad flash USB
- Unidad de CD-ROM

Enfoques para la instalación por script

Puede instalar ESXi en varios equipos con un único script para todos o un script separado para cada uno.

Por ejemplo, debido a que los nombres de disco varían de un equipo a otro, una de las opciones de configuración que se recomienda seleccionar en un script es el disco en el que se va a instalar ESXi.

Tabla 4-1. Opciones de una instalación por script

Opción	Acción
Instalar siempre en el primer disco de varios equipos.	Crear un solo script.
Instalar ESXi en un disco distinto para cada equipo.	Crear varios scripts.

Para obtener información sobre los comandos necesarios para especificar el disco en el que se va a realizar la instalación, consulte [Comandos de scripts de instalación y actualización](#).

Introducir las opciones de arranque para iniciar un script de instalación o actualización

Puede iniciar un script de instalación o actualización introduciendo las opciones de arranque en la línea de comandos de arranque del instalador de ESXi.

En el momento del arranque, es posible que necesite especificar opciones para acceder al archivo de inicio. Puede introducir opciones de arranque presionando Shift+O en el gestor de arranque. Para una instalación de arranque PXE, puede pasar opciones a través de la línea `kernelopts` del archivo `boot.cfg`. Consulte [Acerca del archivo boot.cfg](#) y [Arranque PXE del instalador de ESXi](#).

Para especificar la ubicación del script de instalación, defina la opción `ks=filepath`, donde *filepath* indica la ubicación del archivo Kickstart. De lo contrario, no se podrá iniciar una instalación o actualización generadas por script. Si se omite `ks=filepath`, se ejecuta el instalador de texto.

Las opciones de arranque compatibles se detallan en [Opciones de arranque](#).

Procedimiento

- 1 Inicie el host.

- 2 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



- 3 En el símbolo del sistema `runweasel`, introduzca ***ks=location of installation script plus boot command-line options.***

Ejemplo: Opción de arranque

Introduzca las siguientes opciones de arranque:

```
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000
netmask=255.255.255.0 gateway=00.00.00.000
```

Opciones de arranque

Cuando realice una instalación por script, es posible que necesite especificar opciones en el arranque para acceder al archivo de inicio.

Opciones de arranque compatibles

Tabla 4-2. Opciones de arranque para la instalación de ESXi

Opción de arranque	Descripción
<code>BOOTIF=hwtype-MAC address</code>	Similar a la opción <code>netdevice</code> , excepto en el formato PXELINUX, tal como se describe en la opción <code>IPAPPEND</code> en SYSLINUX en el sitio syslinux.zytor.com .
<code>gateway=ip address</code>	Permite establecer esta puerta de enlace de red como la puerta de enlace predeterminada para utilizarla en la descarga de scripts de instalación y medios de instalación.
<code>ip=ip address</code>	Permite configurar una dirección IP estática para utilizarla en la descarga de scripts de instalación y medios de instalación. Nota: también se admite el formato PXELINUX para esta opción. Consulte la opción <code>IPAPPEND</code> en SYSLINUX en el sitio syslinux.zytor.com .

Tabla 4-2. Opciones de arranque para la instalación de ESXi (continuación)

Opción de arranque	Descripción
<code>ks=cdrom:/path</code>	<p>Permite realizar una instalación por script con el script en <i>path</i>, que se encuentra en el CD de la unidad de CD-ROM. Cada CDROM se monta y se comprueba hasta que se encuentre el archivo que coincida con la ruta de acceso.</p> <p>Importante Si creó una imagen ISO de instalador con un script de instalación o actualización personalizado, debe utilizar caracteres en mayúscula para proporcionar la ruta de acceso del script, por ejemplo, <code>ks=cdrom:/KS_CUST.CFG</code>.</p>
<code>ks=file://path</code>	Realiza una instalación por script con el script en <i>path</i> .
<code>ks=protocol://serverpath</code>	Realiza una instalación por script con un script ubicado en la red en la dirección URL determinada. <i>protocol</i> puede ser <code>http</code> , <code>https</code> , <code>ftp</code> o <code>nfs</code> . Un ejemplo de uso del protocolo <code>nfs</code> es <code>ks=nfs://host/porturl-path</code> . El formato de la URL de NFS se especifica en RFC 2224.
<code>ks=usb</code>	Realiza una instalación por script mediante el acceso al script desde la unidad USB conectada. Busca un archivo con el nombre <code>ks.cfg</code> . El archivo debe estar ubicado en el directorio raíz de la unidad. Si se conectan varias unidades flash USB, se realizará la búsqueda hasta que se encuentre el archivo <code>ks.cfg</code> . Solo se admiten los sistemas de archivos FAT16 y FAT32.
<code>ks=usb:/path</code>	Realiza una instalación por script con un archivo de script en la ruta especificada, que se encuentra en USB.
<code>ksdevice=device</code>	Intenta utilizar un adaptador de red <i>device</i> cuando se realiza la búsqueda de un script de instalación y un medio de instalación. Se especifica como una dirección MAC, por ejemplo, <code>00:50:56:C0:00:01</code> . Esta ubicación también puede ser un nombre <code>vmnicNN</code> . Si no se especifica y los archivos deben obtenerse a través de la red, el instalador utiliza de forma predeterminada el primer adaptador de red detectado que esté conectado.
<code>nameserver=ip address</code>	Especifica un servidor de nombres de dominio para utilizarlo en la descarga de scripts de instalación y medios de instalación.
<code>netdevice=device</code>	Intenta utilizar un adaptador de red <i>device</i> cuando se realiza la búsqueda de un script de instalación y un medio de instalación. Se especifica como una dirección MAC, por ejemplo, <code>00:50:56:C0:00:01</code> . Esta ubicación también puede ser un nombre <code>vmnicNN</code> . Si no se especifica y los archivos deben obtenerse a través de la red, el instalador utiliza de forma predeterminada el primer adaptador de red detectado que esté conectado.

Tabla 4-2. Opciones de arranque para la instalación de ESXi (continuación)

Opción de arranque	Descripción
<code>netmask=subnet mask</code>	Especifica una máscara de subred para la interfaz de red que descarga los scripts de instalación y los medios de instalación.
<code>vlanid=vlanid</code>	Configure la tarjeta de red para que se encuentre en la VLAN especificada.

Acerca de los scripts de instalación y actualización

El script de instalación o actualización es un archivo de texto que contiene los comandos compatibles (por ejemplo, `ks.cfg`).

La sección de comandos del script contiene las opciones de instalación de ESXi. Esta sección es obligatoria y debe aparecer primero en el script.

Acerca del script de instalación predeterminado `ks.cfg`

El instalador de ESXi incluye un script de instalación predeterminado que realiza una instalación estándar en el primer disco detectado.

El script de instalación `ks.cfg` predeterminado está ubicado en el disco RAM inicial en `/etc/vmware/weasel/ks.cfg`. Puede especificar la ubicación del archivo `ks.cfg` predeterminado con la opción de arranque `ks=file:///etc/vmware/weasel/ks.cfg`. Consulte [Introducir las opciones de arranque para iniciar un script de instalación o actualización](#).

Cuando instale ESXi con el script `ks.cfg`, la contraseña raíz predeterminada será `mypassword`.

No puede modificar el script predeterminado en los medios de instalación. Después de la instalación, puede utilizar vSphere Web Client para iniciar sesión en vCenter Server que administra el host ESXi y modificar la configuración predeterminada.

El script predeterminado contiene los siguientes comandos:

```
#
# Sample scripted installation file
#

# Accept the VMware End User License Agreement
vmaccepteula

# Set the root password for the DCUI and Tech Support Mode
rootpw mypassword

# Install on the first local disk available on machine
install --firstdisk --overwritevmfs

# Set the network to DHCP on the first network adapter
network --bootproto=dhcp --device=vmnic0

# A sample post-install script
```

```
%post --interpreter=python --ignorefailure=true
import time
stampFile = open('/finished.stamp', mode='w')
stampFile.write( time.asctime() )
```

Ubicaciones admitidas para scripts de instalación o actualización

En instalaciones y actualizaciones generadas por script, el instalador de ESXi puede acceder al script de la instalación o actualización, que también se conoce como el archivo inicial, desde varias ubicaciones.

Se admiten las siguientes ubicaciones para el script de instalación o actualización:

- CD/DVD. Consulte [Crear una imagen ISO de instalador con un script de instalación o actualización personalizado](#).
- Unidad flash USB. Consulte [Crear una unidad flash USB para almacenar el script de instalación o actualización de ESXi](#).
- Una ubicación local de red a la que se puede acceder mediante los siguientes protocolos: NFS, HTTP, HTTPS, FTP

Ruta de acceso del script de instalación o actualización

Puede especificar la ruta de acceso de un script de instalación o actualización.

`ks=http://XXX.XXX.XXX.XXX/kickstart/KS.CFG` es la ruta de acceso del script de instalación de ESXi, donde `XXX.XXX.XXX.XXX` es la dirección IP del equipo donde reside el script. Consulte [Acerca de los scripts de instalación y actualización](#).

Para iniciar un script de instalación desde una instalación interactiva, escriba la opción `ks=` de forma manual. Consulte [Introducir las opciones de arranque para iniciar un script de instalación o actualización](#).

Comandos de scripts de instalación y actualización

Para modificar el script predeterminado de instalación o actualización, o para crear su propio script, use comandos compatibles. Use comandos compatibles en el script de instalación, que se especifica mediante un comando de arranque cuando se arranca el instalador.

Para determinar en qué disco instalar o actualizar ESXi, el script de instalación requiere uno de los comandos siguientes: `install`, `upgrade` o `installorupgrade`. El comando `install` crea las particiones predeterminadas, que incluyen un almacén de datos de VMFS que ocupa todo el espacio disponible después de que se crean las demás particiones.

accepteula o vmaccepteula (obligatorio)

Acepta el contrato de licencia de ESXi.

clearpart (opcional)

Borra las particiones existentes del disco. Requiere que se especifique el comando `install`. Edite cuidadosamente el comando `clearpart` en sus scripts existentes.

<code>--drives=</code>	Quita las particiones en las unidades especificadas.
<code>--alldrives</code>	Ignora el requisito de <code>--drives=</code> y permite borrar las particiones de cada unidad.
<code>--ignoredrives=</code>	Elimina las particiones en todas las unidades, excepto las especificadas. Es obligatorio a menos que se especifiquen las marcas <code>--drives=0 --alldrives</code> .
<code>--overwritevmfs</code>	Permite sobrescribir las particiones de VMFS en las unidades especificadas. De forma predeterminada, no se permite sobrescribir las particiones de VMFS.
<code>--firstdisk=</code> <i>disk-type1</i> <i>[disk-type2,...]</i>	<p>Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:</p> <ol style="list-style-type: none"> 1 Almacenamiento conectado a nivel local (<i>local</i>) 2 Almacenamiento en red (<i>remote</i>) 3 Discos USB (<i>usb</i>) <p>Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye <i>esx</i> para el primer disco en el que se haya instalado ESXi, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es <code>--firstdisk=ST3120814A,mptsas,local</code>.</p>

dryrun (opcional)

Analiza y comprueba el script de instalación. No ejecuta la instalación.

instalar

Especifica que se trata de una instalación nueva. Reemplaza el comando `autopart` obsoleto que se utilizaba para las instalaciones generadas por script de ESXi 4.1. Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

`--disk=` or `--drive=`

Especifica el disco que se particionará. En el comando `--disk=`*diskname*, el valor *diskname* puede tener cualquiera de los formatos que se muestran en los ejemplos siguientes:

- Ruta de acceso: `--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`
- Nombre de MPX: `--disk=mpx.vmhba1:C0:T0:L0`
- Nombre de VML: `--disk=vml.000000034211234`
- UID de vmkLUN: `--disk=vmkLUN_UID`

Para conocer los formatos admitidos de nombre de disco, consulte [Nombre de los dispositivos de disco](#).

`--firstdisk=`

disk-type1,

[*disk-type2*,...]

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

- 1 Almacenamiento conectado a nivel local (`local`)
- 2 Almacenamiento en red (`remote`)
- 3 Discos USB (`usb`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`.

`--ignoressd`

Excluye los discos de estado sólido de los que satisfacen las condiciones para el particionamiento. Esta opción puede utilizarse con el comando `install` y la opción `--firstdisk`. Esta opción tiene prioridad sobre la opción `--firstdisk`. Esta opción no es válida con las opciones `--drive` o `--disk` ni con los comandos `upgrade` o `installorupgrade`. Consulte la documentación de *Almacenamiento*

de *vSphere* para obtener más información sobre la prevención del formateo de SSD durante la creación automática de particiones.

--overwritevsan

Debe usar la opción `--overwritevsan` al instalar ESXi en un disco, ya sea SSD o HDD (magnética), que forme parte de un grupo de discos de Virtual SAN. Si usa esta opción y no hay ninguna partición de Virtual SAN en el disco seleccionado, se produce un error en la instalación. Al instalar ESXi en un disco que forma parte de un grupo de discos de Virtual SAN, el resultado depende del disco que se selecciona:

- Si selecciona una SSD, esta y todas las HDD subyacentes del mismo grupo de discos se borrarán.
- Si selecciona una HDD, y el tamaño del grupo de discos es mayor que 2, solo se borrarán las HDD seleccionadas.
- Si selecciona una HDD y el tamaño del grupo de discos es 2 o menos, se borrarán la SSD y las HDD seleccionadas.

Para obtener más información acerca de la administración de grupos de discos de Virtual SAN, consulte la documentación de *Almacenamiento de vSphere*.

--overwritevmfs

Es obligatorio para sobrescribir un almacén de datos existente de VMFS en el disco antes de la instalación.

--preservevmfs

Conserva el almacén de datos existente de VMFS en el disco durante la instalación.

--novmfsondisk

Impide que se cree una partición de VMFS en este disco. Debe utilizarse con `--overwritevmfs` si ya existe una partición de VMFS en el disco.

installorupgrade

Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

--disk= or --drive=

Especifica el disco que se particionará. En el comando `--disk=` *diskname*, el valor *diskname* puede tener cualquiera de los formatos que se muestran en los ejemplos siguientes:

- Ruta de acceso: `--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`
- Nombre de MPX: `--disk=mpx.vmhba1:C0:T0:L0`
- Nombre de VML: `--disk=vm1.000000034211234`
- UID de vmkLUN: `--disk=vmkLUN_UID`

Para conocer los formatos admitidos de nombre de disco, consulte [Nombre de los dispositivos de disco](#).

`--firstdisk=`
`disk-type1,`
`[disk-type2,...]`

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

- 1 Almacenamiento conectado a nivel local (`local`)
- 2 Almacenamiento en red (`remote`)
- 3 Discos USB (`usb`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`.

`--overwritevsan`

Debe usar la opción `--overwritevsan` al instalar ESXi en un disco, ya sea SSD o HDD (magnética), que forme parte de un grupo de discos de Virtual SAN. Si usa esta opción y no hay ninguna partición de Virtual SAN en el disco seleccionado, se produce un error en la instalación. Al instalar ESXi en un disco que forma parte de un grupo de discos de Virtual SAN, el resultado depende del disco que se selecciona:

- Si selecciona una SSD, esta y todas las HDD subyacentes del mismo grupo de discos se borrarán.
- Si selecciona una HDD, y el tamaño del grupo de discos es mayor que 2, solo se borrarán las HDD seleccionadas.
- Si selecciona una HDD y el tamaño del grupo de discos es 2 o menos, se borrarán la SSD y las HDD seleccionadas.

Para obtener más información acerca de la administración de grupos de discos de Virtual SAN, consulte la documentación de *Almacenamiento de vSphere*.

`--overwritevmfs`

Instale ESXi si en el disco existe una partición de VMFS, pero no una instalación de ESX ni ESXi. A menos que esta opción esté presente, se producirá un error en el instalador si en el disco existe una partición de VMFS, pero no una instalación de ESX ni ESXi.

keyboard (opcional)

Configura el tipo de teclado para el sistema.

keyboardType

Especifica la distribución del teclado para el tipo de teclado seleccionado. El parámetro *keyboardType* debe ser de uno de los tipos siguientes.

- Belgian
- Brazilian
- Croatian
- Czechoslovakian
- Danish
- Predeterminado
- Estonian
- Finnish
- French
- German
- Greek
- Icelandic
- Italian
- Japanese
- Latin American
- Norwegian
- Polish
- Portuguese
- Russian
- Slovenian
- Spanish
- Swedish
- Swiss French
- Swiss German
- Turkish
- US Dvorak
- Ukrainian

■ United Kingdom

serialnum o vmserialnum (opcional)

Obsoletos en ESXi 5.0.x. Compatibles con ESXi 5.1 y versiones superiores. Configura las licencias. Si no se incluye, ESXi se instala en modo de evaluación.

--esx=<license-key> Especifica la clave de licencia de vSphere que se utilizará. El formato corresponde a cinco grupos de cinco caracteres (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX).

network (opcional)

Especifica una dirección de red para el sistema.

--bootproto=[dhcp|static] Especifica si la configuración de red se debe obtener desde DHCP o si se debe configurar de forma manual.

--device= Especifica la dirección MAC de la tarjeta de red o el nombre del dispositivo, con el formato `vmnicNN` (por ejemplo, `vmnic0`). Esta opción hace referencia al dispositivo del vínculo superior para el conmutador virtual.

--ip= Establece una dirección IP para el equipo que se va a instalar, con el formato `xxx.xxx.xxx.xxx`. Es obligatorio cuando se usa la opción `--bootproto=static` y se ignora en los demás casos.

--gateway= Designa la puerta de enlace predeterminada como una dirección IP, con el formato `xxx.xxx.xxx.xxx`. Se usa con la opción `--bootproto=static`.

--nameserver= Designa el servidor de nombre principal como una dirección IP. Se usa con la opción `--bootproto=static`. Omita esta opción si no va a usar DNS.

La opción `--nameserver` puede admitir dos direcciones IP. Por ejemplo: `--nameserver="10.126.87.104[,10.126.87.120]"`

--netmask= Especifica la máscara de subred para el sistema instalado, con el formato `255.xxx.xxx.xxx`. Se usa con la opción `--bootproto=static`.

--hostname= Especifica el nombre de host para el sistema instalado.

<code>--vlanid= <i>vlanid</i></code>	Especifica la VLAN en la que reside el sistema. Se usa con las opciones <code>--bootproto=dhcp</code> o <code>--bootproto=static</code> . Se establece como un valor entero entre 1 y 4096.
<code>--addvmportgroup=(0 1)</code>	Especifica si se debe agregar el grupo de puertos de la red de máquinas virtuales (VM), que utilizan las máquinas virtuales. El valor predeterminado es 1.

paranoid (opcional)

Hace que los mensajes de advertencia interrumpan la instalación. Si omite este comando, los mensajes de advertencia se registran.

part o partition (opcional)

Crea un almacén de datos de VMFS en el sistema. Solo se puede crear un almacén de datos por cada disco. No se puede usar en el mismo disco que el comando `install`. Solo se puede especificar una partición por cada disco y solo puede ser una partición de VMFS.

<code><i>datastore name</i></code>	Especifica dónde se debe montar la partición.
<code>--ondisk=</code> or <code>--ondrive=</code>	Especifica el disco o la unidad en la que se crea la partición.
<code>--firstdisk=</code> <code><i>disk-type1,</i></code> <code><i>[disk-type2,...]</i></code>	<p>Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:</p> <ol style="list-style-type: none"> 1 Almacenamiento conectado a nivel local (<code>local</code>) 2 Almacenamiento en red (<code>remote</code>) 3 Discos USB (<code>usb</code>) <p>Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye <code>esx</code> para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es <code>--firstdisk=ST3120814A,mptsas,local</code>.</p>

reboot (opcional)

Reinicia la máquina después de que finaliza la instalación generada por script.

<code><--noeject></code>	No se expulsa el CD después de la instalación.
--------------------------------	--

rootpw (obligatorio)

Configura la contraseña raíz para el sistema.

<code>--iscripted</code>	Especifica que la contraseña está cifrada.
<code>password</code>	Especifica el valor de la contraseña.

actualizar

Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

<code>--disk=</code> or <code>--drive=</code>	Especifica el disco que se particionará. En el comando <code>--disk=diskname</code> , el valor <i>diskname</i> puede tener cualquiera de los formatos que se muestran en los ejemplos siguientes:
---	---

- Ruta de acceso: `--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`
- Nombre de MPX: `--disk=mpx.vmhba1:C0:T0:L0`
- Nombre de VML: `--disk=vml.000000034211234`
- UID de vmkLUN: `--disk=vmkLUN_UID`

Para conocer los formatos admitidos de nombre de disco, consulte [Nombre de los dispositivos de disco](#).

<code>--firstdisk=</code> <code>disk-type1,</code> <code>[disk-type2,...]</code>	Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:
--	---

- 1 Almacenamiento conectado a nivel local (`local`)
- 2 Almacenamiento en red (`remote`)
- 3 Discos USB (`usb`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`.

%include o include (opcional)

Especifica otro script de instalación para analizar. Este comando se utiliza de manera similar a un comando de varias líneas, pero usa solamente un argumento.

filename Por ejemplo: %include part.cfg

%pre (opcional)

Especifica un script para ejecutar antes de que se evalúe la configuración de inicio. Por ejemplo, puede usarse para generar los archivos que incluirá el archivo de inicio.

--interpreter Especifica el intérprete que se usará. El valor predeterminado es
=[python|busybox] busybox.

%post (opcional)

Ejecuta el script especificado después de que finaliza la instalación del paquete. Si se especifican varias secciones %post, se ejecutan en el orden en que aparecen en el script de instalación.

--interpreter Especifica el intérprete que se usará. El valor predeterminado es
=[python|busybox] busybox.

--timeout=secs Especifica el límite de tiempo de espera para la ejecución del script. Si el script no ha finalizado cuando se agota el tiempo de espera, se interrumpe de manera forzosa.

--ignorefailure Si se configura como true, la instalación se considera correcta aunque el script %post haya terminado con un error.
=[true|false]

%firstboot

Crea un script `init` que se ejecuta solamente durante el primer arranque. El script no afecta los arranques posteriores. Si se especifican varias secciones %firstboot, se ejecutan en el orden en que aparecen en el archivo de inicio.

Nota No es posible comprobar la semántica de los scripts %firstboot hasta el primer arranque del sistema. Un script %firstboot puede contener errores potencialmente catastróficos que no se detectan sino hasta después de la finalización de la instalación.

--interpreter Especifica el intérprete que se usará. El valor predeterminado es
=[python|busybox] busybox.

Nota No es posible comprobar la semántica del script %firstboot hasta el primer arranque del sistema. Si el script contiene errores, no se detectan sino hasta después de la finalización de la instalación.

Nombre de los dispositivos de disco

Para los comandos del script de instalación `install`, `upgrade` e `installorupgrade`, es necesario usar los nombres de dispositivos de disco.

Tabla 4-3. Nombre de los dispositivos de disco

Formato	Ejemplo	Descripción
VML	vml.00025261	El nombre del dispositivo que indica el VMkernel
MPX	mpx.vmhba0:C0:T0:L0	El nombre del dispositivo

Acerca del archivo boot.cfg

El archivo de configuración del cargador de arranque `boot.cfg` especifica el kernel, las opciones del kernel y los módulos de arranque que utiliza el cargador de arranque `mboot.c32` en una instalación de ESXi.

El archivo `boot.cfg` se incluye en el instalador de ESXi. Puede modificar la línea `kernelopt` del archivo `boot.cfg` para especificar la ubicación de un script de instalación o para pasar otras opciones de arranque.

El archivo `boot.cfg` tiene la siguiente sintaxis:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn

# Any other line must remain unchanged.
```

Los comandos de `boot.cfg` configuran el cargador de arranque.

Tabla 4-4. Comandos de boot.cfg.

Comando	Descripción
<code>title=STRING</code>	Establece el título del cargador de arranque como <code>STRING</code> .
<code>kernel=FILEPATH</code>	Establece la ruta de acceso del kernel como <code>FILEPATH</code> .
<code>kernelopt=STRING</code>	Anexa <code>STRING</code> a las opciones de arranque del kernel.
<code>modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn</code>	Enumera los módulos que se van a cargar, separados por tres guiones (---).

Por ejemplo, para modificar el archivo `boot.cfg` con información para un servidor HTTP, consulte [Arranque PXE del instalador de ESXi mediante gPXE](#).

Consulte también [Crear una imagen ISO de instalador con un script de instalación o actualización personalizado](#), [Realizar arranque PXE del instalador de ESXi con PXELINUX y un archivo de configuración de PXE](#), [Arranque PXE del instalador de ESXi a través de PXELINUX y un archivo de configuración de isolinux.cfg](#) y [Arranque PXE del instalador de ESXi](#).

Instalar o actualizar ESXi desde un CD o DVD con un script

Puede instalar o actualizar ESXi desde una unidad de CD-ROM o DVD-ROM utilizando un script que especifique las opciones de instalación o actualización.

Puede iniciar el script de instalación o actualización introduciendo una opción de arranque cuando inicie el host. También puede crear una imagen ISO de instalador que incluya el script de instalación. Puede utilizar una imagen ISO de instalador para realizar una instalación generada por script y desatendida cuando arranque con la imagen ISO de instalador resultante. Consulte [Crear una imagen ISO de instalador con un script de instalación o actualización personalizado](#).

Requisitos previos

Antes de ejecutar la instalación o la actualización generadas por script, asegúrese de que se cumplen los siguientes requisitos previos:

- El sistema en el que va a realizar la instalación o actualización cumple con los requisitos de hardware. Consulte [Requisitos de hardware de ESXi](#).
- Tiene el ISO con el instalador de ESXi en un CD o DVD de instalación. Consulte [Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi](#).
- El sistema puede acceder al script de instalación o actualización predeterminado (`ks.cfg`) o a un script de instalación o actualización personalizado. Consulte [Acerca de los scripts de instalación y actualización](#).
- Ha seleccionado un comando de arranque para ejecutar la instalación o actualización generada por script. Consulte [Introducir las opciones de arranque para iniciar un script de instalación o actualización](#). Para obtener una lista completa de los comandos de arranque, consulte [Opciones de arranque](#).

Procedimiento

- 1 Arranque el instalador de ESXi desde la unidad de CD-ROM o DVD-ROM local.

- 2 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



- 3 Introduzca una opción de arranque que invoque al archivo de script de instalación o actualización predeterminado o uno que haya creado.

La opción de arranque tiene el formato `ks=`.

- 4 Presione Intro.

Resultados

Se ejecuta la operación de instalación, actualización o migración, utilizando las opciones que especificó.

Instalar o actualizar ESXi desde una unidad flash USB mediante un script

Puede instalar o actualizar ESXi desde una unidad flash USB utilizando un script que especifique las opciones de instalación o actualización.

Las opciones de arranque compatibles se detallan en [Opciones de arranque](#).

Requisitos previos

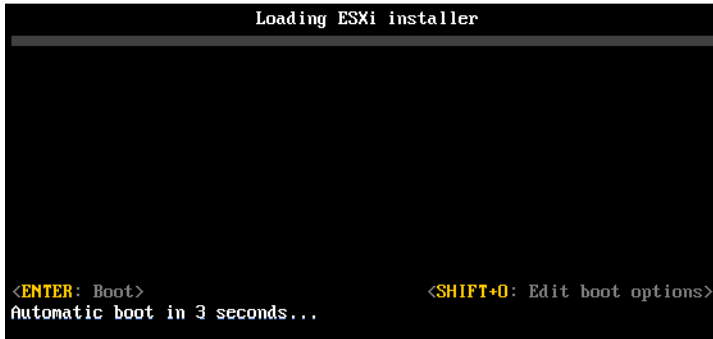
Antes de ejecutar la instalación o la actualización generadas por script, asegúrese de que se cumplen los siguientes requisitos previos:

- El sistema en el que va a realizar la instalación o la actualización a ESXi cumple con los requisitos de hardware para la instalación o la actualización. Consulte [Requisitos de hardware de ESXi](#).
- Tiene el ISO con el instalador de ESXi en una unidad USB flash de arranque. Consulte [Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi](#).
- El sistema puede acceder al script de instalación o actualización predeterminado (`ks.cfg`) o a un script de instalación o actualización personalizado. Consulte [Acerca de los scripts de instalación y actualización](#).

- Ha seleccionado una opción de arranque para ejecutar la instalación, la actualización o la migración generadas por script. Consulte [Introducir las opciones de arranque para iniciar un script de instalación o actualización](#).

Procedimiento

- 1 Arranque el instalador de ESXi desde la unidad flash USB.
- 2 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



- 3 Introduzca una opción de arranque que invoque al archivo de script de instalación o actualización predeterminado o uno que haya creado.

La opción de arranque tiene el formato `ks=`.

- 4 Presione Intro.

Resultados

Se ejecuta la operación de instalación, actualización o migración, utilizando las opciones que especificó.

Realizar una instalación o actualización generada por script de ESXi a través de PXE para arrancar el instalador

ESXi 6.0 ofrece varias opciones para utilizar PXE para arrancar el instalador y utilizar un script de instalación o actualización.

- Para obtener información sobre la configuración de una infraestructura PXE, consulte [Arranque PXE del instalador de ESXi](#).
- Para obtener información sobre la creación y ubicación de un script de instalación, consulte [Acerca de los scripts de instalación y actualización](#).
- Para procedimientos específicos para utilizar PXE para arrancar el instalador de ESXi y utilizar un script de instalación, consulte uno de los siguientes temas:
 - [Arranque PXE del instalador de ESXi a través de PXELINUX y un archivo de configuración de isolinux.cfg](#)

- Realizar arranque PXE del instalador de ESXi con PXELINUX y un archivo de configuración de PXE
- Arranque PXE del instalador de ESXi mediante gPXE
- Para obtener información sobre la utilización de vSphere Auto Deploy para realizar una instalación generada por script a través de PXE para arrancar, consulte [Instalar ESXi con vSphere Auto Deploy](#).

Instalar ESXi con vSphere Auto Deploy

vSphere Auto Deploy permite aprovisionar cientos de hosts físicos con el software ESXi.

Mediante el uso de Auto Deploy, los administradores de sistemas experimentados pueden administrar de forma eficiente implementaciones grandes. Los hosts se arrancan mediante la red desde un servidor Auto Deploy central. De forma opcional, se configuran los hosts con un perfil de host de un host de referencia. El perfil de host se puede configurar para que le solicite al usuario información. Después que concluya el arranque y la configuración, los hosts los administra vCenter Server al igual que otros hosts ESXi.

Auto Deploy también se puede utilizar para almacenamientos en caché sin estado o instalaciones con estado.

Importante Auto Deploy requiere una separación segura entre la red de producción y las redes de administración o implementación, según se describe en [Consideraciones de seguridad de Auto Deploy](#). No es seguro utilizar Auto Deploy sin esta separación.

Almacenamiento en caché sin estado

De manera predeterminada, Auto Deploy no almacena la configuración o estado de ESXi en el disco host. En su lugar, un perfil de imagen define la imagen con la que se aprovisiona el host. Los otros atributos de host se administran mediante perfiles de host. El host que utiliza Auto Deploy para el almacenamiento en caché sin estado debe conectarse al servidor Auto Deploy y a vCenter Server.

Instalaciones con estado

Puede aprovisionar un host con Auto Deploy y configurar el host para que almacene la imagen en el disco. En los arranques posteriores, el host lo hará desde el disco.

Información sobre vSphere Auto Deploy

vSphere Auto Deploy puede aprovisionar cientos de hosts físicos con el software ESXi. Se puede especificar la imagen que se implementará y los hosts que se aprovisionarán con esa imagen. De manera opcional, se pueden especificar los perfiles de host que se aplican a los hosts y una ubicación de vCenter Server (carpeta o clúster) para cada host.

Introducción a vSphere Auto Deploy

Cuando se inicia un host físico configurado para vSphere Auto Deploy, vSphere Auto Deploy usa la infraestructura de arranque PXE junto con perfiles de host de vSphere para aprovisionar y personalizar ese host. No se almacena ningún estado en el propio host. En su lugar, el servidor vSphere Auto Deploy administra la información de estado de cada host.

Información de estado de hosts ESXi

vSphere Auto Deploy almacena la información de los hosts ESXi que se van a aprovisionar en distintas ubicaciones. La información sobre la ubicación de los perfiles de imagen y de host se especifica inicialmente en las reglas que asignan equipos a perfiles de imagen y de host.

Tabla 4-5. vSphere Auto Deploy almacena información de implementación

Tipo de información	Descripción	Origen de información
Estado de imagen	El software ejecutable que se va a ejecutar en un host ESXi.	Perfil de imagen, creado con vSphere ESXi Image Builder.
Estado de configuración	Los parámetros que se pueden configurar, los cuales determinan el modo en que se configura el host; por ejemplo, conmutadores virtuales y su configuración, configuración de controladores y parámetros de arranque, etc.	Perfil de host, creado mediante la interfaz de usuario del perfil de host. A menudo proviene de un host de plantillas.
Estado dinámico	El estado de tiempo de ejecución que genera el software en ejecución; por ejemplo, claves privadas generadas o bases de datos de tiempo de ejecución.	Memoria de host, que se pierde durante el reinicio.
Estado de máquina virtual	Las máquinas virtuales almacenadas en un host y la información de inicio automático de máquinas virtuales (solo arranques posteriores).	La información de máquinas virtuales que envía vCenter Server a vSphere Auto Deploy debe estar disponible para suministrar información de máquinas virtuales a vSphere Auto Deploy.
Intervención del usuario	El estado basado en la intervención del usuario (por ejemplo, una dirección IP que el usuario proporciona cuando se inicia el sistema) no se puede incluir automáticamente en el perfil de host.	<p>Información de personalización del host, almacenada por vCenter Server durante el primer arranque.</p> <p>Puede crear un perfil de host que requiera la intervención del usuario para determinados valores.</p> <p>Cuando vSphere Auto Deploy aplica un perfil de host para el que se requiere información que proporcionó el usuario, el host se coloca en modo de mantenimiento. Utilice la interfaz de usuario del perfil de host para comprobar el cumplimiento del perfil de host y responda al aviso para personalizar el host.</p>

Arquitectura de vSphere Auto Deploy

La infraestructura de vSphere Auto Deploy consta de varios componentes.

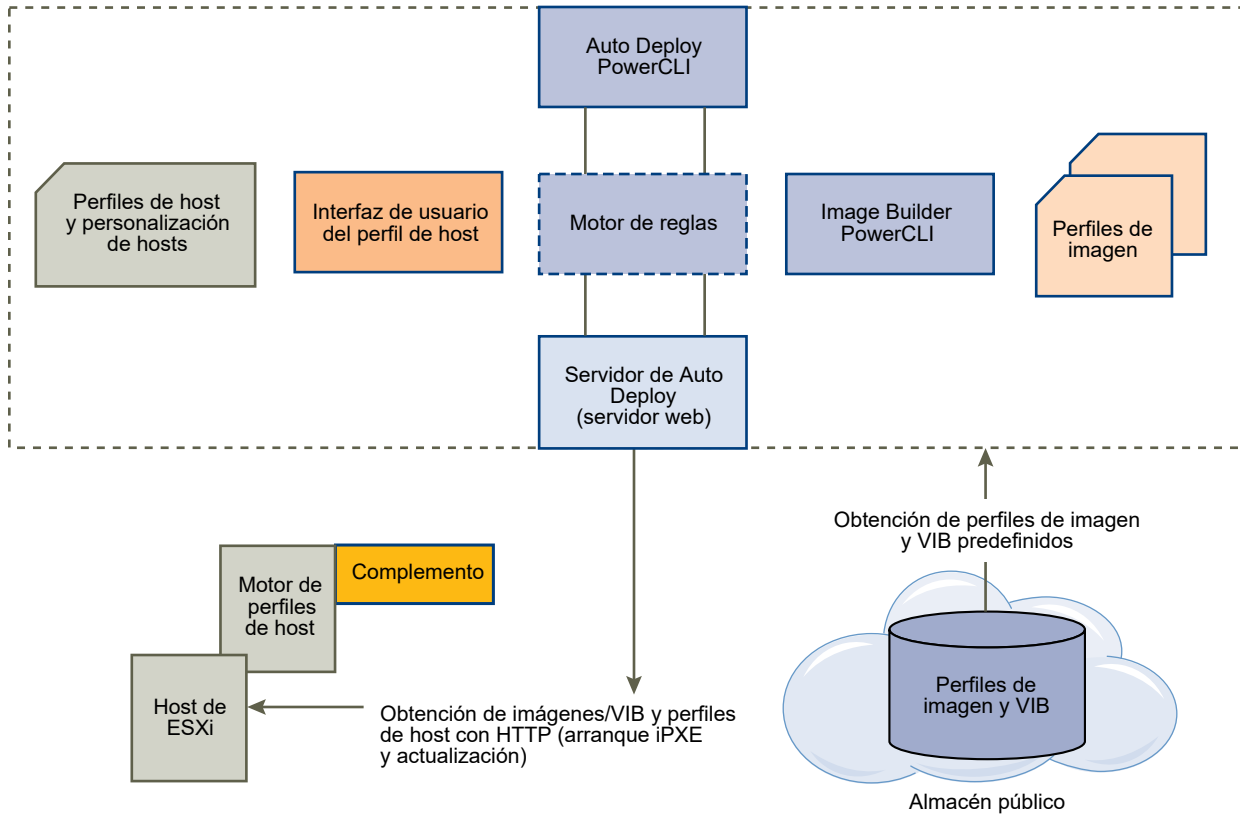
Para obtener más información, vea el vídeo "Arquitectura de Auto Deploy":



Arquitectura de Auto Deploy

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_i4ajkcm2/uiConfId/49694343/)

Figura 4-1. Arquitectura de vSphere Auto Deploy



Servidor vSphere Auto Deploy

Sirve imágenes y perfiles de host a hosts ESXi.

Motor de reglas de vSphere Auto Deploy

Envía información al servidor vSphere Auto Deploy sobre qué perfil de imagen y qué perfil de host asignar a qué host. Los administradores utilizan vSphere Auto Deploy para definir las reglas que asignan perfiles de imagen y perfiles de host a los hosts. Para obtener más información sobre las reglas y los conjuntos de reglas de vSphere Auto Deploy, consulte [Reglas y conjuntos de reglas](#).

Perfiles de imagen

Defina el conjunto de VIB para arrancar hosts ESXi.

- VMware y los partners de VMware ponen perfiles de imagen y VIB a disposición en almacenes públicos. Utilice vSphere ESXi Image Builder para examinar el almacén y use el motor de reglas de vSphere Auto Deploy para especificar qué perfil de imagen se debe asignar a qué host.

- Los clientes de VMware pueden crear un perfil de imagen personalizado basado en los perfiles de imagen y VIB públicos del almacén y aplicar ese perfil de imagen al host. Consulte [Personalizar instalaciones con ESXi Image Builder CLI](#).

Perfiles de host

Defina la configuración específica de equipo, como parámetros de red o almacenamiento. Utilice la interfaz de usuario del perfil de host para crear perfiles de host. Puede crear un perfil de host para un host de referencia y aplicar dicho perfil a otros hosts del entorno para obtener una configuración coherente. Para obtener más información, consulte la documentación *Perfiles de host de vSphere* o la sección [Configurar un host de referencia de Auto Deploy](#).

Personalizar hosts

Almacena información que el usuario proporciona cuando se aplican perfiles de host al host. La personalización de host podría contener direcciones IP u otra información que el usuario suministró para ese host. Para obtener más información sobre la personalización de host, consulte la documentación *Perfiles de host de vSphere*.

En las versiones anteriores de vSphere Auto Deploy, la personalización de host se denominaba archivo de respuesta.

Reglas y conjuntos de reglas

El comportamiento del servidor Auto Deploy se especifica con un conjunto de reglas escritas en PowerCLI. El motor de reglas de Auto Deploy comprueba la regla para patrones de host coincidentes a fin de decidir con qué elementos (perfil de imagen, perfil de host o ubicación de vCenter Server) se debe aprovisionar cada host.

El motor de reglas asigna parámetros de software y configuración a los hosts según los atributos del host. Por ejemplo, puede implementar perfiles de imagen o perfiles de host a dos clústeres de hosts escribiendo dos reglas, cada una de las cuales debe coincidir con la dirección de red de un clúster.

Para hosts que aún no se han agregado a un sistema vCenter Server, el servidor Auto Deploy comprueba con el motor de reglas antes de entregar perfiles de imagen, perfiles de host e información de ubicación de inventario a los hosts. Para hosts administrados por un sistema vCenter Server, se usa el perfil de imagen, perfil de host y ubicación de inventario que vCenter Server tiene almacenados en el objeto de host. Si hace cambios a las reglas, puede usar los cmdlets de PowerCLI de Auto Deploy para probar y reparar el cumplimiento de reglas. Cuando se repara el cumplimiento de reglas para un host, se actualizan las asignaciones de perfil de imagen y perfil de host de ese host.

El motor de reglas incluye reglas y conjuntos de reglas.

Reglas

Las reglas pueden asignar perfiles de imagen y de host a un conjunto de hosts, o bien especificar la ubicación (carpeta o clúster) de un host en el sistema vCenter Server destino. Una regla puede identificar hosts de destino mediante la dirección MAC de arranque, la

información del SMBIOS, la UUID del BIOS, el proveedor, el modelo o la dirección IP de DHCP fija. En la mayoría de los casos, se aplican reglas a varios hosts. Las reglas se crean mediante los cmdlets de PowerCLI de Auto Deploy. Después de crear una regla, se la debe agregar a un conjunto de reglas. Solo se admiten dos conjuntos de reglas: el conjunto de reglas activas y el conjunto de reglas de trabajo. Una regla puede pertenecer a ambos conjuntos, al predeterminado o solo al conjunto de reglas de trabajo. Una vez que la regla se agrega a un conjunto de reglas, ya no se puede cambiar. En su lugar, copie la regla y reemplace los elementos o los patrones en la copia.

Conjunto de reglas activas

Cuando un host iniciado recientemente contacta al servidor Auto Deploy con una solicitud de perfil de imagen, el servidor Auto Deploy comprueba que el conjunto de reglas activas tenga reglas coincidentes. El perfil de imagen, el perfil de host y la ubicación de inventario de vCenter Server que se asignan mediante reglas coincidentes se utilizan posteriormente para arrancar el host. Si las reglas asignan más de un elemento del mismo tipo, el servidor Auto Deploy utiliza el elemento que aparezca primero en el conjunto de reglas.

Conjunto de reglas de trabajo

El conjunto de reglas de trabajo permite probar cambios en las reglas antes de que se activen dichos cambios. Por ejemplo, puede usar cmdlets de PowerCLI de Auto Deploy para probar el cumplimiento del conjunto de reglas de trabajo. La prueba verifica que los hosts administrados por un sistema vCenter Server sigan las reglas en el conjunto de reglas de trabajo. De manera predeterminada, los cmdlets agregan la regla al conjunto de reglas de trabajo y activan las reglas. Utilice el parámetro `NoActivate` para agregar una regla solamente al conjunto de reglas de trabajo.

Con las reglas y los conjuntos de reglas se usa el siguiente flujo de trabajo.

- 1 Haga cambios en el conjunto de reglas de trabajo.
- 2 Use cmdlets que ejecuten las reglas del conjunto de reglas de trabajo para un host a fin de garantizar que todo funcione correctamente.
- 3 Refine y vuelva a probar las reglas en el conjunto de reglas de trabajo.
- 4 Active las reglas en el conjunto de reglas de trabajo.

Si agrega una regla y no especifica el parámetro `NoActivate`, se activan todas las reglas que se encuentran actualmente en el conjunto de reglas de trabajo. No puede activar reglas individuales.

Consulte la ayuda de la línea de comandos de PowerCLI y [Administrar Auto Deploy con los cmdlets de PowerCLI](#).

Proceso de arranque de Auto Deploy

Al arrancar un host que desea aprovisionar o reaprovisionar con vSphere Auto Deploy, la infraestructura de Auto Deploy suministra el perfil de imagen y, opcionalmente, un perfil de host y una ubicación de vCenter Server para ese host.

El proceso de arranque para los hosts que aún no se han aprovisionado con Auto Deploy (primer arranque) es distinto que el de los hosts que sí se aprovisionaron y se agregaron a un sistema vCenter Server (arranque posterior).

Requisitos previos para primer arranque

Antes de un proceso de primer arranque, debe configurar el sistema. La configuración incluye las siguientes tareas, que se tratan más detalladamente en [Prepararse para vSphere Auto Deploy](#).

- Configure un servidor DHCP que asigne una dirección IP a cada host durante el inicio y que apunte el host al servidor TFTP desde el que se va a descargar el cargador de arranque iPXE.
- Compruebe que el servidor Auto Deploy tenga una dirección IPv4. El arranque PXE solo es compatible con IPv4.
- Identifique el perfil de imagen que se va a usar de una de las siguientes maneras.
 - Elija un perfil de imagen de ESXi de un almacén público.
 - (opcional) Cree un perfil de imagen personalizado mediante Image Builder PowerCLI y colóquelo en un almacén al que pueda acceder el servidor Auto Deploy. El perfil de imagen debe incluir un VIB de ESXi de base.
- (opcional) Si tiene un host de referencia en el entorno, exporte el perfil de host de este y defina una regla que aplique el perfil a uno o más hosts. Consulte [Configurar un host de referencia de Auto Deploy](#).
- Especifique reglas para la implementación del host y agréguelas al conjunto de reglas activo.

Información general sobre el primer arranque

Cuando se arranca un host que aún no se aprovisionó con vSphere Auto Deploy (primer arranque), este interactúa con varios componentes de Auto Deploy.

- 1 Cuando el administrador enciende un host, este inicia una secuencia de arranque PXE.
El servidor DHCP asigna una dirección IP al host y le indica que debe ponerse en contacto con el servidor TFTP.
- 2 El host realiza esta acción y descarga el archivo iPXE (cargador de arranque ejecutable) y un archivo de configuración iPXE.
- 3 iPXE comienza a ejecutarse.
El archivo de configuración le indica al host que realice una solicitud de arranque HTTP al servidor Auto Deploy. La solicitud HTTP incluye información de hardware y de red.
- 4 En respuesta, el servidor Auto Deploy realiza estas tareas:
 - a Consulta al motor de reglas la información sobre el host.
 - b Transmite los componentes especificados en el perfil de imagen, el perfil de host opcional e información de ubicación de vCenter Server opcional.
- 5 El host arranca mediante el perfil de imagen.

Si el servidor Auto Deploy proporcionó un perfil de host, este se aplica al host.

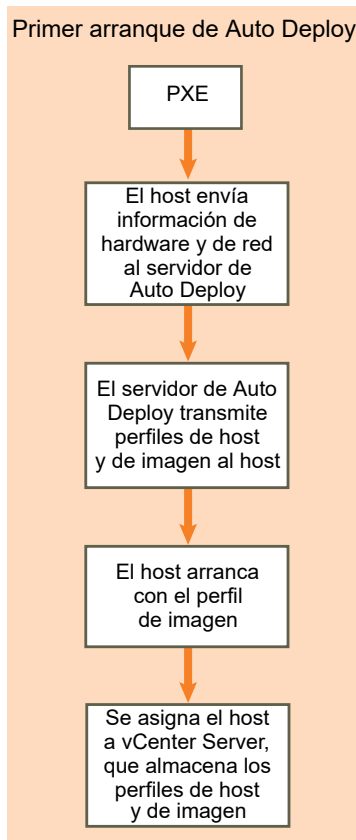
- 6 Auto Deploy agrega el host al sistema vCenter Server en el que está registrado Auto Deploy.
 - a Si una regla especifica una carpeta o un clúster de destino en el sistema vCenter Server, el host se coloca en esa carpeta o ese clúster. La carpeta de destino debe estar dentro de un centro de datos.
 - b Si no existe una regla que especifique una ubicación de inventario de vCenter Server, Auto Deploy agrega el host al primer centro de datos que aparece en la interfaz de usuario de vSphere Web Client.
- 7 (opcional) Si el perfil de host requiere que el usuario especifique cierta información, como una dirección IP estática, el host se coloca en modo de mantenimiento cuando se lo agrega al sistema vCenter Server.

Debe volver a aplicar el perfil de host y actualizar la personalización del host para que este salga del modo de mantenimiento. Al actualizar la personalización del host, debe responder las preguntas cuando se le pida.

- 8 Si el host forma parte de un clúster de DRS, las máquinas virtuales de otros hosts podrían migrarse al host después de que este se haya agregado correctamente al sistema vCenter Server.

Consulte [Aprovisionar un host \(primer arranque\)](#).

Figura 4-2. Instalar Auto Deploy, primer arranque



Arranques posteriores sin actualizaciones

En el caso de los hosts aprovisionados con Auto Deploy y administrados por un sistema vCenter Server, los arranques posteriores pueden volverse completamente automáticos.

- 1 El administrador reinicia el host.
- 2 A medida que el host arranca, Auto Deploy lo aprovisiona con su perfil de imagen y su perfil de host.
- 3 Las máquinas virtuales se activan o se migran al host en base a la configuración del host.
 - Host independiente. Las máquinas virtuales se encienden de acuerdo con las reglas de inicio automático definidas en el host.
 - Host del clúster de DRS. Las máquinas virtuales que se migraron correctamente a otros hosts permanecen allí. Las máquinas virtuales para las que ningún host tenía recursos suficientes se registran en el host que se reinició.

Si el sistema vCenter Server no está disponible, el host se pone en contacto con Auto Deploy y se aprovisiona con un perfil de imagen. El host continúa poniéndose en contacto con el servidor Auto Deploy hasta que Auto Deploy vuelve a conectarse con el sistema vCenter Server.

Auto Deploy no puede configurar los conmutadores distribuidos de vSphere si vCenter Server no está disponible. Asimismo, las máquinas virtuales se asignan a hosts solo si forman parte de un clúster HA. Una vez que el host vuelva a conectarse a vCenter Server y se aplique el perfil de host, podrá crear el conmutador. Debido a que el host se encuentra en modo de mantenimiento, no es posible iniciar las máquinas virtuales. Consulte [Reaprovisionar hosts con operaciones de reinicio simples](#).

Los hosts que están configurados para pedir intervención del usuario se colocan en modo de mantenimiento. Consulte [Actualizar la personalización de hosts en vSphere Web Client](#).

Arranques posteriores con actualizaciones

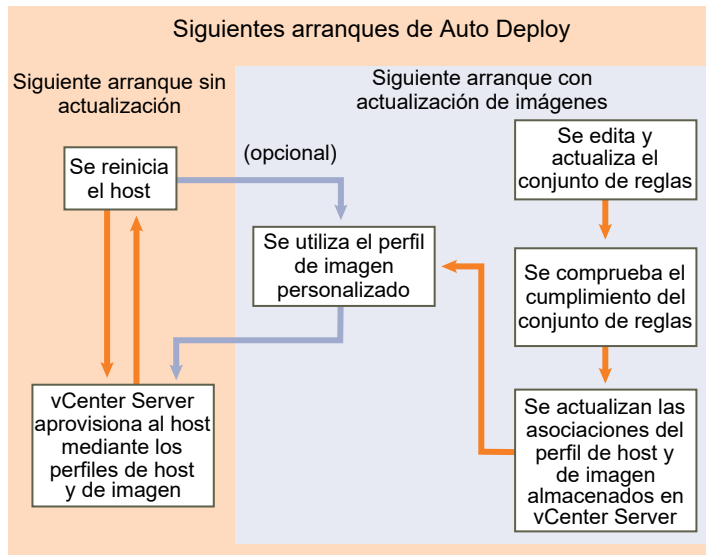
Puede cambiar el perfil de imagen, el perfil de host o la ubicación de vCenter Server para hosts. El proceso involucra cambiar reglas, así como probar y reparar el cumplimiento de reglas del host.

- 1 El administrador utiliza el cmdlet `Copy-DeployRule` de PowerCLI para copiar y editar una o más reglas. A continuación, actualiza el conjunto de reglas. Consulte [Inicio rápido de Auto Deploy](#) para ver un ejemplo.
- 2 El administrador ejecuta el cmdlet `Test-DeployRulesetCompliance` para comprobar si cada host utiliza la información que especifica el conjunto de reglas actual.
- 3 El host devuelve un objeto de PowerCLI que encapsula la información de cumplimiento.
- 4 El administrador ejecuta el cmdlet `Repair-DeployRulesetCompliance` para actualizar el perfil de imagen, el perfil de host o la ubicación de vCenter Server donde el sistema vCenter Server se almacena para cada host.
- 5 Cuando el host se reinicia, utiliza el perfil de imagen, el perfil de host o la ubicación de vCenter Server del host actualizados.

Si el perfil de host está configurado para solicitar la intervención del usuario, el host se coloca en modo de mantenimiento. Siga los pasos descritos en [Actualizar la personalización de hosts en vSphere Web Client](#).

Consulte [Probar y reparar cumplimiento de reglas](#).

Figura 4-3. Instalar Auto Deploy, arranques posteriores



Aprovisionar sistemas que tienen conmutadores distribuidos

Puede configurar el perfil de host de un host de referencia de Auto Deploy con un conmutador distribuido.

Cuando configura el conmutador distribuido, la directiva de parámetros de configuración de arranque se establece automáticamente para que coincida con los parámetros de red necesarios para la conectividad del host después de un reinicio.

Cuando Auto Deploy aprovisiona el host ESXi con el perfil de host, el host pasa por un proceso de dos pasos.

- 1 Crea un conmutador estándar virtual con las propiedades especificadas en el campo de parámetros de configuración de arranque.
- 2 Crea las NIC de VMkernel. Las NIC de VMkernel permiten que el host se conecte con Auto Deploy y el sistema vCenter Server.

Cuando el host se agrega a vCenter Server, vCenter Server elimina el conmutador estándar y vuelve a aplicar el conmutador distribuido al host.

Nota No modifique los parámetros de configuración de arranque del host para evitar problemas con el conmutador distribuido.

Información general del cmdlet y el inicio rápido de Auto Deploy

Para utilizar Auto Deploy correctamente, debe conocer las tareas involucradas en el aprovisionamiento de hosts, los componentes de Auto Deploy y su interacción, así como los cmdlets de PowerCLI.

Inicio rápido de Auto Deploy

Para comenzar a usar Auto Deploy, debe aprender cómo funciona Auto Deploy, instalar el servidor Auto Deploy, instalar vSphere PowerCLI, escribir reglas de vSphere PowerCLI que aprovisionen hosts y encender los hosts que deben arrancarse con el perfil de imagen especificado. Puede personalizar el perfil de imagen, el perfil de host y la ubicación de vCenter Server.

Consulte [Configurar prueba de concepto de Auto Deploy](#) para obtener un ejercicio paso a paso que lo ayudará a configurar su primer entorno de Auto Deploy en un sistema Windows Server 2008.

Para aprovisionar correctamente los hosts en su entorno con Auto Deploy, puede seguir estos pasos.

- 1 Instale vCenter Server y los componentes de vCenter Server, o implemente vCenter Server Appliance.

El servidor Auto Deploy se incluye junto con el nodo de administración.

- 2 Instale vSphere PowerCLI, que incluye cmdlets de Auto Deploy e Image Builder.

Consulte [Instalar vSphere PowerCLI y software de requisito previo](#) y [Usar los cmdlets de Auto Deploy](#).

- 3 Busque el perfil de imagen que incluye los VIB que desea implementar en los hosts.

- En la mayoría de los casos, debe agregar los almacenes que contienen el software necesario a la sesión de vSphere PowerCLI y, a continuación, seleccionar un perfil de imagen desde uno de esos almacenes.
- Si desea crear un perfil de imagen personalizado, use los cmdlets de Image Builder para clonar un perfil de imagen existente y agregue los VIB personalizados al clon. Agregue el perfil de imagen personalizado a la sesión de vSphere PowerCLI.

Debe utilizar Image Builder para la personalización solamente si tiene que agregar o quitar VIB. En la mayoría de los casos, puede agregar el almacén en el que VMware aloja los perfiles de imagen a la sesión de vSphere PowerCLI como una URL.

- 4 Use el cmdlet `New-DeployRule` de vSphere PowerCLI para escribir una regla que asigne el perfil de imagen a un host, a varios hosts especificados mediante un patrón o a todos los hosts.

```
New-DeployRule -Name "testrule" -Item image-profile -AllHosts
```

Consulte [Asignar un perfil de imagen a hosts](#).

Nota Auto Deploy está optimizado para aprovisionar hosts que tienen una dirección MAC fija a una asignación de dirección IP en DHCP (a veces denominadas reservas de DHCP). Si desea utilizar direcciones IP estáticas, debe configurar el perfil de host para que solicite la personalización del host. Consulte [Configurar Host Profiles para direcciones IP estáticas en vSphere Web Client](#).

- 5 Encienda el host para que Auto Deploy aprovisione el host con el perfil de imagen especificado.
- 6 Configure el host aprovisionado como host de referencia para el perfil de host.
Puede especificar la configuración de Syslog del host de referencia, la configuración del firewall, el almacenamiento, las redes, etc. Consulte [Configurar un host de referencia de Auto Deploy](#).
- 7 Cree y exporte un perfil de host para el host de referencia.
Consulte la documentación sobre *Host Profiles*.
- 8 Para aprovisionar varios hosts, puede utilizar el cmdlet `Copy-DeployRule`.
Puede modificar la regla para asignar no solo un perfil de imagen, sino también un perfil de host y una ubicación de clúster.

```
Copy-DeployRule -DeployRule "testrule" -ReplaceItem
my_host_profile_from_reference_host,my_target_cluster
-ReplacePattern "ipv4=192.XXX.1.10-192.XXX.1.20"
```

Donde *my_host_profile_from_reference_host* es el nombre del perfil de host de referencia y *my_target_cluster* es el nombre del clúster de destino.

- 9 Encienda los hosts que desea aprovisionar.
Si los hosts que se especifican mediante el patrón actualmente no son administrados por un sistema vCenter Server, Auto Deploy los aprovisiona con el perfil de imagen ya almacenado y el perfil de host especificado, y los agrega al clúster de destino.
- 10 Compruebe que los hosts aprovisionados cumplan los siguientes requisitos:
 - Cada host está conectado al sistema vCenter Server.
 - Los hosts no están en modo de mantenimiento.
 - Los hosts no presentan instancias de incumplimiento de normas.
 - Cada host con un perfil de host que requiere entradas del usuario tiene información actualizada de personalización del host.

Corrija los problemas de cumplimiento de normas y personalización del host, y reinicie los hosts hasta que todos los hosts cumplan con los requisitos.

Consulte [Información sobre vSphere Auto Deploy](#) para obtener una introducción al proceso de arranque, las diferencias entre el primer arranque y los arranques posteriores y una descripción general del uso de la personalización de hosts.

Descripción general de cmdlets de Auto Deploy PowerCLI

El usuario especifica las reglas que asignan perfiles de imagen y perfiles de host a los hosts mediante un conjunto de cmdlets de PowerCLI que se incluyen en VMware PowerCLI.

Si no está familiarizado con PowerCLI, lea la documentación de PowerCLI y consulte [Usar los cmdlets de Auto Deploy](#). Puede obtener ayuda en relación con cualquier comando en la línea de comandos de PowerShell.

- Ayuda básica: `Get-Help cmdlet_name`
- Ayuda detallada: `Get-Help cmdlet_name-Detailed`

Nota Al ejecutar cmdlets de Auto Deploy, proporcione todos los parámetros en la línea de comandos cuando invoque el cmdlet. No se recomienda proporcionar parámetros en modo interactivo.

Tabla 4-6. Cmdlets de PowerCLI del motor de reglas

Comando	Descripción
<code>Get-DeployCommand</code>	Devuelve una lista de cmdlets de Auto Deploy.
<code>New-DeployRule</code>	Crea una nueva regla con los elementos y los patrones especificados.
<code>Set-DeployRule</code>	Actualiza una regla existente con los elementos y los patrones especificados. No es posible actualizar una regla que forma parte de un conjunto de reglas.
<code>Get-DeployRule</code>	Recupera las reglas con los nombres especificados.
<code>Copy-DeployRule</code>	Clona y actualiza una regla existente.
<code>Add-DeployRule</code>	Agrega una regla o más al conjunto de reglas de trabajo y, de forma predeterminada, también al conjunto de reglas activo. Utilice el parámetro <code>NoActivate</code> para agregar una regla solamente al conjunto de reglas de trabajo.
<code>Remove-DeployRule</code>	Elimina una regla o más del conjunto de reglas de trabajo y del conjunto de reglas activo. Ejecute este comando con el parámetro <code>-Delete</code> para eliminar la regla por completo.
<code>Set-DeployRuleset</code>	Establece de manera explícita la lista de reglas en el conjunto de reglas de trabajo.
<code>Get-DeployRuleset</code>	Recupera el conjunto de reglas de trabajo o el conjunto de reglas activo actuales.
<code>Switch-ActiveDeployRuleset</code>	Activa un conjunto de reglas para que todas las solicitudes nuevas se evalúen mediante el conjunto de reglas.
<code>Get-VMHostMatchingRules</code>	Recupera las reglas que coinciden con un patrón. Por ejemplo, es posible recuperar todas las reglas que se aplican a un host o a varios. Utilice este cmdlet principalmente para depuración.
<code>Test-DeployRulesetCompliance</code>	Comprueba si los elementos asociados con un host especificado cumplen los criterios del conjunto de reglas activo.

Tabla 4-6. Cmdlets de PowerCLI del motor de reglas (continuación)

Comando	Descripción
<code>Repair-DeployRulesetCompliance</code>	En función del resultado de <code>Test-DeployRulesetCompliance</code> , este cmdlet actualiza el perfil de imagen, el perfil de host y la ubicación de cada host en el inventario de vCenter Server. El cmdlet puede aplicar perfiles de imagen, aplicar perfiles de host o transferir hosts a carpetas o clústeres especificados previamente en el sistema vCenter Server.
<code>Apply-EsxImageProfile</code>	Asocia el perfil de imagen especificado con el host especificado.
<code>Get-VMHostImageProfile</code>	Recupera el perfil de imagen que utiliza un host especificado. Este cmdlet es diferente al cmdlet <code>Get-EsxImageProfile</code> en Image Builder PowerCLI.
<code>Repair-DeployImageCache</code>	Utilice este cmdlet solamente si la memoria caché de imagen de Auto Deploy se elimina accidentalmente.
<code>Get-VMHostAttributes</code>	Recupera los atributos de un host que se utilizan cuando el servidor Auto Deploy evalúa las reglas.
<code>Get-DeployMachineIdentity</code>	Devuelve un valor de cadena que Auto Deploy utiliza para vincular lógicamente un host ESXi de vCenter con una máquina física.
<code>Set-DeployMachineIdentity</code>	Vincula lógicamente un objeto de host en la base de datos de vCenter Server con una máquina física. Utilice este cmdlet para agregar hosts sin especificar reglas.
<code>Get-DeployOption</code>	Recupera las opciones de configuración globales de Auto Deploy. Actualmente, este cmdlet es compatible con la opción <code>vlan-id</code> , que especifica el identificador de la VLAN predeterminado para la red de administración de ESXi de un host aprovisionado con Auto Deploy. Auto Deploy utiliza el valor solo si el host se arranca sin un perfil de host.
<code>Set-DeployOption</code>	Establece el valor de una opción de configuración global. Actualmente, es compatible con la opción <code>vlan-id</code> para establecer un identificador de la VLAN predeterminado para la red de administración de ESXi.

Prepararse para vSphere Auto Deploy

Antes de comenzar a usar vSphere Auto Deploy, debe preparar el entorno. Comience con la configuración de los servidores y la preparación del hardware. Es necesario que registre el software Auto Deploy en el sistema vCenter Server que va a utilizar para administrar los hosts que aprovisiona. Además, debe instalar VMware PowerCLI.

■ Preparar el sistema e instalación del servidor Auto Deploy

Antes de que pueda realizar un arranque PXE de un host ESXi mediante vSphere Auto Deploy, debe instalar el software necesario y configurar los servidores DHCP y TFTP con los que interactúa Auto Deploy.

- [Instalar vSphere PowerCLI y software de requisito previo](#)

Antes de que pueda ejecutar los cmdlets de Auto Deploy para crear y modificar las reglas y los conjuntos de reglas que controlan el comportamiento de Auto Deploy, deberá instalar vSphere PowerCLI y todo el software de requisito previo. Los cmdlets de Auto Deploy se incluyen con la instalación de vSphere PowerCLI.

- [Usar los cmdlets de Auto Deploy](#)

Los cmdlets de Auto Deploy se implementan como cmdlets de Microsoft PowerShell y se incluyen en vSphere PowerCLI. Los usuarios de los cmdlets de Auto Deploy pueden aprovechar todas las funciones de vSphere PowerCLI.

- [Configurar licencias masivas](#)

Puede utilizar vSphere Web Client o ESXi Shell para especificar claves de licencia individuales o configurar licencias masivas mediante los cmdlets de PowerCLI. Las licencias masivas funcionan para todos los hosts ESXi, pero son especialmente útiles para los hosts aprovisionados con Auto Deploy.

Preparar el sistema e instalación del servidor Auto Deploy

Antes de que pueda realizar un arranque PXE de un host ESXi mediante vSphere Auto Deploy, debe instalar el software necesario y configurar los servidores DHCP y TFTP con los que interactúa Auto Deploy.

Requisitos previos

- Compruebe que los hosts que desea aprovisionar con Auto Deploy cumplan los requisitos de hardware para ESXi. Consulte [Requisitos de hardware de ESXi](#).

Nota No puede aprovisionar los hosts de EFI con Auto Deploy a menos que cambie el sistema EFI al modo de compatibilidad de BIOS.

- Compruebe que los hosts ESXi tengan conectividad de red con vCenter Server y que se cumplan todos los requisitos de puerto. Consulte [Puertos necesarios para vCenter Server y Platform Services Controller](#).
- Si desea usar las VLAN en el entorno de Auto Deploy, debe configurar las redes de extremo a extremo correctamente. Cuando el host realiza el arranque PXE, se debe configurar el controlador UNDI de manera que los marcos se etiqueten con los identificadores de VLAN apropiados. Debe realizar los cambios apropiados en el BIOS de forma manual para establecer esta configuración. De forma similar, debe configurar los grupos de puertos de ESXi correctamente con los identificadores de VLAN adecuados. Póngase en contacto con su administrador de red para obtener más información sobre la manera en la que los identificadores de VLAN se utilizan en el entorno.
- Asegúrese de contar con suficiente espacio de almacenamiento para el repositorio de Auto Deploy. El servidor Auto Deploy utiliza el repositorio para almacenar los datos que necesita, incluidos las reglas y los conjuntos de reglas que usted crea, así como los VIB y los perfiles de imagen que se especifican en las reglas.

Se recomienda asignar 2 GB para que haya suficiente espacio para almacenar cuatro perfiles de imagen y quede espacio adicional. Cada perfil de imagen requiere aproximadamente 350 MB. Determine cuántos perfiles de imagen utilizará para definir la cantidad de espacio que debe reservar para el repositorio de Auto Deploy.

- Otorgue privilegios administrativos al servidor DHCP que administra el segmento de red desde el cual desea realizar el arranque. Puede utilizar un servidor DHCP que ya se encuentre en el entorno, o bien instalarlo. Para configurar Auto Deploy, sustituya el nombre de archivo `gpxelinux.0` por `undionly.kpxe.vmw-hardwired`.
- Proteja la red como lo haría para cualquier otro método de implementación basado en PXE. Auto Deploy transfiere datos por SSL para evitar interferencias accidentales e intromisiones. No obstante, la autenticidad del cliente o del servidor Auto Deploy no se comprueba durante el arranque PXE.
- Configure un servidor remoto de Syslog. Consulte la documentación *vCenter Server and Host Management* para obtener información sobre la configuración del servidor de Syslog. Configure el primer host que arranque para que use el servidor remoto de Syslog y aplique el perfil de host de dicho host a todos los demás hosts de destino. También puede instalar y utilizar vSphere Syslog Collector, una herramienta de soporte de vCenter Server que proporciona una arquitectura unificada de registros del sistema y habilita el registro de red, así como la combinación de registros de varios hosts.
- Instale ESXi Dump Collector, configure el primer host de manera que todos los volcados de memoria del núcleo se direccionen a ESXi Dump Collector y aplique el perfil de host de ese host a todos los otros hosts. Consulte [Configurar ESXi Dump Collector con ESXCLI](#).
- Compruebe que el servidor Auto Deploy tenga una dirección IPv4. Auto Deploy no es compatible con entornos que solo utilicen IPv6 de extremo a extremo. La infraestructura de arranque PXE no es compatible con IPv6. Después de la implementación, puede volver a configurar los hosts de forma manual de manera que utilicen IPv6 y agregarlos a vCenter Server por IPv6. Sin embargo, la configuración de IPv6 de un host sin estado se pierde al reiniciarlo.

Procedimiento

- 1 Instale vCenter Server o implemente vCenter Server Appliance.
El servidor Auto Deploy se incluye junto con el nodo de administración.
- 2 Configure el tipo de inicio del servicio de Auto Deploy.
 - a Inicie sesión en el sistema de vCenter Server mediante vSphere Web Client.
 - b En la página de inicio de vSphere Web Client, haga clic en **Administración**.

- c En **Configuración del sistema**, haga clic en **Servicios**.
 - d Seleccione **Auto Deploy**, haga clic en el menú **Acciones** y seleccione **Editar tipo de inicio**.
 - En Windows, se deshabilita el servicio de Auto Deploy. En la ventana **Editar tipo de inicio**, seleccione **Manual** o **Automático** para habilitar Auto Deploy.
 - En el vCenter Server Appliance, el servicio de Auto Deploy está establecido de forma predeterminada en **Manual**. Si desea que el servicio de Auto Deploy se inicie de manera automática al iniciar el sistema operativo, seleccione **Automático**.
- 3 Configure el servidor TFTP.
- a En vSphere Web Client conectado al sistema de vCenter Server, seleccione el sistema de vCenter Server en la lista de inventario.
 - b Haga clic en la pestaña **Administrar**, seleccione **Configuración** y haga clic en **Auto Deploy**.
 - c Haga clic en **Descargar ZIP de arranque TFTP** para descargar el archivo de configuración de TFTP y, a continuación, descomprima el archivo en el directorio en el que el servidor TFTP almacena los archivos.
- 4 Configure el servidor DHCP de manera que apunte al servidor TFTP en el que se encuentra el archivo ZIP de TFTP.
- a Especifique la dirección IP del servidor TFTP en la opción 66 del DHCP, la cual se suele llamar `next-server`.
 - b Especifique el nombre del archivo de arranque, el cual es `undionly.kpxe.vmw-hardwired` en la opción 67 del DHCP, el cual se suele llamar `boot-filename`.
- 5 Configure todos los hosts que desea aprovisionar con Auto Deploy para realizar un arranque de red o un arranque PXE, según las instrucciones del fabricante.
- 6 Busque el perfil de imagen que desea utilizar y el almacén en el que se encuentra.
- En la mayoría de los casos, se apunta a un perfil de imagen que VMware pone a su disposición en un almacén público. Si desea incluir VIB personalizados junto con la imagen base, puede utilizar un perfil de imagen que se crea mediante vSphere ESXi Image Builder.
- 7 Cree una regla que asigne un perfil de imagen a los hosts.
- 8 (opcional) Si configura el entorno de manera que se utilice el modo de huellas digitales, puede reemplazar el certificado `rbd-ca.crt` de OpenSSL y la clave privada `rbd-ca.key` de OpenSSL por un certificado y una clave privada personales para utilizar su propia entidad de certificación (Certificate Authority, CA).
- En Windows, los archivos se encuentran en la subcarpeta `SSL` del directorio de instalación de Auto Deploy. Por ejemplo, la ruta de acceso predeterminada en Windows 7 es `C:\ProgramData\VMware\VMware vSphere Auto Deploy\ssl`.
 - En vCenter Server Appliance, los archivos se encuentran en `/etc/vmware-rbd/ssl/`.
- De manera predeterminada, vCenter Server 6.0 y posterior utilizan una entidad de certificación de vSphere.

Resultados

Al iniciar un host que se configura para Auto Deploy, este se comunica con el servidor DHCP y, a continuación, es dirigido al servidor Auto Deploy, el cual aprovisiona el host con el perfil de imagen que se especifica en el conjunto de reglas activo.

Pasos siguientes

- Instale vSphere PowerCLI. Consulte [Instalar vSphere PowerCLI y software de requisito previo](#).
- Utilice los cmdlets de vSphere PowerCLI para definir una regla que asigne un perfil de imagen y un perfil de host opcional al host.
- (opcional) Configure el primer host que aprovisiona como un host de referencia. Utilice el almacenamiento y la red, entre otras opciones que desea que el host de destino comparta. Cree un perfil de host para el host de referencia y escriba una regla que asigne tanto el perfil de imagen que ya se ha probado como el perfil de host a los hosts de destino.
- Si desea que Auto Deploy sobrescriba particiones existentes, configure un host de referencia de manera que realice la partición de forma automática y, a continuación, aplique el perfil de host del host de referencia a otros hosts. Consulte [Planificar e implementar la estrategia de creación de particiones](#).
- Si debe configurar información específica de un host, configure el perfil de host del host de referencia de manera que solicite la interacción del usuario. Consulte [Personalizar hosts en vSphere Web Client](#).

Instalar vSphere PowerCLI y software de requisito previo

Antes de que pueda ejecutar los cmdlets de Auto Deploy para crear y modificar las reglas y los conjuntos de reglas que controlan el comportamiento de Auto Deploy, deberá instalar vSphere PowerCLI y todo el software de requisito previo. Los cmdlets de Auto Deploy se incluyen con la instalación de vSphere PowerCLI.

Instale vSphere PowerCLI y el software de requisito previo en un sistema Microsoft Windows. Consulte el sitio web de Microsoft para obtener información sobre la instalación del software de Microsoft. Consulte la *Guía del usuario de vSphere PowerCLI* para obtener instrucciones detalladas para la instalación de vSphere PowerCLI.

Requisitos previos

- Compruebe que Microsoft .NET 4.5 SP2 esté instalado o instálelo desde el sitio web de Microsoft siguiendo las instrucciones detalladas en dicho sitio web.
- Compruebe que Windows PowerShell 3.0 esté instalado o instálelo desde el sitio web de Microsoft siguiendo las instrucciones detalladas en dicho sitio web.

Procedimiento

- ◆ Instale vSphere PowerCLI, que incluye los cmdlets de Auto Deploy.

Pasos siguientes

Revise [Usar los cmdlets de Auto Deploy](#). Si estos son sus primeros pasos con vSphere PowerCLI, lea la documentación de vSphere PowerCLI.

Utilice los cmdlets de Auto Deploy y otros cmdlets de vSphere PowerCLI y cmdlets de PowerShell para administrar las reglas y conjuntos de reglas de Auto Deploy. Utilice `Get-Help cmdlet_name` para obtener ayuda de la línea de comandos.

Usar los cmdlets de Auto Deploy

Los cmdlets de Auto Deploy se implementan como cmdlets de Microsoft PowerShell y se incluyen en vSphere PowerCLI. Los usuarios de los cmdlets de Auto Deploy pueden aprovechar todas las funciones de vSphere PowerCLI.

Los usuarios experimentados de PowerShell también pueden utilizar los cmdlets de Auto Deploy del mismo modo que los cmdlets de PowerShell. Si no está familiarizado con PowerShell y vSphere PowerCLI, las sugerencias siguientes pueden ser de utilidad.

Puede escribir cmdlets, parámetros y valores de parámetros en el shell de vSphere PowerCLI.

- Obtenga ayuda para cualquier cmdlet a través de `Get-Help cmdlet_name`.
- Recuerde que PowerShell no distingue mayúsculas de minúsculas.
- Utilice la opción de finalización con tabulación para los nombres de cmdlets y parámetros.
- Puede aplicar formato a cualquier resultado de cmdlet o variable mediante `Format-List` o `Format-Table`, o mediante sus formas abreviadas: `fl` o `ft`. Para obtener más información, ejecute el cmdlet `Get-Help Format-List`.

Transmitir parámetros por nombre

Puede transmitir parámetros por nombre en la mayoría de los casos y rodear los valores de parámetros que contienen espacios o caracteres especiales con comillas dobles.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

La mayoría de los ejemplos de la documentación *Instalación y configuración de vSphere* transmiten parámetros por nombre.

Transmitir parámetros como objetos

Puede transmitir parámetros como objetos si desea ejecutar scripts y automatización. Transmitir parámetros como objetos resulta útil con los cmdlets que devuelven varios objetos y con los cmdlets que devuelven un solo objeto. Tenga en cuenta el ejemplo siguiente:

- 1 Vincule a una variable el objeto que contiene la información de cumplimiento de normas de un conjunto de reglas para un host.

```
$tr = Test-DeployRuleSetCompliance MyEsxi42
```

- 2 Vea la propiedad `itemlist` del objeto para determinar la diferencia entre lo que contiene el conjunto de reglas y lo que usa el host actualmente.

```
$tr.itemlist
```

- 3 Corrija el host para que use el conjunto de reglas modificado, utilizando el cmdlet `Repair-DeployRuleSetCompliance` con la variable.

```
Repair-DeployRuleSetCompliance $tr
```

En este ejemplo, se corrige el host la próxima vez que se arranca.

Configurar licencias masivas

Puede utilizar vSphere Web Client o ESXi Shell para especificar claves de licencia individuales o configurar licencias masivas mediante los cmdlets de PowerCLI. Las licencias masivas funcionan para todos los hosts ESXi, pero son especialmente útiles para los hosts aprovisionados con Auto Deploy.

En el ejemplo siguiente, se asignan licencias a todos los hosts de un centro de datos. También puede asociar licencias con hosts y clústeres.

El ejemplo siguiente está destinado a usuarios avanzados de PowerCLI que saben cómo usar variables de PowerShell.

Requisitos previos

Instale PowerCLI. Consulte [Instalar vSphere PowerCLI y software de requisito previo](#).

La asignación de claves de licencia mediante vSphere Web Client y la asignación de licencias mediante los cmdlets de PowerCLI funcionan de manera diferente.

Asignación de claves de licencia mediante vSphere Web Client

Puede asignar claves de licencia a un host al agregar el host al sistema vCenter Server o cuando un sistema vCenter Server administra el host.

Asignación de claves de licencia mediante LicenseDataManager PowerCLI

Puede especificar un conjunto de claves de licencia para agregar a un conjunto de hosts. Las claves de licencia se agregan a la base de datos de vCenter Server. Cada vez que un host se agrega al sistema vCenter Server o vuelve a conectarse al sistema vCenter Server, se asigna una clave de licencia al host. Una clave de licencia que se asigna mediante PowerCLI se trata como una clave de licencia predeterminada. Cuando se agrega o se vuelve a conectar un host sin licencia, se le asigna la clave de licencia predeterminada. Si un host ya tiene licencia, mantiene su clave de licencia.

Procedimiento

- 1 Conecte el sistema vCenter Server que desea usar y vincule el gestor de licencias asociado a una variable.

```
Connect-VIServer -Server 192.XXX.X.XX -User username -Password password
$licenseDataManager = Get-LicenseDataManager
```

- 2 Ejecute un cmdlet que recupere el centro de datos en el que se encuentran los hosts para los cuales desea utilizar la característica de licencias masivas.

```
$hostContainer = Get-Datacenter -Name Datacenter-X
```

También puede ejecutar un cmdlet que recupere un clúster con la finalidad de utilizar licencias masivas para todos los hosts de un clúster, o que recupere una carpeta con la finalidad de utilizar licencias masivas para todos los hosts de una carpeta.

- 3 Cree un nuevo objeto `LicenseData` y un objeto `LicenseKeyEntry` con la clave de licencia y el identificador de tipo asociados.

```
$licenseData = New-Object VMware.VimAutomation.License.Types.LicenseData
$licenseKeyEntry = New-Object VMware.VimAutomation.License.Types.LicenseKeyEntry
$licenseKeyEntry.TypeId = "vmware-vsphere" $licenseKeyEntry.LicenseKey = "XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX"
```

- 4 Asocie el atributo `LicenseKeys` del objeto `LicenseData` que creó en el paso 3 con el objeto `LicenseKeyEntry`.

```
$licenseData.LicenseKeys += $licenseKeyEntry
```

- 5 Actualice los datos de licencias del centro de datos con el objeto `LicenseData` y compruebe que la licencia esté asociada con el contenedor de host.

```
$licenseDataManager.UpdateAssociatedLicenseData($hostContainer.Uid,
$licenseData) $licenseDataManager.QueryAssociatedLicenseData($hostContainer.Uid)
```

- 6 Aprovechone un host o más con Auto Deploy y asígnelos al centro de datos o al clúster al que le asignaron los datos de licencias.
- 7 Puede usar vSphere Web Client para verificar que el host se haya asignado correctamente a la licencia predeterminada `XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX`.

Resultados

Todos los hosts que se hayan asignado al centro de datos ahora cuentan con licencia de manera automática.

Administrar Auto Deploy con los cmdlets de PowerCLI

Puede usar los cmdlets de Auto Deploy PowerCLI para crear reglas que asocien los hosts con perfiles de imagen, perfiles de host y una ubicación en el destino de vCenter Server. También es posible actualizar los hosts mediante la comprobación del cumplimiento de normas y la corrección de los problemas de cumplimiento de normas que correspondan.

Asignar un perfil de imagen a hosts

Antes de que pueda aprovisionar un host, deberá crear reglas que asignen un perfil de imagen a cada host que desee aprovisionar con Auto Deploy.

Las reglas de extensibilidad de Auto Deploy obligan a que los VIB en el nivel `CommunitySupported` solo puedan contener archivos de determinadas ubicaciones predefinidas, como la ruta de complementos de ESXCLI, la ruta de complementos de jumpstart, etc. Si agrega un VIB que se encuentra en una ubicación diferente de la de un perfil de imagen, aparecerá una advertencia. Puede anular la advertencia utilizando la opción `force` (forzar).

Si realiza una llamada al cmdlet `New-DeployRule` en un perfil de imagen que incluye VIB en el nivel `CommunitySupported` que infrinja la regla, establezca `$DeployNoSignatureCheck = $true` antes de agregar el perfil de imagen. Con esta configuración, el sistema omitirá la validación de firma y no realizará la comprobación de reglas de extensibilidad.

Nota Los perfiles de imagen que incluyen VIB en el nivel `CommunitySupported` no se admiten en los sistemas de producción.

Requisitos previos

- Instale VMware PowerCLI y todo el software de requisito previo.
- Si encuentra problemas al ejecutar cmdlets de PowerCLI, considere cambiar la directiva de ejecución. Consulte [Usar los cmdlets de Auto Deploy](#).

Procedimiento

- 1 Ejecute el cmdlet de PowerCLI `Connect-VIServer` para realizar la conexión con el sistema vCenter Server al que está registrado Auto Deploy.

Connect-VIServer 192.XXX.X.XX

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

- 2 Determine la ubicación del almacén de software público o defina un perfil de imagen personalizado con Image Builder PowerCLI.

- 3 Ejecute `Add-EsxSoftwareDepot` para agregar el almacén de software que contiene el perfil de imagen a la sesión de PowerCLI.

Tipo de almacén	Cmdlet
Almacén remoto	Ejecute <code>Add-EsxSoftwareDepot depot_url</code> .
Archivo ZIP	<ol style="list-style-type: none"> Descargue el archivo ZIP en la ruta de acceso de archivo local. Ejecute <code>Add-EsxSoftwareDepot C:\file_path\my_offline_depot.zip</code>.

- 4 En el almacén, busque el perfil de imagen que desea utilizar ejecutando el cmdlet `Get-EsxImageProfile`.

De manera predeterminada, el almacén de ESXi incluye un perfil de imagen base que incluye VMware Tools y tiene la cadena `standard` en su nombre y un perfil de imagen base que no incluye VMware Tools.

- 5 Defina una regla en la que los hosts con determinados atributos, por ejemplo un rango de direcciones IP, estén asignados al perfil de imagen.

```
New-DeployRule -Name "testrule" -Item "My Profile25" -Pattern "vendor=Acme,Zven", "ipv4=192.XXX.1.10-192.XXX.1.20"
```

Si un nombre contiene espacios, se requieren comillas dobles. De lo contrario, es opcional. Especifique `-AllHosts` en lugar de un patrón para aplicar el elemento a todos los hosts.

El cmdlet crea una regla con el nombre `testrule`. La regla asigna el perfil de imagen con el nombre `My Profile25` a todos los hosts con un proveedor de Acme o Zven que también tienen una dirección IP en el rango especificado.

- 6 Agregue la regla al conjunto de reglas.

```
Add-DeployRule testrule
```

De manera predeterminada, la regla se agrega al conjunto de reglas en funcionamiento y al conjunto de reglas activo. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Resultados

Cuando el host arranca desde iPXE, informa de los atributos de la máquina a la consola. Utilice el mismo formato de los atributos al escribir reglas de implementación.

```
*****
* Booting through VMware AutoDeploy...
*
* Machine attributes:
* . asset=No Asset Tag
* . domain=vmware.com
* . hostname=myhost.mycompany.com
* . ipv4=XX.XX.XXX.XXX
* . mac=XX:XX:XX:XX:XX:XX
```

```
* . model=MyVendorModel
* . oemstring=Product ID: XXXXXX-XXX
* . serial=XX XX XX XX XX XX...
* . uuid=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
* . vendor=MyVendor
*****
```

Pasos siguientes

- Para los hosts que ya se han aprovisionado con Auto Deploy, realice la prueba de cumplimiento de normas y las operaciones de reparación con la finalidad de aprovisionarlos con el nuevo perfil de imagen. Consulte [Probar y reparar cumplimiento de reglas](#).
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de imagen.

Escribir una regla y asignar un perfil de host a hosts

Auto Deploy puede asignar un perfil de host a uno o más hosts. El perfil de host puede incluir información sobre la configuración de almacenamiento, la configuración de red u otras características del host. Si agrega un host a un clúster, se utiliza el perfil de host de ese clúster.

En muchos casos, puede asignar un host a un clúster en lugar de especificar un perfil de host explícitamente. El host utiliza el perfil de host del clúster.

Requisitos previos

- Instale vSphere PowerCLI y todas las herramientas de software que constituyan un requisito previo. Consulte [Instalar vSphere PowerCLI y software de requisito previo](#).
- Exporte el perfil de host que desea utilizar.

Procedimiento

- 1 Ejecute el cmdlet `Connect-VIServer` vSphere PowerCLI para conectarse con el sistema vCenter Server en el que está registrado Auto Deploy.

```
Connect-VIServer 192.XXX.X.XX
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

- 2 Con vSphere Web Client, configure un host con los parámetros que desee usar y cree un perfil de host a partir de él.
- 3 Busque el nombre del perfil de host mediante la ejecución del cmdlet `Get-VMhostProfile` de vSphere PowerCLI, pasando el host ESXi a partir del cual creó un perfil de host.
- 4 En el símbolo de vSphere PowerCLI, defina una regla en la que los perfiles de host se asignen a hosts con ciertos atributos; por ejemplo, un intervalo de direcciones IP.

```
New-DeployRule -Name "testrule2" -Item my_host_profile -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

El elemento especificado se asigna a todos los hosts que posean los atributos especificados. Este ejemplo especifica una regla denominada `testrule2`. Esta asigna el perfil de host especificado `my_host_profile` a todos los hosts que tengan una dirección IP dentro del intervalo especificado y cuyo fabricante sea Acme o Zven.

5 Agregue la regla al conjunto de reglas.

```
Add-DeployRule testrule2
```

De forma predeterminada, el conjunto de reglas en funcionamiento se convierte en el conjunto de reglas activo y los cambios en él se vuelven activos cuando agrega una regla. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Pasos siguientes

- Asigne un host ya aprovisionado con Auto Deploy al nuevo perfil de host. Para ello, realice operaciones de prueba de cumplimiento y reparación en esos hosts. Para obtener más información, consulte [Probar y reparar cumplimiento de reglas](#).
- Encienda los hosts no aprovisionados para aprovisionarlos con el perfil de host.

Escribir una regla y asignar un host a una carpeta o un clúster

Auto Deploy puede asignar un host a una carpeta o un clúster. Cuando el host arranca, Auto Deploy lo agrega a la ubicación que se especifica en vCenter Server. El host asignado a un clúster hereda el perfil de host del clúster.

Requisitos previos

- Instale vSphere PowerCLI y todo el software requerido previamente.
- Compruebe que la carpeta seleccionada esté en un centro de datos o clúster. No puede asignar el host a una carpeta de nivel superior independiente.

Procedimiento

- 1 Ejecute el cmdlet `Connect-VIServer` vSphere PowerCLI para conectarse con el sistema vCenter Server en el que está registrado Auto Deploy.

```
Connect-VIServer 192.XXX.X.XX
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no aparezca ninguna advertencia de certificados del servidor. En un entorno de desarrollo, puede omitir la advertencia.

- 2 Defina una regla en la que los hosts con ciertos atributos, por ejemplo, un rango de direcciones IP, se asignan a una carpeta o un clúster.

```
New-DeployRule -Name testrule3 -Item "my folder" -Pattern "vendor=Acme,Zven",  
"ipv4=192.XXX.1.10-192.XXX.1.20"
```


Este ejemplo pasa la carpeta por el nombre. En cambio, puede pasar una carpeta, un clúster o un objeto de centro de datos que recupere con el comando cmdlet `Get-Folder`, `Get-Cluster` o `Get-Datacenter`.

3 Agregue la regla al conjunto de reglas.

```
Add-DeployRule testrule3
```

De forma predeterminada, el conjunto de reglas en funcionamiento se convierte en el conjunto de reglas activo y los cambios en él se vuelven activos cuando agrega una regla. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Pasos siguientes

- Para asignar un host ya aprovisionado con Auto Deploy a la nueva ubicación de carpeta o clúster, realice una operación de cumplimiento de prueba y reparación. Consulte [Probar y reparar cumplimiento de reglas](#).
- Encienda los hosts no aprovisionados para agregarlos a la ubicación especificada de vCenter Server.

Probar y reparar cumplimiento de reglas

Cuando se agrega una regla al conjunto de reglas de Auto Deploy o cuando se realizan cambios en una regla o más, los hosts no se actualizan de manera automática. Auto Deploy aplica las reglas nuevas únicamente cuando se prueba el cumplimiento de reglas y se realizan las correcciones pertinentes.

Requisitos previos

- Instale vSphere PowerCLI y todas las herramientas de software que constituyan un requisito previo.
- Compruebe que la infraestructura incluya un host ESXi o más aprovisionado con Auto Deploy y que el host en el que ha instalado vSphere PowerCLI pueda acceder a esos hosts ESXi.

Procedimiento

- 1 Use vSphere PowerCLI para comprobar qué reglas de Auto Deploy están disponibles actualmente.

```
Get-DeployRule
```

El sistema devuelve las reglas y los patrones, y los elementos asociados.

- 2 Realice un cambio en una de las reglas disponibles.

Por ejemplo, puede cambiar el perfil de imagen y el nombre de la regla.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

No se puede editar una regla que ya se agregó a un conjunto de reglas. En lugar de ello, debe copiar la regla y reemplazar el elemento o el patrón que desea cambiar.

- 3 Compruebe que pueda acceder al host para el cual desea probar el cumplimiento del conjunto de reglas.

```
Get-VMHost -Name MyEsxi42
```

- 4 Ejecute el cmdlet que prueba el cumplimiento del conjunto de reglas para el host y vincule el valor devuelto a una variable para usarlo en otro momento.

```
$tr = Test-DeployRuleSetCompliance MyEsxi42
```

- 5 Examine las diferencias entre el contenido del conjunto de reglas y la configuración del host.

```
$tr.itemlist
```

El sistema devuelve una tabla de elementos actuales y esperados.

CurrentItem	ExpectedItem
-----	-----
My Profile 25MyProfileUpdate	

- 6 Corrija el host para que use el conjunto de reglas modificado la próxima vez que arranque.

```
Repair-DeployRuleSetCompliance $tr
```

Pasos siguientes

Si la regla que modificó ha especificado la ubicación en el inventario, el cambio se aplica cuando se corrigen los problemas de cumplimiento. Para todos los demás cambios, arranque el host para que Auto Deploy aplique la nueva regla y logre el cumplimiento entre el conjunto de reglas y el host.

Aprovisionar sistemas ESXi con vSphere Auto Deploy

vSphere Auto Deploy puede aprovisionar cientos de hosts físicos con el software ESXi. Se pueden aprovisionar los hosts que no ejecutaron previamente el software ESXi (primer arranque), así como reiniciar o reaprovisionar los hosts con un perfil de imagen, un perfil de host, una carpeta o una ubicación de clúster diferentes.

El proceso de Auto Deploy varía según el estado del host y según los cambios que desea realizar el usuario.

Aprovisionar un host (primer arranque)

Aprovisionar un host que nunca se aprovisionó con Auto Deploy (primer arranque) es una acción diferente a los procesos de arranque subsiguientes. Es necesario preparar el host y cumplir con todos los otros requisitos previos para poder aprovisionar el host. Puede definir opcionalmente un perfil de imagen personalizado con los cmdlets de Image Builder PowerCLI.

Requisitos previos

- Asegúrese de que el host cumpla con los requisitos de hardware para los hosts ESXi.
Consulte [Requisitos de hardware de ESXi](#).
- Prepare el sistema para vSphere Auto Deploy (consulte [Prepararse para vSphere Auto Deploy](#)).
- Escriba reglas para asignar un perfil de imagen al host, y asignar de forma opcional un perfil de host y una ubicación de vCenter Server al host. Consulte [Administrar Auto Deploy con los cmdlets de PowerCLI](#).

Cuando se complete la instalación, el servidor Auto Deploy y PowerCLI estarán instalados, la configuración de DHCP estará completada y las reglas para el host que desea aprovisionar se encontrarán en el conjunto de reglas activas.

Procedimiento

1 Encienda el host.

El host se comunica con el servidor DHCP y descarga iPXE desde la ubicación que el servidor indica. A continuación, el servidor Auto Deploy aprovisiona al host con la imagen especificada por el motor de reglas. El servidor Auto Deploy también puede aplicar un perfil de host al host si existe uno especificado en el conjunto de reglas. Por último, Auto Deploy agrega el host al sistema vCenter Server especificado en el conjunto de reglas.

- ### 2 (opcional) Si Auto Deploy aplica un perfil de host que requiere alguna entrada del usuario, como una dirección IP, el host se coloca en el modo de mantenimiento. Vuelva a aplicar el perfil de host con vSphere Web Client y proporcione las entradas del usuario cuando se solicite.

Resultados

Después de un proceso de primer arranque, el host se ejecuta y administra a través de un sistema vCenter Server. vCenter Server almacena el perfil de imagen, el perfil de host y la información de ubicación del host.

Ahora puede reiniciar el host según sea necesario. Cada vez que reinicie, el host se reaprovisionará a través del sistema vCenter Server.

Pasos siguientes

Reaprovisione los hosts según sea necesario. Consulte [Reaprovisionar hosts](#).

Si desea cambiar el perfil de imagen, el perfil de host o la ubicación del host, actualice las reglas, realice una prueba y repare la operación de cumplimiento. Consulte [Probar y reparar cumplimiento de reglas](#).

Reaprovisionar hosts

vSphere Auto Deploy admite varias opciones de reaprovisionamiento. Puede realizar un reinicio o un reaprovisionamiento sencillos con otro perfil de imagen o de host.

Para un primer arranque con Auto Deploy debe configurar el entorno y agregar reglas al conjunto de reglas. Consulte [Prepararse para vSphere Auto Deploy](#).

Están disponibles las siguientes operaciones de reaprovisionamiento.

- Reinicio simple.
- Reinicio de hosts sobre los que el usuario respondió preguntas durante la operación de arranque.
- Reaprovisionamiento con un perfil de imagen diferente.
- Reaprovisionamiento con un perfil de host diferente.

Reaprovisionar hosts con operaciones de reinicio simples

El reinicio simple de un host aprovisionado con Auto Deploy solo requiere que se sigan cumpliendo todos los requisitos previos. El proceso utiliza el perfil de imagen asignado previamente, el perfil de host y la ubicación de vCenter Server.

La tarea de configuración incluye configurar el servidor DHCP, escribir reglas y poner a disposición un perfil de imagen para la infraestructura de Auto Deploy.

Requisitos previos

Asegúrese de que la configuración que realizó durante la primera operación de arranque esté lista.

Procedimiento

- 1 Compruebe que el perfil de imagen y el perfil de host para el host sigan estando disponibles y que el host tenga la información de identificación (etiqueta de inventario, dirección IP) que tenía durante las operaciones de arranque anteriores.
- 2 Coloque el host en modo de mantenimiento.

Tipo de host	Acción
El host es parte de un clúster de DRS	VMware DRS migra las máquinas virtuales a los hosts adecuados cuando coloca el host en modo de mantenimiento.
El host no es parte de un clúster de DRS	Debe migrar todas las máquinas virtuales a distintos hosts y poner todos los hosts en modo de mantenimiento.

- 3 Reinicie el host.

Resultados

El host se apaga. Al reiniciarse, el host utiliza el perfil de imagen que proporciona el servidor Auto Deploy. El servidor Auto Deploy también aplica el perfil de host almacenado en el sistema vCenter Server.

Reaprovisionar un host con un nuevo perfil de imagen

Puede reaprovisionar el host con un nuevo perfil de imagen, un perfil de host o una ubicación de vCenter Server si modifica la regla para el host y realiza una operación de cumplimiento de prueba y reparación.

Existen varias opciones para reaprovisionar hosts.

- Si los VIB que desea usar son compatibles con la actualización directa, puede usar un comando `esxcli software vib`. En ese caso, también debe actualizar el conjunto de reglas que se va a usar en un perfil de imagen que incluya los nuevos VIB.
- Durante las pruebas, puede aplicar un perfil de imagen a un host individual con el cmdlet `Apply-EsxImageProfile` y reiniciar el host para que el cambio sea efectivo. El cmdlet `Apply-EsxImageProfile` actualiza la asociación entre el host y el perfil de imagen, pero no instala ningún VIB en el host.
- En todos los demás casos, utilice este procedimiento.

Requisitos previos

- Cree el perfil de imagen con el que desea arrancar el host. Use Image Builder PowerCLI, como se describe en [Usar vSphere ESXi Image Builder](#).
- Asegúrese de que la configuración que realizó durante la primera operación de arranque esté lista.

Procedimiento

- 1 En el símbolo de PowerShell, ejecute el cmdlet `Connect-VIServer` de PowerCLI para conectarse con el sistema vCenter Server en el que está registrado Auto Deploy.

Connect-VIServer myVCServer

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

- 2 Determine la ubicación de un almacén de software público que contenga el perfil de imagen que desea utilizar o defina un perfil de imagen personalizado con Image Builder PowerCLI.
- 3 Ejecute `Add-EsxSoftwareDepot` para agregar el almacén de software que contiene el perfil de imagen a la sesión de PowerCLI.

Tipo de almacén	Cmdlet
Almacén remoto	Ejecute <code>Add-EsxSoftwareDepot depot_url</code> .
Archivo ZIP	<ol style="list-style-type: none"> a Descargue el archivo ZIP a una ruta de acceso de archivos local o cree un punto de montaje local en el equipo de PowerCLI. b Ejecute <code>Add-EsxSoftwareDepot C:\file_path\my_offline_depot.zip</code>.

- 4 Ejecute `Get-EsxImageProfile` para ver una lista de perfiles de imagen y determine qué perfil desea utilizar.
- 5 Ejecute `Copy-DeployRule` y especifique el parámetro `ReplaceItem` para cambiar la regla que asigna un perfil de imagen a hosts.

El siguiente cmdlet reemplaza el perfil de imagen actual que la regla asigna al host con el perfil *my_new_imageprofile*. Cuando el cmdlet finaliza, *myrule* asigna el nuevo perfil de imagen a los hosts. Se cambia el nombre de la antigua versión de *myrule* y se la oculta.

`Copy-DeployRule myrule -ReplaceItem my_new_imageprofile`

- 6 Pruebe y repare el cumplimiento de reglas para cada host en el que desee implementar la imagen.

Consulte [Probar y reparar cumplimiento de reglas](#) .

Resultados

Al reiniciar los hosts tras una reparación del cumplimiento, Auto Deploy reaprovisiona los hosts con el nuevo perfil de imagen.

Actualizar la personalización de hosts en vSphere Web Client

Si un host requería la intervención del usuario durante un arranque anterior, las respuestas estarán guardadas con vCenter Server. Si desea solicitar información nueva al usuario, debe corregir el host.

Requisitos previos

Conecte un perfil de host que solicite entrada de datos del usuario en el host.

Procedimiento

- 1 Migre todas las máquinas virtuales a distintos hosts y ponga el host en modo de mantenimiento.

Tipo de host	Acción
El host es parte de un clúster de DRS	VMware DRS migra las máquinas virtuales a los hosts adecuados cuando coloca el host en modo de mantenimiento.
El host no es parte de un clúster de DRS	Debe migrar todas las máquinas virtuales a distintos hosts y poner todos los hosts en modo de mantenimiento.

- 2 En vSphere Web Client, haga clic con el botón derecho en el host y seleccione **Todas las acciones de vCenter > Perfiles de host > Corregir** para corregir el host.
- 3 Cuando se le solicite, proporcione la entrada de datos del usuario.
Ahora, puede hacer que el host salga del modo de mantenimiento.

Resultados

Se guarda la personalización del host. En el próximo arranque, se aplicará la personalización del host.

Usar Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado

La característica de almacenamiento en caché sin estado de Auto Deploy permite almacenar la imagen del host en la memoria caché. La característica de instalaciones con estado de Auto Deploy permite instalar hosts por medio de la red. Después del primer arranque de red, estos hosts arrancan como cualquier otro host ESXi.

La solución de almacenamiento en caché sin estado está destinada principalmente a las situaciones en las que varios hosts arrancan en simultáneo. La imagen almacenada en la memoria caché local ayuda a prevenir un cuello de botella que se produce si cientos de hosts se conectan simultáneamente al servidor Auto Deploy. Una vez finalizada la operación de arranque, los hosts se conectan a Auto Deploy para completar la configuración.

La característica de instalaciones con estado permite aprovisionar hosts con el perfil de imagen por medio de la red sin necesidad de configurar la infraestructura de arranque PXE.

- [Introducción a almacenamiento en caché sin estado e instalaciones con estado](#)
Es posible usar el perfil de host de Configuración de la memoria caché del sistema para aprovisionar hosts con almacenamiento en caché sin estado e instalaciones con estado de Auto Deploy.
- [Descripción general de las instalaciones con estado y el almacenamiento en caché sin estado](#)
Cuando desee utilizar Auto Deploy con almacenamiento en caché sin estado o con instalaciones con estado, deberá configurar un perfil de host, aplicar dicho perfil y establecer el orden de arranque.
- [Configurar hosts sin estado para utilizar Auto Deploy con almacenamiento en caché](#)
Puede configurar su sistema para aprovisionar hosts con Auto Deploy y configurar los hosts para utilizar el almacenamiento en caché sin estado. Si el servidor Auto Deploy no está disponible cuando se reinicia un host, el host utiliza la imagen almacenada en caché.
- [Habilitar instalaciones con estado para hosts aprovisionados con Auto Deploy](#)
Puede configurar hosts aprovisionados con Auto Deploy para almacenar en caché la imagen en el disco y usar la imagen almacenada en la memoria caché para los arranques posteriores. Después de que la imagen se almacena en la memoria caché, los hosts actúan como hosts en los cuales está instalada una imagen.

Introducción a almacenamiento en caché sin estado e instalaciones con estado

Es posible usar el perfil de host de Configuración de la memoria caché del sistema para aprovisionar hosts con almacenamiento en caché sin estado e instalaciones con estado de Auto Deploy.

Ejemplos de almacenamiento en caché sin estado e instalaciones con estado

Hosts aprovisionados con Auto Deploy que almacenan en caché la imagen (almacenamiento en caché sin estado)

Configure y aplique un perfil de host para el almacenamiento en caché sin estado. Puede almacenar la imagen en la memoria caché de un disco local, un disco remoto o una unidad USB. Continúe aprovisionando este host con Auto Deploy. Si el servidor Auto Deploy no está disponible, por ejemplo, debido a que cientos de hosts intentan acceder a él de forma simultánea, el host arranca desde la memoria caché. Después de la operación de arranque, el host intenta comunicarse con el servidor Auto Deploy para completar la configuración.

Los hosts aprovisionados con Auto Deploy se convierten en hosts con estado

Configure y aplique un perfil de host para instalaciones con estado. Cuando aprovisiona un host con Auto Deploy, la imagen se instala en el disco local, un disco remoto o una unidad USB. Para arranques posteriores, hágalo desde el disco. El host ya no usa Auto Deploy.

Preparar

Para usar correctamente el almacenamiento en caché sin estado o instalaciones con estado, debe decidir cómo configurar el sistema y establecer el orden de arranque.

Tabla 4-7. Preparar almacenamiento en caché sin estado o instalaciones con estado

Requisito o decisión	Descripción
Decidir sobre la sobrescritura de la partición de VMFS	<p>Cuando instale ESXi mediante el instalador interactivo, se le consulta si desea sobrescribir un almacén de datos existente de VMFS. El perfil de host de Configuración de la memoria caché del sistema proporciona una opción para sobrescribir particiones existentes de VMFS.</p> <p>La opción no está disponible si configura el perfil de host para que use una unidad USB.</p>
Decidir si se necesita un entorno de alta disponibilidad	<p>Si usa Auto Deploy con almacenamiento en caché sin estado, puede configurar un entorno de Auto Deploy de alta disponibilidad para garantizar que las máquinas virtuales migren a hosts aprovisionados recientemente y que el entorno admita vNetwork Distributed Switch incluso si el sistema vCenter Server queda temporalmente no disponible.</p>
Establecer el orden de arranque	<p>El orden de arranque que especifica para los hosts depende de la característica que desea usar.</p> <ul style="list-style-type: none"> ■ Para configurar Auto Deploy con almacenamiento en caché sin estado, configure el host para que primero intente arrancar desde la red y, luego, intente arrancar desde el disco. Si el servidor Auto Deploy no está disponible, el host arranca usando la memoria caché. ■ Para configurar Auto Deploy para instalaciones con estado en hosts que actualmente no tienen un disco de arranque, configure sus hosts para que primero intenten arrancar desde el disco y, luego, intenten hacerlo desde la red. <p>Nota Si actualmente tiene una imagen de arranque en el disco, configure los hosts para un arranque PXE único y aprovisiona el host con Auto Deploy para que use un perfil de host que especifique instalaciones con estado.</p>

Almacenamiento en caché sin estado y pérdida de conectividad

Si los hosts ESXi que se ejecutan en las máquinas virtuales pierden conectividad con el servidor Auto Deploy, el sistema vCenter Server, o ambos, se aplican algunas limitaciones la próxima vez que reinicie el host.

- Si vCenter Server está disponible, pero el servidor Auto Deploy no está disponible, los hosts no se conectan al sistema vCenter Server de forma automática. Puede conectar manualmente los hosts a vCenter Server o esperar hasta que el servidor Auto Deploy vuelva a estar disponible.
- Si tanto vCenter Server como Auto Deploy no están disponibles, puede conectarse a cada host ESXi mediante vSphere Client y agregar máquinas virtuales a cada host.

- Si vCenter Server no está disponible, vSphere DRS no funciona. El servidor Auto Deploy no puede agregar hosts a vCenter Server. Puede conectarse a cada host ESXi mediante vSphere Client y agregar máquinas virtuales a cada host.
- Si realiza cambios a la configuración mientras está perdida la conectividad, los cambios se pierden cuando se restaura la conexión del servidor Auto Deploy.

Descripción general de las instalaciones con estado y el almacenamiento en caché sin estado

Cuando desee utilizar Auto Deploy con almacenamiento en caché sin estado o con instalaciones con estado, deberá configurar un perfil de host, aplicar dicho perfil y establecer el orden de arranque.

Cuando se aplica un perfil de host que permite el almacenamiento en caché en un host, Auto Deploy particiona el disco especificado. Lo que ocurre después depende de la forma en que configure el perfil de host y establezca el orden de arranque en el host.

- Si se ha seleccionado **Habilitar almacenamiento en caché sin estado en el host** en el perfil del host de configuración de caché del sistema, Auto Deploy almacenará la imagen en caché cuando aplique el perfil de host. No se requiere reiniciar. Cuando reinicie más tarde, el host continuará utilizando la infraestructura de Auto Deploy para recuperar su imagen. Si el servidor Auto Deploy no está disponible, el host utiliza la imagen almacenada en caché.
- Auto Deploy instala la imagen si **Habilitar instalaciones con estado en el host** está seleccionado en el perfil de host de configuración de caché del sistema. Cuando reinicie, el host arrancará desde el disco, al igual que un host que se haya aprovisionado con el instalador. Auto Deploy ya no realiza el aprovisionamiento del host.

Puede aplicar el perfil de host desde vSphere Web Client o escribir una regla de PowerCLI de Auto Deploy que aplique el perfil de host.

Usar vSphere Web Client para configurar Auto Deploy para el almacenamiento en caché con estado o las instalaciones sin estado

Puede crear un perfil de host en un host de referencia y aplicar dicho perfil de host a hosts adicionales, o a una carpeta o clúster de vCenter Server. Aparece el siguiente flujo de trabajo.

- 1 Aprovisiona un host con Auto Deploy y edita el perfil de host de configuración de caché de imagen del sistema del host.
- 2 Coloque uno más hosts de destino en el modo de mantenimiento, aplique el perfil de host a cada host e indique al host que salga del modo de mantenimiento.
- 3 Lo que ocurra después depende del perfil de host seleccionado.
 - Si el perfil de host habilitó el almacenamiento en caché sin estado, la imagen se almacenará en caché en el disco. No se requiere reiniciar.
 - Si el perfil de host habilitó las instalaciones con estado, se instalará la imagen. Cuando reinicie, el host utilizará la imagen instalada.
- 4 Se requiere un reinicio para que los cambios surtan efecto.

Usar PowerCLI para configurar Auto Deploy para el almacenamiento en caché con estado o las instalaciones sin estado

Puede crear un perfil de host para un host de referencia y escribir una regla de PowerCLI de Auto Deploy que aplique dicho perfil de host a otros hosts de destino. Aparece el siguiente flujo de trabajo.

- 1 Aprovechone una referencia con Auto Deploy y cree un perfil de host para habilitar una forma de almacenamiento en caché.
- 2 Escriba una regla que aproveche hosts adicionales con Auto Deploy y que aplique el perfil de host de referencia a otros hosts.
- 3 Auto Deploy aprovisiona cada host con el perfil de imagen nuevo. El efecto exacto de aplicar el perfil de host depende del perfil del host seleccionado.
 - En el caso de instalaciones con estado, Auto Deploy procederá de la siguiente manera:
 - Durante el primer arranque, Auto Deploy instala la imagen en el host.
 - Durante los arranques siguientes, el host arranca desde el disco. Auto Deploy ya no está involucrado.
 - En el caso del almacenamiento en caché sin estado, Auto Deploy procederá de la siguiente manera:
 - Durante el primer arranque, Auto Deploy aprovisiona el host y almacena la imagen en caché.
 - Durante los arranques siguientes, Auto Deploy aprovisiona el host. Si Auto Deploy no está disponible, el host arranca desde la imagen almacenada en caché. Sin embargo, la configuración solo puede completarse cuando el host puede llegar al servidor Auto Deploy.

Configurar hosts sin estado para utilizar Auto Deploy con almacenamiento en caché

Puede configurar su sistema para aprovisionar hosts con Auto Deploy y configurar los hosts para utilizar el almacenamiento en caché sin estado. Si el servidor Auto Deploy no está disponible cuando se reinicia un host, el host utiliza la imagen almacenada en caché.

Un host que se configura para el almacenamiento en caché sin estado utiliza solo la imagen almacenada en caché si el servidor Auto Deploy no está disponible cuando se reinicia el host. En todas las otras situaciones, el host se aprovisiona con Auto Deploy. Si cambia la regla que se aplica a un perfil de imagen del host y realiza una operación de cumplimiento de prueba y reparación, Auto Deploy aprovisiona el host con la imagen nueva y la imagen nueva se almacena en caché.

Configure una infraestructura de Auto Deploy de alta disponibilidad para garantizar que las máquinas virtuales se migren al host si se reinicia el host. Debido a que vCenter Server asigna máquinas virtuales al host, vCenter Server deberá estar disponible. Consulte [Configurar la infraestructura de vSphere Auto Deploy de alta disponibilidad](#).

Puede configurar su entorno para el almacenamiento en caché sin estado aplicando perfiles de host directamente o mediante la utilización de reglas de PowerCLI.

Tabla 4-8. Configurar hosts para el almacenamiento en caché sin estado o instalaciones con estado

Flujo de trabajo	Almacenamiento en caché sin estado	Instalación con estado
Aplicación directa del perfil de host	Aplique el perfil de host a hosts individuales o a todos los hosts de una carpeta o clúster. Consulte Configurar un perfil de host para utilizar el almacenamiento en caché sin estado .	Aplique el perfil de host a hosts individuales o a todos los hosts de una carpeta o clúster. Consulte Configurar un perfil de host para habilitar instalaciones con estado .
Escritura y aplicación de reglas de PowerCLI	Configure un host de referencia con un perfil de host que posea la configuración de almacenamiento en caché que desea. Escriba una regla de PowerCLI de Auto Deploy que aprovisione el host y que aplique un perfil de host que esté configurado para el almacenamiento en caché sin estado. Consulte Escribir una regla y asignar un perfil de host a hosts .	Configure un host de referencia con un perfil de host que posea la configuración de almacenamiento en caché que desea. Escriba una regla de PowerCLI de Auto Deploy que aprovisione el host y que aplique un perfil de host que esté configurado para las instalaciones con estado. Consulte Escribir una regla y asignar un perfil de host a hosts .

Prepararse para Auto Deploy con almacenamiento en caché sin estado

Antes de comenzar a aprovisionar un host que utiliza almacenamiento en caché sin estado con Auto Deploy, debe comprobar que el entorno esté configurado para Auto Deploy, preparar reglas de PowerCLI de Auto Deploy y establecer el orden de arranque para el host.

Requisitos previos

- Decida qué disco desea utilizar para almacenamiento en caché y determine si el proceso de almacenamiento en caché sobrescribirá una partición de VMFS existente.
- En entornos de producción, incluya el sistema vCenter Server y el servidor Auto Deploy en un entorno altamente disponible para protegerlos. Tener vCenter Server en un clúster de administración garantiza que VDS y la migración de máquinas virtuales estén disponibles. De ser posible, proteja otros elementos de la infraestructura. Consulte [Configurar la infraestructura de vSphere Auto Deploy de alta disponibilidad](#).

Procedimiento

- 1 Configure el entorno para Auto Deploy e instale PowerCLI.
Consulte [Prepararse para vSphere Auto Deploy](#).
- 2 Compruebe que haya un disco con al menos 1 GB de espacio libre disponible.
Si el disco aún no está particionado, este procedimiento se lleva a cabo cuando aplica el perfil de host.

- 3 Configure el host para que primero intente realizar un arranque de red y, si es incorrecto, que arranque desde un disco.

Consulte la documentación del proveedor de hardware.

Pasos siguientes

Configure un perfil de host para almacenamiento en caché sin estado. En la mayoría de los casos, puede crear el perfil de host en un host de referencia y aplicar ese perfil a otros hosts.

Configurar un perfil de host para utilizar el almacenamiento en caché sin estado

Si se configura un host para utilizar el almacenamiento en caché sin estado, este utiliza una imagen en caché cuando el servidor Auto Deploy no está disponible. Para utilizar el almacenamiento en caché sin estado, debe configurar un perfil de host. Puede aplicar ese perfil a otros hosts que desee configurar para el almacenamiento en caché sin estado.

Puede configurar el perfil de host en un único host que desee configurar para que use el almacenamiento en caché. También puede crear un perfil de host que use el almacenamiento en caché en un host de referencia y aplicar ese perfil de host a otros hosts.

Requisitos previos

Prepare el host para el almacenamiento en caché sin estado. Consulte [Prepararse para Auto Deploy con almacenamiento en caché sin estado](#).

Procedimiento

- 1 En vSphere Web Client, cree un perfil de host.
Consulte la documentación sobre *Host Profiles*.
- 2 Seleccione el perfil de host y haga clic en **Editar perfil de host**.
- 3 Conserve el nombre y la descripción, y haga clic en **Siguiente**.
- 4 Haga clic en **Opciones de configuración avanzadas** y, a continuación, en la carpeta **Configuración de caché de imagen del sistema**.
- 5 Haga clic en el icono **Configuración de caché de imagen del sistema**.
- 6 Seleccione la opción que desee en el menú desplegable Configuración de perfil de caché de imagen del sistema.

Opción	Descripción
Habilitar almacenamiento en caché sin estado en el host	Almacena en caché la imagen en el disco.
Habilitar almacenamiento en caché sin estado en un disco USB del host	Almacena en caché la imagen en un disco USB asociado al host.

- 7 Si seleccionó **Habilitar almacenamiento en caché sin estado en el host**, especifique la información sobre el disco que se va a utilizar.

Opción	Descripción
Argumentos para el primer disco	<p>De forma predeterminada, el sistema intenta reemplazar una instalación de ESXi existente y, a continuación, intenta escribir en el disco local.</p> <p>Puede utilizar el campo Argumentos para primer disco para especificar una lista separada por comas de los discos que se van a utilizar, en orden de preferencia. Puede especificar más de un disco. Utilice esx para el primer disco que tenga ESX instalado, use la información del modelo y del proveedor, o bien especifique el nombre del controlador de dispositivos vmkernel. Por ejemplo, para que el sistema busque primero un disco con el nombre de modelo ST3120814A, segundo cualquier disco que utilice el controlador mptsas y tercero el disco local, especifique ST3120814A,mptsas,local como el valor para el campo.</p> <p>La primera configuración de disco del perfil de host especifica el orden de búsqueda para determinar qué disco se va a usar para la memoria caché. El orden de búsqueda se especifica como una lista de valores delimitados por comas. El valor predeterminado esx,local especifica que Auto Deploy debe buscar primero un disco de memoria caché existente. El disco de memoria caché se identifica como un disco con la imagen del software ESXi existente. Si Auto Deploy no puede encontrar un disco de memoria caché existente, busca un dispositivo de disco local disponible. Al buscar un disco disponible, Auto Deploy usa el primer disco vacío que no tenga una partición de VMFS existente.</p> <p>Puede utilizar el primer argumento de disco solo para especificar el orden de búsqueda. No puede especificar un disco explícitamente. Por ejemplo, no puede especificar un determinado LUN o una SAN.</p>
Marcar para sobrescribir los volúmenes VMFS en el disco seleccionado	<p>Si marca esta casilla, el sistema sobrescribe los volúmenes VMFS existentes cuando no hay suficiente espacio disponible para almacenar la imagen, el perfil de imagen y el perfil de host.</p>

- 8 Haga clic en **Finalizar** para completar la configuración del perfil de host.
- 9 Aplique el perfil de host con vSphere Web Client o vSphere PowerCLI.

Opción	Descripción
vSphere Web Client	Use la interfaz de Host Profiles de vSphere Web Client. Consulte la documentación sobre <i>Host Profiles</i> .
vSphere PowerCLI	Consulte Escribir una regla y asignar un perfil de host a hosts .

Habilitar instalaciones con estado para hosts aprovisionados con Auto Deploy

Puede configurar hosts aprovisionados con Auto Deploy para almacenar en caché la imagen en el disco y usar la imagen almacenada en la memoria caché para los arranques posteriores. Después de que la imagen se almacena en la memoria caché, los hosts actúan como hosts en los cuales está instalada una imagen.

Preparar los hosts aprovisionados con Auto Deploy para instalaciones con estado

En algunas situaciones, puede resultar útil aprovisionar los hosts con Auto Deploy y realizar todos los arranques siguientes desde el disco. Este enfoque se conoce como “instalaciones con estado”.

Requisitos previos

Decida qué disco desea usar para almacenar la imagen y determine si la nueva imagen sobrescribirá una partición actual de VMFS.

Procedimiento

- 1 Configure el entorno para Auto Deploy e instale PowerCLI.
Consulte [Prepararse para vSphere Auto Deploy](#).
- 2 Compruebe que haya un disco con al menos 1 GB de espacio libre disponible.
Si el disco no se ha particionado, el particionamiento se efectúa al aplicar el perfil de host.
- 3 Configure el host para arrancar desde el disco.
Consulte la documentación del proveedor de hardware.

Configurar un perfil de host para habilitar instalaciones con estado

Si desea configurar un host aprovisionado con Auto Deploy para que arranque desde el disco, debe configurar un perfil de host. Es posible aplicar ese perfil de host a otros hosts que desee configurar para instalaciones con estado.

Puede configurar el perfil de host en un único host. También puede crear un perfil de host en un host de referencia y aplicarlo a otros hosts.

Requisitos previos

Asegúrese de que el host esté configurado para Auto Deploy y de cumplir con los demás requisitos previos de las instalaciones con estado. Consulte [Preparar los hosts aprovisionados con Auto Deploy para instalaciones con estado](#).

Procedimiento

- 1 En vSphere Web Client, cree un perfil de host.
Consulte la documentación sobre *Host Profiles*.
- 2 Con el objeto del perfil de host visible, haga clic en el icono Editar configuración del perfil de host.
- 3 Conserve el nombre y la descripción, y haga clic en **Siguiente**.
- 4 Haga clic en **Opciones de configuración avanzadas** y, a continuación, en la carpeta **Configuración de caché de imagen del sistema**.
- 5 Haga clic en el icono **Configuración de caché de imagen del sistema**.

- 6 Seleccione la opción que desee en el menú desplegable Configuración de perfil de caché de imagen del sistema.

Opción	Descripción
Habilitar instalaciones con estado en el host	Almacena la imagen en la memoria caché, en un disco.
Habilitar instalaciones con estado en un disco USB del host	Almacena en caché la imagen en un disco USB asociado al host.

- 7 Si selecciona la opción **Habilitar instalaciones con estado en el host**, especifique la información del disco que va a usar.

Opción	Descripción
Argumentos para el primer disco	<p>De forma predeterminada, el sistema intenta reemplazar una instalación de ESXi existente y, a continuación, intenta escribir en el disco local.</p> <p>Puede utilizar el campo Argumentos para primer disco para especificar una lista separada por comas de los discos que se van a utilizar, en orden de preferencia. Puede especificar más de un disco. Utilice esx para el primer disco que tenga ESX instalado, use la información del modelo y del proveedor, o bien especifique el nombre del controlador de dispositivos vmkernel. Por ejemplo, para que el sistema busque primero un disco con el nombre de modelo ST3120814A, segundo cualquier disco que utilice el controlador mptsas y tercero el disco local, especifique ST3120814A,mptsas,local como el valor para el campo.</p> <p>La primera configuración de disco del perfil de host especifica el orden de búsqueda para determinar qué disco se va a usar para la memoria caché. El orden de búsqueda se especifica como una lista de valores delimitados por comas. El valor predeterminado esx,local especifica que Auto Deploy debe buscar primero un disco de memoria caché existente. El disco de memoria caché se identifica como un disco con la imagen del software ESXi existente. Si Auto Deploy no puede encontrar un disco de memoria caché existente, busca un dispositivo de disco local disponible. Al buscar un disco disponible, Auto Deploy usa el primer disco vacío que no tenga una partición de VMFS existente.</p> <p>Puede utilizar el primer argumento de disco solo para especificar el orden de búsqueda. No puede especificar un disco explícitamente. Por ejemplo, no puede especificar un determinado LUN o una SAN.</p>
Marcar para sobrescribir los volúmenes VMFS en el disco seleccionado	Si marca esta casilla, el sistema sobrescribe los volúmenes VMFS existentes cuando no hay suficiente espacio disponible para almacenar la imagen, el perfil de imagen y el perfil de host.

- 8 Haga clic en **Finalizar** para completar la configuración del perfil de host.

9 Aplique el perfil de host con vSphere Web Client o vSphere PowerCLI.

Opción	Descripción
vSphere Web Client	Para aplicar el perfil de host en hosts individuales, use la interfaz de perfiles de host de vSphere Web Client. Consulte la documentación sobre <i>Host Profiles</i> .
vSphere PowerCLI	Para aplicar el perfil de host en un host o más mediante PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts .

Configurar un host de referencia de Auto Deploy

En un entorno donde no se almacena ningún estado en el host, un host de referencia ayuda a configurar varios hosts con la misma configuración. Puede configurar el host de referencia con generación de registros, volcado de memoria y otra configuración que desea, guardar el perfil de host y escribir una regla que aplique el perfil de host a otros hosts según sea necesario.

Puede ajustar la configuración de almacenamiento, conexión de redes y seguridad en el host de referencia y configurar servicios, como syslog y NTP.

Información sobre la configuración del host de referencia

Un host de referencia bien diseñado se conecta con todos los servicios, como syslog, NTP, etc. La configuración del host de referencia también podría incluir seguridad, almacenamiento, conexión de redes y ESXi Dump Collector. Puede aplicar la configuración de dicho host a otros hosts a través de los perfiles de host.

La configuración exacta de su host de referencia depende de su entorno, pero podría considerar la siguiente personalización.

Configuración de servidor NTP

Al recopilar información de generación de registros en entornos grandes, deberá asegurarse que las horas de los registros se encuentren coordinadas. Configure el host de referencia para utilizar el servidor NTP en su entorno que todos los hosts puedan compartir. Puede especificar un servidor NTP ejecutando el comando `vicfg-ntp`. Puede iniciar y detener el servicio NTP para un host con el comando `vicfg-ntp` o con vSphere Client.

Configuración del servidor de syslog

Todos los hosts ESXi ejecutan un servicio de Syslog (`vm syslogd`), que registra mensajes desde VMkernel y otros componentes del sistema en un archivo. Puede especificar el host de registro y administrar la ubicación, rotación, tamaño y otros archivos del registro ejecutando el comando de vCLI `esxcli system syslog` o a través de vSphere Client. La configuración de la generación de registros en un host remoto es especialmente importante para los hosts aprovisionados con vSphere Auto Deploy que no poseen almacenamiento local. Puede instalar opcionalmente vSphere Syslog Collector para recopilar registros de todos los hosts.

Configuración de volcados de memoria

Puede configurar su host de referencia para enviar volcados de memoria a un LUN SAN compartido o puede instalar ESXi Dump Collector en su entorno y configurar el host de referencia para utilizar ESXi Dump Collector. Consulte [Configurar ESXi Dump Collector con ESXCLI](#) . Puede instalar ESXi Dump Collector a través del medio de instalación de vCenter Server o utilizar ESXi Dump Collector que se incluye en vCenter Server Appliance. Después de que se complete la configuración, la memoria de VMkernel se envía al servidor de red especificado cuando el sistema encuentra un error crítico.

Configuración de seguridad

En la mayoría de las implementaciones, todos los hosts que aprovisiona con vSphere Auto Deploy deberán tener la misma configuración de seguridad. Puede, por ejemplo, configurar el firewall para que permita el acceso de determinados servicios al sistema de ESXi, establecer la configuración de seguridad, la configuración de usuario y la configuración del grupo de usuarios para el host de referencia con los comandos vCLI o vSphere Client. La configuración de seguridad incluye la configuración compartida de acceso de usuarios para todos los hosts. Puede lograr un acceso de usuarios unificado mediante la configuración de su host de referencia para la utilización de Active Directory. Consulte la documentación sobre *seguridad de vSphere*.

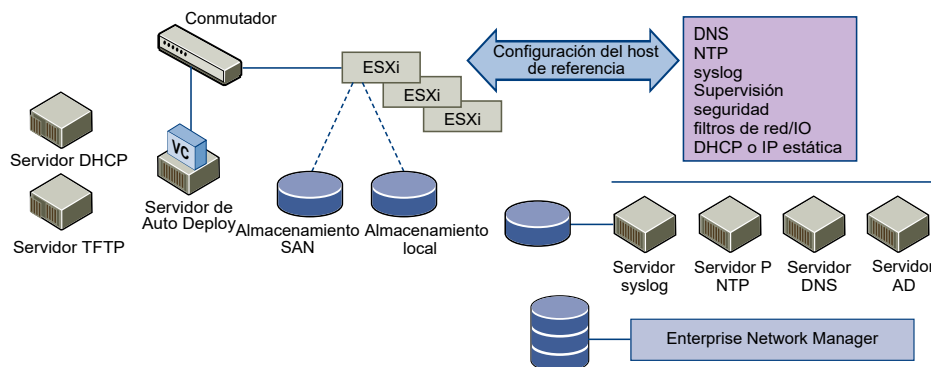
Nota Si configura Active Directory utilizando perfiles de host, las contraseñas no poseen protección. Utilice vSphere Authentication Service para configurar Active Directory para evitar la exposición de la contraseña de Active Directory.

Configuración de conexión de redes y almacenamiento

Si reserva un conjunto de recursos de conexión de redes y almacenamiento para la utilización por parte de los hosts aprovisionados con vSphere Auto Deploy, puede configurar su host de referencia para utilizar dichos recursos.

En implementaciones muy grandes, la configuración del host de referencia admite un Enterprise Network Manager, que recolecta toda la información proveniente de diferentes servicios de supervisión que se ejecutan en su entorno.

Figura 4-4. Configurar el host de referencia con vSphere Auto Deploy



[Configurar un host de referencia de Auto Deploy](#) explica cómo realizar esta configuración.

Vea el vídeo Hosts de referencia con Auto Deploy para obtener información sobre la configuración del host de referencia:



Configurar los hosts de referencia con vSphere Auto Deploy

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_fpu1jo7j/uiConfId/49694343/)

Configurar un host de referencia de Auto Deploy

vSphere permite configurar un host de referencia a través de vSphere Web Client, vCLI o los perfiles de host.

Para configurar un host de referencia, puede utilizar el enfoque que mejor se adapte a sus necesidades.

vSphere Web Client

vSphere Web Client admite la configuración de la conexión de red, almacenamiento, seguridad y muchos otros aspectos de un host ESXi. Configure su entorno y cree un perfil de host desde el host de referencia para la utilización por parte de Auto Deploy.

vSphere Command-Line Interface

Puede utilizar los comandos vCLI para configurar varios aspectos de su host. vCLI es adecuado para la configuración de muchos de los servicios del entorno de vSphere. Los comandos incluyen `vicfg-ntp` (configuración de un servidor NTP), `esxcli system syslog` (configuración de un servidor de syslog) y `esxcli network route` (agregado de rutas y configuración de la ruta predeterminada). Consulte [Configurar ESXi Dump Collector con ESXCLI](#).

Interfaz de Host Profiles

La práctica recomendada es configurar un host con vSphere Web Client o vCLI y crear un perfil de host desde dicho host. O, en cambio, puede utilizar la interfaz Perfiles del host en vSphere Web Client y guardar dicho perfil de host. Consulte [Configurar Host Profiles para un host de referencia de Auto Deploy con vSphere Web Client](#).

Configurar ESXi Dump Collector con ESXCLI

Un volcado de núcleo es el estado de la memoria de trabajo en caso de que se produzca un error en el host. De forma predeterminada, los volcados de núcleos se guardan en el disco local. Puede usar ESXi Dump Collector para mantener los volcados de núcleos en un servidor de red con la finalidad de usarlos durante las operaciones de depuración. ESXi Dump Collector es especialmente útil para Auto Deploy, pero es compatible con cualquier host ESXi. ESXi Dump Collector es compatible con otras opciones de personalización, incluido el envío de volcados de núcleos al disco local.

Si va a usar IPv6 y el host ESXi y ESXi Dump Collector se encuentran en el mismo vínculo local, ambos pueden usar direcciones IPv6 de vínculo de alcance local o direcciones IPv6 de alcance global.

Si va a usar IPv6 y ESXi y ESXi Dump Collector se encuentran en hosts diferentes, ambos requieren direcciones IPv6 de alcance global. El tráfico se enruta por medio de la puerta de enlace IPv6 predeterminada.

Requisitos previos

- ESXi Dump Collector se incluye con el nodo de administración de vCenter Server.
- Instale vCLI si quiere configurar el host para que use ESXi Dump Collector. En situaciones de solución de problemas, puede usar ESXCLI en ESXi Shell en su lugar.

Procedimiento

- 1 Configure un sistema ESXi para que use ESXi Dump Collector; para ello, ejecute `esxcli system coredump` en la instancia de ESXi Shell local o use vCLI.

```
esxcli system coredump network set --interface-name vmk0 --server-ip 10xx.xx.xx.xx --server-port 6500
```

Debe especificar una dirección IP y la NIC de VMkernel, además de un puerto opcional del servidor al cual se deben enviar los volcados de núcleos. Puede usar una dirección IPv4 o IPv6. Si configura un sistema ESXi que se ejecuta en una máquina virtual que usa un conmutador vSphere estándar, debe seleccionar un puerto de VMkernel que esté en modo promiscuo.

- 2 Habilite ESXi Dump Collector.

```
esxcli system coredump network set --enable true
```

- 3 (opcional) Compruebe que ESXi Dump Collector esté configurado correctamente.

```
esxcli system coredump network check
```

Resultados

El host en el que ha configurado ESXi Dump Collector está configurado para enviar los volcados de núcleos al servidor indicado mediante la NIC de VMkernel y el puerto opcional especificados.

Pasos siguientes

- Escriba una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Consulte [Escribir una regla y asignar un perfil de host a hosts](#).
- Para los hosts que ya se aprovisionaron con Auto Deploy, realice las operaciones de prueba y reparación de cumplimiento para aprovisionarlos con el nuevo perfil de host. Consulte [Probar y reparar cumplimiento de reglas](#).
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar Host Profiles para un host de referencia de Auto Deploy con vSphere Web Client

Puede configurar perfiles de host en un host de referencia y aplicar la configuración de los perfiles de host a todos los demás hosts aprovisionados con vSphere Auto Deploy. Puede configurar el host de referencia y exportar el perfil de host, o bien, para cambios menores, editar los perfiles de host en forma directa.

Requisitos previos

Compruebe que tenga acceso a vSphere Web client que pueda conectarse al sistema vCenter Server.

Procedimiento

- 1 En vSphere Web Client, haga clic en **Reglas y perfiles** y en **Perfiles de host**.
- 2 Para un perfil nuevo, haga clic en el icono **Crear perfil a partir de un host** o haga clic con el botón derecho en un perfil que desee modificar y seleccione **Editar perfil de host**.
- 3 Personalice el host de referencia mediante vCLI, mediante la interfaz de usuario del cliente o mediante la interfaz de Host Profiles.

Directiva	Descripción
ESXi Dump Collector	Configure ESXi Dump Collector con el comando <code>esxcli system coredump</code> y guarde el perfil de host (práctica recomendada), o configure el perfil de host en forma directa. Consulte Configurar Syslog desde la interfaz de Host Profiles en vSphere Web Client .
Syslog	Configure Syslog para el host con el comando <code>esxcli system syslog</code> . Guarde el perfil de host (práctica recomendada) o configure el perfil de host en forma directa. Consulte Configurar Syslog desde la interfaz de Host Profiles en vSphere Web Client .
NTP	Use el comando <code>vicfg-ntp</code> de vCLI o vSphere Web Client para configurar un host. Si usa vSphere Web Client para iniciar el servidor NTP, asegúrese de que la directiva de inicio del daemon NTP esté configurada correctamente. <ol style="list-style-type: none"> a En vSphere Web Client, seleccione el host. b Seleccione la pestaña Administrar y haga clic en Configuración de hora. c Haga clic en Editar y, a continuación, en Usar protocolo de hora de red (Habilitar el cliente NTP). d Seleccione la opción Iniciar y detener con el host como la directiva de inicio del servicio NTP.
Seguridad	Establezca la configuración del firewall, los parámetros de seguridad, la configuración del usuario y la configuración del grupo de usuarios para el host de referencia con los comandos de vCLI o vSphere Web Client. Consulte la documentación sobre <i>seguridad de vSphere</i> .
Redes y almacenamiento	Configure las directivas de redes y almacenamiento para el host de referencia con el comando de vCLI o vSphere Web Client.

- 4 Haga clic en **Aceptar** para guardar la configuración del perfil de host.

Pasos siguientes

Escriba una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración que especificó en el host de referencia (consulte [Escribir una regla y asignar un perfil de host a hosts](#)). Realice una operación de prueba y reparación de cumplimiento.

Configurar ESXi Dump Collector desde la interfaz de Host Profiles en vSphere Web Client

Puede configurar ESXi Dump Collector para un host de referencia con `esxcli` o directamente en los paneles de Host Profiles de vSphere Web Client. Puede exportar el perfil de host y escribir una regla que aplique el perfil a todos los hosts aprovisionados con Auto Deploy.

La práctica recomendada es usar ESXi Dump Collector con el comando `esxcli system coredump` y guardar el perfil de host (consulte [Configurar ESXi Dump Collector con ESXCLI](#)). Si prefiere usar una GUI, configure ESXi Dump Collector desde la interfaz de Host Profiles.

Requisitos previos

Compruebe que al menos una partición disponga de capacidad de almacenamiento suficiente para los volcados de núcleos de varios hosts aprovisionados con vSphere Auto Deploy.

Procedimiento

- 1 En vSphere Web Client, haga clic en **Reglas y perfiles** y en **Perfiles de host**.
- 2 Para un perfil nuevo, haga clic en el icono **Crear perfil a partir de un host** o haga clic con el botón derecho en un perfil que desee modificar y seleccione **Editar perfil de host**.
- 3 Conserve el nombre y la descripción, y haga clic en **Siguiente**.
- 4 Seleccione **Configuración de red**.
- 5 Seleccione **Configuración de volcados de núcleos de red**.
- 6 Haga clic en la casilla **Habilitado**.
- 7 Especifique la NIC del host que se debe usar, la IP del servidor de volcados de núcleos de red y el puerto del servidor de volcados de núcleos de red.
- 8 Haga clic en **Finalizar** para guardar la configuración del perfil de host.

Pasos siguientes

- Escriba una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración que especificó en el host de referencia. Consulte [Escribir una regla y asignar un perfil de host a hosts](#).
- Para los hosts que ya se han aprovisionado con Auto Deploy, realice la prueba de cumplimiento y las operaciones de reparación para aprovisionarlos con el nuevo perfil de host. Consulte [Probar y reparar cumplimiento de reglas](#).
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar Syslog desde la interfaz de Host Profiles en vSphere Web Client

Por lo general, los hosts aprovisionados con Auto Deploy no cuentan con almacenamiento local suficiente para almacenar los registros del sistema. Puede especificar un servidor remoto de Syslog para esos hosts. Para ello, debe configurar un host de referencia, guardar el perfil de host y aplicar dicho perfil de host a los demás hosts según sea necesario.

La práctica recomendada es configurar el servidor de Syslog en el host de referencia con vSphere Web Client o con el comando `esxcli system syslog` y guardar el perfil de host. También puede configurar Syslog desde la interfaz de Host Profiles.

Requisitos previos

- Si va a usar un host de Syslog remoto, configure ese host antes de personalizar los perfiles de host.
- Compruebe que tenga acceso a una instancia de vSphere Web Client que pueda conectarse al sistema vCenter Server.

Procedimiento

- 1 En vSphere Web Client, haga clic en **Reglas y perfiles** y en **Perfiles de host**.
- 2 (opcional) Si no existe ningún host de referencia en el entorno, haga clic en el icono **Extraer perfil de host** para crear un perfil de host.
- 3 Haga clic con el botón derecho en el perfil de host que desea modificar y seleccione **Editar perfil de host**.
- 4 Conserve el nombre y la descripción, y haga clic en **Siguiente**.
- 5 Haga clic en **Opciones de configuración avanzadas**, luego en la carpeta **Opciones avanzadas** y, a continuación, en **Opciones de configuración avanzadas**.

Puede especificar la configuración de Syslog desde aquí.

- 6 Si va a configurar un host ESXi 5.0 que no tenía un servidor de Syslog configurado previamente, debe crear una opción de configuración avanzada.
 - a Haga clic en el signo más (+).
 - b Haga clic en la nueva opción de configuración avanzada, ubicada en la posición superior de la lista de opciones, y seleccione **Configurar una opción fija** en el menú desplegable.
 - c Especifique Syslog.global.loghost como la opción y el host como el valor.

Si va a configurar un host ESXi versión 5.1 o superior, o un host ESXi 5.0 que tiene Syslog configurado, la opción Syslog.global.loghost ya aparece en la lista de opciones avanzadas.

- 7 Haga clic en **Aceptar** para guardar la configuración del perfil de host.

Pasos siguientes

- Escriba una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración que especificó en el host de referencia (consulte [Escribir una regla y asignar un perfil de host a hosts](#)).
- Para los hosts que ya se han aprovisionado con Auto Deploy, realice la prueba de cumplimiento de normas y las operaciones de reparación con la finalidad de aprovisionarlos con el nuevo perfil de imagen. Consulte [Probar y reparar cumplimiento de reglas](#).
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de imagen.

Configurar redes para el host de Auto Deploy en vSphere Web Client

Puede configurar redes para el host de referencia de Auto Deploy y aplicar el perfil de host a todos los demás hosts a fin de garantizar un entorno de red completamente funcional.

Requisitos previos

Use Auto Deploy para aprovisionar el host que desea utilizar como host de referencia con una imagen de ESXi.

Procedimiento

- 1 En vSphere Web Client, seleccione el host y haga clic en la pestaña **Redes**.
- 2 Realice la configuración de redes.

Si usa conmutadores virtuales y no vSphere Distributed Switch, no agregue otras NIC de VMkernel a vSwitch0.
- 3 Después de configurar el host de referencia, reinicie el sistema para comprobar que vmk0 esté conectado a la red de administración.
- 4 Cree un perfil de host desde el host.

Pasos siguientes

- Escriba una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración que especificó en el host de referencia. Consulte [Escribir una regla y asignar un perfil de host a hosts](#).
- Para los hosts que ya se han aprovisionado con Auto Deploy, realice la prueba de cumplimiento y las operaciones de reparación para aprovisionarlos con el nuevo perfil de host. Consulte [Probar y reparar cumplimiento de reglas](#).
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Planificar e implementar la estrategia de creación de particiones

De manera predeterminada, Auto Deploy aprovisiona los hosts solo si hay una partición disponible en el host. Puede configurar un host de referencia para crear particiones automáticamente de todos los hosts que aprovisiona con Auto Deploy.

Precaución Si cambia el comportamiento predeterminado de creación automática de particiones, Auto Deploy sobrescribe las particiones existentes independientemente del contenido. Si activa esta opción, asegúrese de que no se produzca una pérdida de datos no intencionada.

A fin de garantizar que las unidades de estado sólido (SSD) locales permanezcan sin particionar durante la creación automática de particiones, deberá establecer el parámetro **skipPartitioningSsds=TRUE** en el host de referencia.

Para obtener más información sobre cómo evitar el formato de las unidades de estado sólido (SSD) durante la creación automática de particiones, consulte la documentación de *Almacenamiento de vSphere*.

Requisitos previos

- Aprovisiona el host que desea utilizar como host de referencia con una imagen de ESXi a través de Auto Deploy.
- Compruebe que tiene acceso a vSphere Web Client y que puede conectarse al sistema vCenter Server.

Procedimiento

- 1 En vSphere Web Client, seleccione el host que desea utilizar como host de referencia y haga clic en **Administrar**.
- 2 Haga clic en **Configuración**.
- 3 Haga clic en **Sistema** para abrir las opciones del sistema y haga clic en **Configuración avanzada del sistema**.
- 4 Desplácese a `VMkernel.Boot.autoPartition` y establezca el valor en `true`.
- 5 (opcional) Si desea que las unidades de estado sólido (SSD) locales permanezcan sin particionar, desplácese a `VMkernel.Boot.skipPartitioningSsds` y establezca el valor en `"true"`.
- 6 Si no existen perfiles de host para su host de referencia, créelo ahora.
- 7 Utilice la PowerCLI de Auto Deploy para escribir una regla que aplique el perfil de host de su host de referencia a todos los hosts inmediatamente al arrancar.

Resultados

La creación automática de particiones se realiza cuando se arrancan los hosts.

Tareas de administración avanzadas

En la mayoría de los casos, usted administra el entorno de Auto Deploy al preparar la configuración del sistema, escribir reglas y aprovisionar hosts. En algunos casos, podría ejecutar tareas de administración avanzadas, como registrar nuevamente el servidor Auto Deploy o asignar una dirección IP estática a cada host.

Configurar Host Profiles para direcciones IP estáticas en vSphere Web Client

De forma predeterminada, un servidor DHCP asigna direcciones DHCP a los hosts aprovisionados con Auto Deploy. Puede usar el mecanismo de personalización de hosts de Auto Deploy para asignar direcciones IP estáticas a los hosts.

Requisitos previos

- Configure el entorno de Auto Deploy.
- Arranque el host mediante Auto Deploy.
- Extraiga un perfil de host del host.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta la instancia de vCenter Server que administra el host de Auto Deploy y seleccione **Directivas y perfiles** y, a continuación, **Perfiles de host**.
- 2 Haga clic con el botón derecho en el perfil de host extraído y, a continuación, haga clic en **Editar configuración**.
- 3 Utilice los valores predeterminados de nombre y descripción, y haga clic en **Siguiente**.
- 4 Cambie la configuración de dirección IP predeterminada haciendo clic en **Configuración de red > Grupos de puertos de host > Red de administración > Configuración de dirección IP**.
- 5 En el menú desplegable **Dirección IPv4**, seleccione **Dirección IPv4 especificada por el usuario que se usará mientras se aplica la configuración**.
- 6 Si el host está en una subred diferente a la del sistema vCenter Server, seleccione **Configuración de red > Instancia de NetStack > Pila de TCP/IP predeterminada > Configuración de DNS** e introduzca la ruta de acceso predeterminada en el cuadro de texto **Puerta de enlace IPv4 predeterminada**.
- 7 Seleccione **Configuración de red > Instancia de NetStack > Pila de TCP/IP predeterminada > Configuración de DNS**.
- 8 Asegúrese de que la casilla **Marca que indica que se debe usar DHCP** no esté seleccionada.
- 9 Haga clic con el botón derecho en el host y seleccione **Todas las acciones de vCenter > Perfiles de host > Adjuntar perfil de host**.
- 10 Seleccione el perfil que desea adjuntar y haga clic en **Siguiente**.
- 11 Especifique la dirección IP y la máscara de red, y haga clic en **Finalizar**.
- 12 Reinicie el host ESXi.

Resultados

La dirección IP se guarda como una opción de personalización del host y se aplica al host.

Personalizar hosts en vSphere Web Client

Para personalizar hosts con atributos compartidos, puede crear un perfil de host en un host de referencia. Para personalizar host individuales, puede configurar algunos campos en el perfil de host para solicitarle al usuario que introduzca información para cada host.

Los perfiles de hosts permiten especificar información previamente, por ejemplo, la configuración del almacenamiento o la configuración de Syslog en un host de referencia, y aplicar el perfil de host a un conjunto de hosts de destino que compartan la misma configuración. También puede usar los perfiles de host para especificar que ciertos parámetros de configuración dependen del host. Si lo hace, el host aparece en modo de mantenimiento cuando lo aprovisiona con Auto Deploy. Corrija el host o restablezca la personalización del host para que solicite la introducción de información. El sistema almacena la información introducida y la usa la próxima vez que el host arranque.

Nota La personalización del host no se almacena en una ubicación o en un formato al que los administradores puedan acceder. Use la interfaz de Perfiles de host en vSphere Web Client para modificar la personalización.

Cuando el perfil de host está configurado para que le solicite al usuario la introducción de información, debe especificar un valor en el cuadro de diálogo que aparece cuando restablece la personalización del host. Si no especifica un valor, se produce un error.

Tabla 4-9. Opciones de perfil de host que solicitan al usuario la introducción de información de iSCSI

Información que se le solicita al usuario	Configuración de la opción de perfil de host
<p>Cuando aplica un perfil de host en un sistema que incluye un perfil para iSCSI, se le solicitan varias propiedades. Se ofrecen valores predeterminados del sistema para muchas de las propiedades. Para algunas propiedades, debe especificar resultados para un valor o un error.</p> <p>Nombre de IQN</p> <p>Si la configuración de iSCSI utiliza un nombre de IQN, se le solicita cuando aplica el perfil de host. No puede continuar hasta que proporcione el nombre.</p> <p>Información de CHAP</p> <p>Si configura iSCSI para que requiera autenticación de CHAP, se le solicita información de CHAP, como el nombre de usuario y la contraseña cuando aplique el perfil de host. No puede continuar hasta que proporcione el nombre.</p>	<ol style="list-style-type: none"> 1 Seleccione Editar perfil de host, haga clic en Configuración de almacenamiento y, luego, en Configuración de iniciador de iSCSI. 2 Seleccione la carpeta de un iniciador ya habilitado y configure el iniciador. 3 Configure el iniciador. En muchos campos, se le solicita al usuario la introducción de información como parte de la personalización del host.

Tabla 4-10. Opciones de perfil de host que solicitan al usuario la introducción de información de almacenamiento

Información que se le solicita al usuario	Configuración de la opción de perfil de host
Va a configurar los valores de PSP fijo y desea solicitar los identificadores del adaptador y de destino para las matrices de almacenamiento que deben usar el PSP fijo.	<p>Puede configurar la opción solo si el adaptador está configurado para utilizar PSP fijo.</p> <ol style="list-style-type: none"> 1 Seleccione Editar perfil de host y haga clic en Configuración de almacenamiento. 2 Haga clic en Múltiples rutas nativas (NMP). 3 Haga clic en Configuración de directivas de selección de ruta de acceso (PSP). 4 En la ventana Ruta de acceso preferida, seleccione Solicitarle al usuario los identificadores del adaptador y de destino en el host.
Configure la activación del adaptador de FCoE en función de la dirección MAC que haya especificado un usuario.	<p>Puede establecer la opción solamente si existe un perfil de activación.</p> <ol style="list-style-type: none"> 1 Seleccione Editar perfil de host y haga clic en Configuración de almacenamiento. 2 Haga clic en Configuración de software FCoE. 3 Haga clic en Configuración del adaptador. 4 Haga clic en el perfil de activación y, a continuación, en Perfil de la directiva. 5 Seleccione Directiva de activación según la dirección MAC del adaptador en el menú desplegable.

Tabla 4-11. Opciones de perfil de host que solicitan al usuario la introducción de información de seguridad

Información que se le solicita al usuario	Configuración de la opción de perfil de host
Contraseña de administrador para el host ESXi cuando el host arranca por primera vez.	<ol style="list-style-type: none"> 1 Seleccione Editar perfil de host y haga clic en Seguridad y servicios. 2 Haga clic en Configuración de seguridad y, a continuación, en Parámetros de seguridad. 3 En el panel derecho, seleccione Contraseña introducida por el usuario que se utilizará para configurar la contraseña de administrador en el menú desplegable Contraseña de administrador.
Preconfigura un usuario para el host ESXi, pero solicita la contraseña para ese usuario en cada host cuando el host arranca por primera vez.	<p>Puede realizar esta tarea solo si ya existe una configuración de usuario. Para configurar el usuario, seleccione una de las opciones.</p> <ul style="list-style-type: none"> ■ Configuraciones de usuario fijas asignadas está disponible para el sistema ESX/ESXi 4.1; esta opción muestra la contraseña sin cifrar. ■ Asignar configuraciones de usuario fijas avanzadas se utiliza para usuarios de sistemas ESXi 5.0 y posteriores. ■ Especificar la configuración de usuario en el perfil, pero solicitar contraseña durante la configuración del host permite especificar la información sobre el usuario, pero solicita una contraseña para cada host.
Solicitarle al usuario credenciales cuando el host se una al dominio de Active Directory.	<ol style="list-style-type: none"> 1 Establezca el perfil de configuración de la autenticación para que use un dominio fijo. <ol style="list-style-type: none"> a Seleccione Editar perfil de host y haga clic en Seguridad y servicios. b Haga clic en Configuración de seguridad y en Configuración de autenticación. c Haga clic en Configuración de Active Directory. d En el menú desplegable Nombre de dominio, seleccione Configurar un nombre de dominio fijo. 2 Establezca el método para unirse al dominio que se le solicitará al usuario. <ol style="list-style-type: none"> a Seleccione Editar perfil de host, haga clic en Seguridad y servicios y, a continuación, en Configuración de autenticación. b Haga clic en Configuración de Active Directory. c En el menú desplegable Método para unirse al dominio, seleccione Usar credenciales de AD especificadas por el usuario para unir el host al dominio.

Tabla 4-12. Opciones de perfil de host que solicitan al usuario la introducción de información de red

Información que se le solicita al usuario	Configuración de la opción de perfil de host
Solicite al usuario la dirección MAC para un grupo de puertos. Puede hacer que el sistema la solicite al usuario en todos los casos (Dirección MAC especificada por el usuario...) o que la solicite al usuario solo si no hay un valor predeterminado disponible.	<ol style="list-style-type: none"> 1 Seleccione Editar perfil de host, haga clic en Configuración de red y en Grupo de puertos de host. 2 Haga clic en Red de administración. 3 En el campo Determinar de qué manera se debe decidir la dirección MAC para vmknic, seleccione de qué forma el sistema debe administrar la dirección MAC. <ul style="list-style-type: none"> ■ Dirección MAC especificada por el usuario que se usará mientras se aplica la configuración ■ Solicitarle al usuario la dirección MAC si no hay un valor predeterminado disponible
Solicite al usuario la dirección IPv4 para cada host ESXi al cual se aplicará el perfil. Puede hacer que el sistema la solicite al usuario en todos los casos (Dirección IPv4 especificada por el usuario...) o que la solicite al usuario solo si no hay un valor predeterminado disponible.	<ol style="list-style-type: none"> 1 Seleccione Editar perfil de host, haga clic en Configuración de red y en Grupo de puertos de host. 2 Haga clic en Red de administración y, a continuación, en Configuración de dirección IP. 3 En el campo Dirección IPv4, seleccione de qué manera el sistema debe administrar la dirección IPv4. <ul style="list-style-type: none"> ■ Dirección IPv4 especificada por el usuario que se usará mientras se aplica la configuración ■ Solicitarle al usuario la dirección IPv4 si no hay un valor predeterminado disponible
Solicite al usuario la dirección IPv6 para cada host ESXi al cual se aplicará el perfil. Puede hacer que el sistema la solicite al usuario en todos los casos (Dirección IPv6 especificada por el usuario...) o que la solicite al usuario solo si no hay un valor predeterminado disponible.	<ol style="list-style-type: none"> 1 Seleccione Editar perfil de host, haga clic en Configuración de red y en Grupo de puertos de host. 2 Haga clic en Red de administración y, a continuación, en Configuración de dirección IP. 3 En el campo Dirección IPv6 estática, seleccione de qué manera el sistema debe administrar la dirección IPv6. <ul style="list-style-type: none"> ■ Dirección IPv6 especificada por el usuario que se usará mientras se aplica la configuración ■ Solicitarle al usuario la dirección IPv6 si no hay un valor predeterminado disponible
Solicítele al usuario el nombre de DNS del host. Puede hacer que el sistema lo solicite al usuario en todos los casos (Nombre de host especificado por el usuario...) o que lo solicite al usuario solo si no hay un valor predeterminado disponible.	<ol style="list-style-type: none"> 1 Seleccione Editar perfil de host, haga clic en Configuración de red y en Configuración de DNS. 2 En el campo Nombre del host, seleccione de qué forma el sistema debe administrar la configuración de DNS. <ul style="list-style-type: none"> ■ Solicitarle al usuario el nombre del host si no hay un valor predeterminado disponible ■ Nombre de host especificado por el usuario que se usará mientras se aplica la configuración

Tabla 4-12. Opciones de perfil de host que solicitan al usuario la introducción de información de red (continuación)

Información que se le solicita al usuario	Configuración de la opción de perfil de host
<p>Solicítele al usuario la dirección MAC de un conmutador distribuido, su grupo de puertos o uno de sus servicios. Haga clic con el botón derecho en el icono de la carpeta de NIC virtual del host y haga clic en el icono Agregar subperfil para determinar el componente al cual se aplicará la configuración.</p> <p>Puede decidir que se le solicite al usuario en todos los casos o solo si no hay un valor predeterminado disponible.</p>	<ol style="list-style-type: none"> 1 Abra Configuración de red. 2 Haga clic en NIC virtual del host. 3 En el campo Determinar de qué manera se debe decidir la dirección MAC para vmknics, seleccione de qué forma el sistema debe administrar la dirección MAC para el conmutador distribuido. <ul style="list-style-type: none"> ■ Dirección MAC especificada por el usuario que se usará mientras se aplica la configuración ■ Solicitarle al usuario la dirección MAC si no hay un valor predeterminado disponible
<p>Solicítele al usuario la dirección IPv4 para un conmutador distribuido, su grupo de puertos o uno de sus servicios. Haga clic con el botón derecho en el icono de la carpeta de NIC virtual del host y haga clic en el icono Agregar subperfil para determinar el componente al cual se aplicará la configuración.</p> <p>Puede decidir que se le solicite al usuario solo si no hay un valor predeterminado disponible o en todos los casos.</p>	<ol style="list-style-type: none"> 1 Abra Configuración de red. 2 Haga clic en NIC virtual del host. 3 Haga clic en Configuración de la dirección IP. 4 En el campo Dirección IPv4, seleccione de qué manera el sistema maneja la dirección IPv4 para el conmutador distribuido. <ul style="list-style-type: none"> ■ Dirección IPv4 especificada por el usuario que se usará mientras se aplica la configuración ■ Solicitar al usuario la dirección IPv4 si no hay un valor predeterminado disponible
<p>Solicítele al usuario la dirección IPv6 para un conmutador distribuido, su grupo de puertos o uno de sus servicios. Haga clic con el botón derecho en el icono de la carpeta de NIC virtual del host y haga clic en el icono Agregar subperfil para determinar el componente al cual se aplicará la configuración.</p> <p>Puede decidir que se le solicite al usuario solo si no hay un valor predeterminado disponible o en todos los casos.</p>	<ol style="list-style-type: none"> 1 Abra Configuración de red. 2 Abra NIC virtual del host. 3 Abra Configuración de dirección IP. 4 En el campo Dirección IPv6 estática, seleccione de qué manera el sistema administra la dirección IPv6 para el conmutador distribuido. <ul style="list-style-type: none"> ■ Dirección IPv6 especificada por el usuario que se usará mientras se aplica la configuración ■ Solicitar al usuario la dirección IPv6 si no hay un valor predeterminado disponible

Prácticas recomendadas y consideración de seguridad de Auto Deploy

Siga las prácticas recomendadas al instalar vSphere Auto Deploy y al utilizar Auto Deploy con otros componentes de vSphere. Configure la infraestructura altamente disponible de Auto Deploy en entornos de producción de gran tamaño o cuando utilice almacenamiento en caché sin estado. Siga todas las instrucciones de seguridad que seguiría en un entorno de arranque PXE y tenga en cuenta las recomendaciones de este capítulo.

Prácticas recomendadas de vSphere Auto Deploy

Existen diversas prácticas recomendadas de vSphere Auto Deploy que puede seguir para configurar redes, configurar vSphere HA y optimizar de otro modo el entorno para vSphere Auto Deploy.

Consulte la base de conocimientos de VMware para obtener más información sobre las prácticas recomendadas.

Prácticas recomendadas de vSphere HA y vSphere Auto Deploy

Siga las prácticas recomendadas para mejorar la disponibilidad de las máquinas virtuales que se ejecutan en los hosts aprovisionados con vSphere Auto Deploy.

En algunos entornos se configuran los hosts aprovisionados con vSphere Auto Deploy con un conmutador distribuido o se configuran las máquinas virtuales que se ejecutan en los hosts con Auto Start Manager. En este tipo de entornos, implemente el sistema vCenter Server de manera que su disponibilidad coincida con la disponibilidad del servidor vSphere Auto Deploy. Se pueden emplear diversos métodos.

- Instale vCenter Server en una máquina virtual o un servidor físico con Windows, o implemente vCenter Server Appliance. Auto Deploy se implementa junto con el sistema vCenter Server.
- Implemente el sistema vCenter Server en una máquina virtual. Ejecute la máquina virtual de vCenter Server en un clúster habilitado para vSphere HA y configure la máquina virtual con una prioridad de reinicio de vSphere HA alta. Incluya dos o más hosts en el clúster que no estén administrados por vSphere Auto Deploy y ancle la máquina virtual de vCenter Server a estos hosts mediante una regla (vSphere HA DRS requiere la regla basada en el anclaje de máquina virtual a hosts). Puede configurar la regla y, a continuación, deshabilitar DRS si no desea usar DRS en el clúster. Cuanto mayor sea la cantidad de hosts no administrados por vSphere Auto Deploy, mayor será la resistencia a errores del host.

Nota Este método no resulta adecuado si se usa Auto Start Manager. Auto Start Manager no es compatible en un clúster habilitado para vSphere HA.

Prácticas recomendadas de red de vSphere Auto Deploy

Siga las prácticas recomendadas de red de vSphere Auto Deploy para prevenir problemas de red.

vSphere Auto Deploy e IPv6

Dado que vSphere Auto Deploy aprovecha la infraestructura de iPXE, si los hosts que desea aprovisionar con vSphere Auto Deploy usan BIOS heredado, el servidor vSphere Auto Deploy debe tener una dirección IPv4. El arranque PXE con firmware de BIOS heredado solo se puede realizar mediante IPv4. El arranque PXE con firmware UEFI se puede realizar mediante IPv4 o IPv6.

Asignación de direcciones IP

Use las reservas de DHCP para la asignación de direcciones. El mecanismo de personalización de hosts admite direcciones IP fijas, pero no se recomienda proporcionar entradas para cada host.

Consideraciones sobre las VLAN

Use vSphere Auto Deploy en los entornos que no emplean VLAN.

Si va a usar vSphere Auto Deploy en un entorno que emplea VLAN, asegúrese de que los hosts que desea aprovisionar puedan comunicarse con el servidor DHCP. La manera en que se asignan los hosts a una VLAN depende de la configuración del sitio. El conmutador o el enrutador pueden asignar el identificador de la VLAN, o bien puede configurarse en el BIOS del host o mediante el perfil de host. Póngase en contacto con su administrador de red a fin de determinar los pasos para permitir que los hosts se comuniquen con el servidor DHCP.

Prácticas recomendadas de VMware Tools y vSphere Auto Deploy

Al aprovisionar hosts con vSphere Auto Deploy, es posible seleccionar un perfil de imagen que incluya VMware Tools o seleccionar la imagen más pequeña asociada con el perfil de imagen que no contenga VMware Tools.

Puede descargar dos perfiles de imagen desde el sitio de descargas de VMware.

- `xxxxx-standard`: un perfil de imagen que incluye los archivos binarios de VMware Tools, necesarios para el sistema operativo invitado que se ejecuta dentro de una máquina virtual. Generalmente, la imagen tiene el nombre `esxi-version-xxxxx-standard`.
- `xxxxx-no-tools`: un perfil de imagen que no incluye los archivos binarios de VMware Tools. Generalmente, este perfil de imagen es más pequeño y tiene una menor sobrecarga de memoria, y se arranca más rápidamente en un entorno de arranque con PXE. Generalmente, esta imagen tiene el nombre `esxi-version-xxxxx-no-tools`.

Con vSphere 5.0 Update 1 y versiones posteriores, es posible implementar ESXi mediante cualquiera de estos dos perfiles de imagen.

- Si el tiempo de arranque de la red no es un factor importante, y el entorno dispone de memoria adicional y sobrecarga de almacenamiento suficientes, use la imagen que incluye VMware Tools.
- Si considera que el tiempo de arranque de la red se extiende demasiado al usar la imagen estándar, o si desea ahorrar espacio en los hosts, puede usar el perfil de imagen que no incluye VMware Tools y colocar los archivos binarios de VMware Tools en almacenamiento compartido. Consulte [Aprovisionar hosts ESXi mediante un perfil de imagen sin VMware Tools](#).

Prácticas recomendadas de administración de cargas de vSphere Auto Deploy

El arranque simultáneo de grandes cantidades de hosts supone una carga considerable para el servidor vSphere Auto Deploy. Debido a que, en esencia, vSphere Auto Deploy es un servidor web, puede usar las tecnologías existentes de escala de servidores web para ayudar a distribuir la carga. Por ejemplo, con vSphere Auto Deploy se pueden usar uno o más servidores proxy inversos de almacenamiento en caché. Los servidores proxy inversos proporcionan los archivos estáticos que constituyen la mayor parte de una imagen de arranque de ESXi. Configure el proxy inverso para que almacene en caché el contenido estático y para que transmita todas las solicitudes por medio del servidor vSphere Auto Deploy. Para obtener más información, vea el vídeo sobre el uso de servidores proxy web inversos para el escalado de vSphere Auto Deploy:



Uso de servidores proxy web inversos para el escalado de vSphere Auto Deploy
(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_9rzporg9/uiConfId/49694343/)

Use varios servidores TFTP para apuntar a diferentes servidores proxy. Use un servidor TFTP para cada servidor proxy inverso. A continuación, configure el servidor DHCP para que envíe diferentes hosts a diferentes servidores TFTP.

Al arrancar los hosts, el servidor DHCP los redirige a diferentes servidores TFTP. Cada servidor TFTP redirige los hosts a un servidor diferente, ya sean el servidor vSphere Auto Deploy o un servidor proxy inverso, lo que reduce de manera sustancial la carga en el servidor vSphere Auto Deploy.

Después de una interrupción de alimentación masiva, vuelva a encender los hosts respetando el orden de cada clúster. Si conecta varios clústeres de forma simultánea, es posible que el servidor vSphere Auto Deploy experimente cuellos de botella de CPU. Todos los hosts se conectan después de una demora. El cuello de botella es menos severo si se configura el proxy inverso.

Prácticas recomendadas de registro y solución de problemas de vSphere Auto Deploy

Con la finalidad de solucionar los problemas experimentados con vSphere Auto Deploy, use la información de registro de vSphere Auto Deploy disponible en vSphere Web Client y configure el entorno para que envíe la información de registro y los volcados de memoria de núcleo a los hosts remotos.

Registros de vSphere Auto Deploy

Descargue los registros de vSphere Auto Deploy desde la página de vSphere Auto Deploy en vSphere Web Client. Consulte [Descargar registros de Auto Deploy](#).

Configuración de Syslog

Configure un servidor remoto de Syslog. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre la configuración del servidor de Syslog.

Configure el primer host que arranque para que use el servidor remoto de Syslog y aplique el perfil de host de dicho host a todos los demás hosts de destino. Opcionalmente, puede instalar y usar vSphere Syslog Collector, una herramienta de apoyo de vCenter Server que proporciona una arquitectura unificada para el registro de sistema, permite el registro de red y permite combinar registros de diversos hosts.

Configuración de ESXi Dump Collector

Los hosts aprovisionados con vSphere Auto Deploy no cuentan con un disco local para almacenar los volcados de memoria de núcleo. Instale ESXi Dump Collector y configure el primer host para que todos los volcados de memoria de núcleos se envíen a ESXi Dump Collector y aplique el perfil de host de dicho host a todos los demás hosts. Consulte [Configurar ESXi Dump Collector con ESXCLI](#).

Usar vSphere Auto Deploy en un entorno de producción

Al cambiar de una configuración de prueba de concepto a un entorno de producción, asegúrese de que el entorno sea resistente.

- Proteja el servidor vSphere Auto Deploy. Consulte [Prácticas recomendadas de vSphere HA y vSphere Auto Deploy](#).
- Proteja todos los demás servidores del entorno, incluidos el servidor DHCP y el servidor TFTP.
- Siga las directrices de seguridad de VMware, incluidas las que se detallan en [#unique_158](#).

Configurar la infraestructura de vSphere Auto Deploy de alta disponibilidad

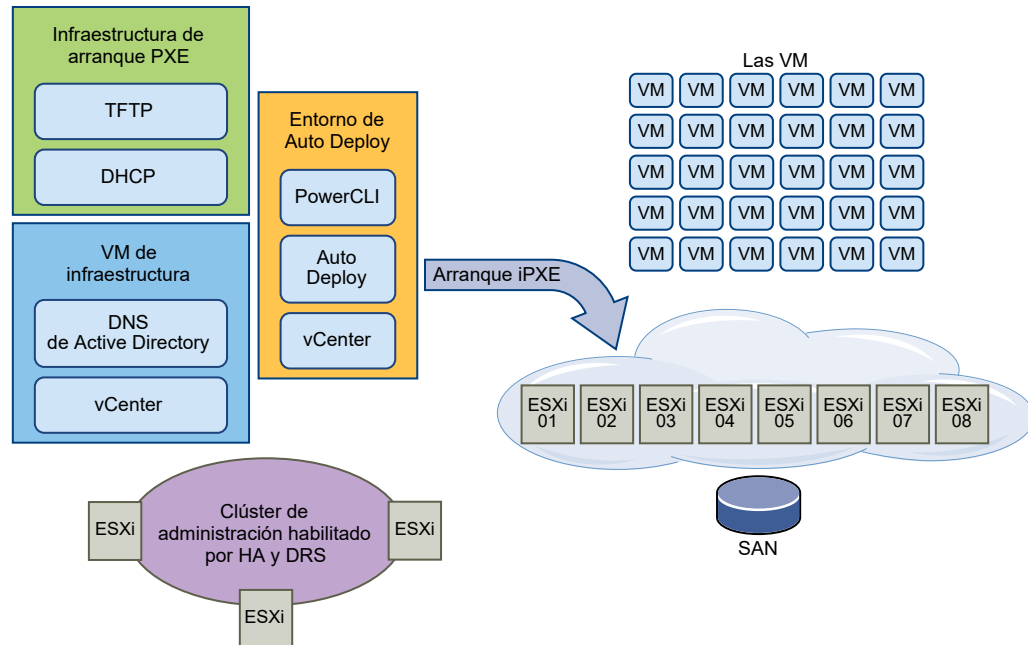
En muchas situaciones de producción, se necesita una infraestructura de vSphere Auto Deploy de alta disponibilidad para evitar la pérdida de datos. Esta infraestructura también es uno de los requisitos previos para usar vSphere Auto Deploy con almacenamiento en caché sin estado.



Infraestructura de vSphere Auto Deploy de alta disponibilidad

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_3gn1maf3/uiConfId/49694343/)

Figura 4-5. Infraestructura de vSphere Auto Deploy de alta disponibilidad



Requisitos previos

Para el clúster de administración, instale ESXi en tres hosts. No aprovisione los hosts del clúster de administración con vSphere Auto Deploy.

Mire el vídeo "Highly Available vSphere Auto Deploy Infrastructure" para obtener información sobre la implementación de una infraestructura de vSphere Auto Deploy de alta disponibilidad:

Procedimiento

- 1 Habilite vSphere HA y vSphere DRS en el clúster de administración.
- 2 Configure las siguientes máquinas virtuales en el clúster de administración.

Componente de infraestructura	Descripción
Infraestructura de arranque PXE	Servidores de DHCP y TFTP.
Máquina virtual de infraestructura	Active Directory, DNS, vCenter Server.
Entorno de vSphere Auto Deploy	vSphere PowerCLI, servidor vSphere Auto Deploy, vCenter Server. Configure este entorno en una sola máquina virtual o en tres máquinas virtuales independientes en los sistemas de producción.

vCenter Server en la máquina virtual de infraestructura es diferente a vCenter Server en el entorno de vSphere Auto Deploy.

- 3 Configure vSphere Auto Deploy para aprovisionar otros hosts según sea necesario.

Debido a que los componentes del clúster de administración están protegidos mediante vSphere HA, la característica de alta disponibilidad es compatible.

Consideraciones de seguridad de Auto Deploy

Comprender los potenciales riesgos de seguridad le ayuda a configurar su entorno de forma segura.

Proteja la red como lo haría para cualquier otro método de implementación basado en PXE. Auto Deploy transfiere datos por SSL para evitar interferencias accidentales e intromisiones. Sin embargo, la autenticidad del cliente o del servidor Auto Deploy no se comprueba durante un arranque PXE.

La imagen de arranque que descarga el servidor 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.
- El certificado y la clave SSL públicas y privadas del host se incluyen en la imagen de arranque.

Puede reducir ampliamente el riesgo de seguridad de Auto Deploy aislando por completo la red donde se utiliza Auto Deploy.

Usar el perfil de host de configuración de alias de dispositivo

En vSphere 5.5 y posterior, puede asignar un dispositivo (dirección de bus) de forma persistente a un nombre de dispositivo (alias). Puede modificar la asignación mediante el perfil de host de configuración de alias de dispositivo. El uso de la asignación persistente puede ayudar a evitar advertencias de cumplimiento para los hosts sin estado y también es útil para los hosts con estado.

El perfil de host de configuración de alias de dispositivo se selecciona de forma predeterminada, lo que implica que los alias se asignan a cada dispositivo. Por ejemplo, si un host no reconoce una de las NIC durante el proceso de arranque, los alias de NIC ya no se modifican. Esto puede ser de ayuda para la administración generada por script y también si aplica un perfil de host desde un host de referencia.

Nota Para evitar errores, no deshabilite ni edite el perfil de host de configuración de alias de dispositivo.

Para asegurarse de que la nomenclatura de los dispositivos sea uniforme, persistente y estable en todos los hosts, utilice el perfil de alias de dispositivo solo con hosts homogéneos. Estos son hosts configurados de forma idéntica con las mismas tarjetas de red y de almacenamiento en el bus PCI.

Nota Lleve siempre el BIOS al nivel más reciente. En el caso de sistemas con versiones del BIOS anteriores, es posible que el BIOS no proporcione información de ubicación precisa para los dispositivos en la tarjeta. En estos casos, ESXi aplica heurística para mantener el alias estable, incluso para estos dispositivos. Es posible que esto no funcione en todas las situaciones, por ejemplo, si los cambios se realizan en la configuración del BIOS o si los dispositivos tienen errores.

Errores de cumplimiento de la configuración de alias de dispositivo

En el caso de los hosts que no son completamente homogéneos (por ejemplo, los hosts que contienen tarjetas PCI distintas o tienen niveles de BIOS diferentes), si aplica el perfil de host desde un host de referencia, es posible que la comprobación de cumplimiento genere un error de cumplimiento. La comprobación de cumplimiento omite los dispositivos adicionales del host que no estaban en el host de referencia. Seleccione el host con menos dispositivos como el host de referencia.

Si la comprobación de cumplimiento muestra que los hosts no son totalmente homogéneos, será necesario modificar el propio hardware para corregir el error de cumplimiento.

Si el error de cumplimiento muestra que los alias de dispositivo (por ejemplo, nombres como vmhba3) son distintos de los que figuran en el host de referencia, es posible realizar la corrección.

- Para corregir un host que no está aprovisionado con Auto Deploy, realice la corrección del perfil de host y reinicie el host.
- Para corregir un host aprovisionado con Auto Deploy, vuelva a aprovisionar un host.

Actualizar sistemas para perfiles de alias de dispositivo

En versiones de ESXi anteriores a 5.5, el perfil de configuración de alias de dispositivo no existe. Tenga en cuenta los siguientes problemas cuando actualice desde versiones anteriores de ESXi a ESXi 5.5:

- En los hosts instalados, es decir, los que no están aprovisionados con Auto Deploy, debe actualizar el host ESXi para conservar los alias. Una vez actualizados, los alias permanecen estables siempre que el BIOS proporcione la información.
- Al actualizar un clúster de host ESXi aprovisionado con una imagen de Auto Deploy, los alias no cambian debido a que ESXi 5.5 usa el mismo algoritmo para generar alias que las versiones anteriores. Genere un nuevo perfil de host para el host de referencia. Este perfil de host incluye el perfil de configuración de alias de dispositivo. Configure Auto Deploy para aplicar el perfil de host del host de referencia a todos los demás hosts, para que la nomenclatura de dispositivos sea coherente en todo el clúster.
- Al actualizar un sistema, no actualice el BIOS, ya que esta acción podría cambiar los alias. La actualización del BIOS al nivel más reciente es más adecuada en el caso de una instalación nueva.

Aprovisionar hosts ESXi mediante un perfil de imagen sin VMware Tools

Cuando se aprovisionan hosts ESXi con Auto Deploy, se puede escoger aprovisionar el host mediante el perfil de imagen que no contiene binarios de VMware Tools. Generalmente, este perfil de imagen es de menor tamaño, posee menos sobrecarga de memoria y arranca más rápido en un entorno de arranque PXE.

Si al usar la imagen estándar encuentra que la red tarda demasiado en arrancar, o bien si desea guardar algo de espacio en los hosts, puede usar el perfil de imagen que no incluye VMware Tools y colocar los binarios de VMware Tools en un almacenamiento compartido.

Requisitos previos

Descargue el perfil de imagen `xxxxxx-no-tools` del sitio de descarga de VMware.

Procedimiento

- 1 Arranque un host ESXi que no se aprovisionó con Auto Deploy.
- 2 Copie el directorio `/productLocker` desde el host ESXi hasta un almacenamiento compartido.
- 3 Cambie la variable `UserVars.ProductLockerLocation` para que apunte al directorio `/productLocker`.
 - a En vSphere Web Client, seleccione el host de referencia y haga clic en la pestaña **Administrar**.
 - b Seleccione **Configuración** y haga clic en **Configuración avanzada del sistema**.

- c Filtre la configuración para **uservars** y seleccione **UserVars.ProductLockerLocation**.
 - d Haga clic en el icono de **lápiz** para editar la configuración para que apunte al almacenamiento compartido.
- 4 Cree un perfil de host desde el host de referencia.
 - 5 Cree una regla de Auto Deploy que asigne el perfil de imagen `xxxxx-no-tools` y el perfil de host desde el host de referencia hasta todos los otros hosts.
 - 6 Arranque sus host de destino con la regla para que elijan la ubicación del casillero del producto desde el host de referencia.

Descargar registros de Auto Deploy

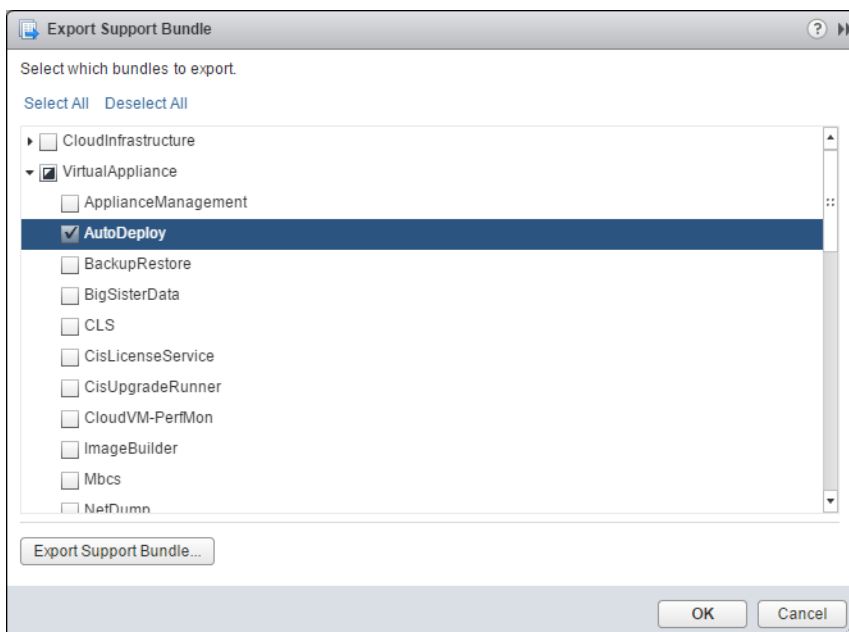
Puede usar la información de registro de Auto Deploy de vSphere Web Client para solucionar los problemas que experimente con vSphere Auto Deploy.

Requisitos previos

Use vSphere Web Client para iniciar sesión en la instancia de vCenter Server con la que se ha registrado Auto Deploy.

Procedimiento

- 1 En **Administración**, seleccione **Implementación > Configuración del sistema**.
- 2 Haga clic en uno de los nodos para el que desea recuperar un paquete de soporte. El paquete de soporte contiene los registros de los servicios.
- 3 En el menú **Acciones**, seleccione la opción **Exportar paquetes de soporte...**
- 4 Seleccione solo **VirtualAppliance > AutoDeploy**.
- 5 Haga clic en el botón **Exportar paquete de soporte...** para descargar los archivos de registro.



Solucionar problemas de Auto Deploy

Los temas de solución de problemas de Auto Deploy ofrecen soluciones a posibles problemas para situaciones cuando el aprovisionamiento de hosts con Auto Deploy no funciona según lo esperado.

Error de tiempo de espera de TFTP de Auto Deploy durante el arranque

Aparece el mensaje de error Tiempo de espera de TFTP cuando arranca un host aprovisionado por Auto Deploy. El texto del mensaje depende del BIOS.

Problema

Aparece el mensaje de error Tiempo de espera de TFTP cuando arranca un host aprovisionado por Auto Deploy. El texto del mensaje depende del BIOS.

Causa

El servidor TFTP está caído o no está accesible.

Solución

- ◆ Asegúrese de que el servicio TFTP esté en ejecución y accesible para el host que está intentando arrancar.

El host Auto Deploy arranca con una configuración incorrecta

Un host está arrancando con una imagen, perfil de host o ubicación de carpeta de ESXi diferentes de los especificados en las reglas.

Problema

Un host está arrancando con un perfil de imagen o configuración de ESXi diferentes a los que especifican las reglas. Por ejemplo, puede cambiar las reglas para asignar un perfil de imagen diferente, pero el host sigue usando el perfil de imagen antiguo.

Causa

Después de que el host se haya agregado a un sistema de vCenter Server, la configuración de arranque la determina el sistema de vCenter Server. El sistema de vCenter Server asocia un perfil de imagen, perfil de host o ubicación de carpeta con el host.

Solución

- ◆ Use los cmdlets de PowerCLI `Test-DeployRuleSetCompliance` y `Repair-DeployRuleSetCompliance` para reevaluar las reglas y asociar el perfil de imagen, perfil de host o ubicación de carpeta correctos con el host.

No se redirige el host al servidor Auto Deploy

Durante un arranque, un host que desea aprovisionar con Auto Deploy carga iPXE. El host no se redirige al servidor Auto Deploy.

Problema

Durante un arranque, un host que desea aprovisionar con Auto Deploy carga iPXE. El host no se redirige al servidor Auto Deploy.

Causa

El archivo `tramp` que está incluido en el archivo ZIP TFTP tiene la dirección IP incorrecta para el servidor Auto Deploy.

Solución

- ◆ Corrija la dirección IP del servidor Auto Deploy en el archivo `tramp`, según se explica en la documentación de *Instalación y configuración de vSphere*.

El host Auto Deploy con una unidad flash USB integrada no envía volcados de núcleo al disco local

Si su host de Auto Deploy tiene una unidad flash USB incorporada y se produce un error en un volcado de memoria, este volcado se pierde. Configure su sistema para que use ESXi Dump Collector para almacenar volcados de memoria en un host en red.

Problema

Si su host de Auto Deploy tiene una unidad USB flash incorporada y encuentra un error que produce un volcado de memoria, el volcado de memoria no se envía al disco local.

Solución

- 1 Instale ESXi Dump Collector en el sistema de su elección.
ESXi Dump Collector está incluido con el instalador de vCenter Server.
- 2 Use ESXCLI para configurar el host para que use ESXi Dump Collector.

```
esxcli conn_options system coredump network set IP-addr,port
esxcli system coredump network set -e true
```

- 3 Utilice ESXCLI para deshabilitar particiones de volcado de memoria locales.

```
esxcli conn_options system coredump partition set -e false
```

Mensaje de advertencia de paquete cuando se asigna un perfil de imagen al host Auto Deploy

Cuando se ejecuta un cmdlet de PowerCLI que asigna un perfil de imagen que no está preparado para Auto Deploy, aparece un mensaje de advertencia.

Problema

Cuando escribe o modifica reglas para asignar un perfil de imagen a uno o más hosts, se produce el siguiente error:

Warning: Image Profile <name-here> contains one or more software packages that are not stateless-ready. You may experience problems when using this profile with Auto Deploy.

Causa

Cada VIB en un perfil de imagen tiene una marca `stateless-ready` que indica que el VIB es para usar con Auto Deploy. Obtiene el error si intenta escribir una regla de Auto Deploy que usa un perfil de imagen en el cual uno o más VIB tienen esa etiqueta configurada en FALSE.

Nota Puede usar hosts aprovisionados con Auto Deploy que incluyen VIB que no están preparados para estar sin estado sin problemas. Sin embargo, un arranque con un perfil de imagen que incluye VIB que no están preparados para estar sin estado se trata como una instalación nueva. Cada vez que arranca el host, pierde datos de configuración que de lo contrario estarían disponibles a través de reinicios para hosts aprovisionados con Auto Deploy.

Solución

- 1 Use cmdlets Image Builder PowerCLI para ver los VIB en el perfil de imagen.
- 2 Quite cualquier VIB que no esté preparado para estar sin estado.
- 3 Vuelva a ejecutar el cmdlet PowerCLI de Auto Deploy.

El host Auto Deploy se reinicia después de cinco minutos

El host de Auto Deploy arranca y muestra información de iPXE, pero se reinicia tras cinco minutos.

Problema

Un host que se aprovisionará con Auto Deploy arranca desde iPXE y muestra información de iPXE en la consola. Sin embargo, tras cinco minutos, el host muestra el siguiente mensaje a la consola y se reinicia.

```
This host is attempting to network-boot using VMware
AutoDeploy. However, there is no ESXi image associated with this host.
Details: No rules containing an Image Profile match this
host. You can create a rule with the New-DeployRule PowerCLI cmdlet
and add it to the rule set with Add-DeployRule or Set-DeployRuleSet.
The rule should have a pattern that matches one or more of the attributes
listed below.
```

El host también podría mostrar los siguientes detalles:

```
Details: This host has been added to VC, but no Image Profile
is associated with it. You can use Apply-ESXImageProfile in the
PowerCLI to associate an Image Profile with this host.
Alternatively, you can reevaluate the rules for this host with the
Test-DeployRuleSetCompliance and Repair-DeployRuleSetCompliance cmdlets.
```

Luego, la consola muestra los atributos de las máquinas del host incluido el proveedor, el número de serie, la dirección IP, etc.

Causa

No hay un perfil de imagen actualmente asociado con este host.

Solución

Puede asignar temporalmente un perfil de imagen al host ejecutando el cmdlet `Apply-EsxImageProfile`.

Puede asignar de forma permanente un perfil de imagen al host de la siguiente manera.

- 1 Ejecute el cmdlet `New-DeployRule` para crear una regla que incluya un patrón que coincida con el host con un perfil de imagen.
- 2 Ejecute el cmdlet `Add-DeployRule` para agregar la regla a un conjunto de reglas.
- 3 Ejecute el cmdlet `Test-DeployRuleSetCompliance` y use el resultado de ese cmdlet como entrada para el cmdlet de `Repair-DeployRuleSetCompliance`.

El host Auto Deploy no realiza el arranque de red

El host que aprovisiona con Auto Deploy se activa pero no realiza el arranque de red.

Problema

Cuando intenta arranque un host aprovisionado con Auto Deploy, el host no inicia el proceso de arranque de red.

Causa

No habilitó el host para el arranque de red.

Solución

- 1 Reinicie el host y siga las instrucciones en pantalla para acceder a la configuración del BIOS.
Si tiene un host EFI, debe cambiar el sistema EFI a modo de compatibilidad del BIOS.
- 2 En la configuración del BIOS, habilite el arranque de red en la configuración de dispositivo de arranque.

El host Auto Deploy no obtiene una dirección asignada por DHCP

El host que aprovisiona con Auto Deploy no recibe una dirección DHCP.

Problema

Cuando intenta arrancar un host aprovisionado con Auto Deploy, el host realiza un arranque de la red pero tiene asignada dirección DHCP. El servidor Auto Deploy no puede aprovisionar el host con el perfil de imagen.

Causa

Puede que tenga un problema con el servicio DHCP o con la instalación del firewall.

Solución

- 1 Compruebe que el servicio de servidor DHCP esté ejecutándose en el sistema Windows en el cual el servidor DHCP está instalado para aprovisionar hosts.
 - a Haga clic en **Inicio > Configuración > Panel de control > Herramientas administrativas**.
 - b Haga doble clic en **Servicios** para abrir el panel Administración de servicios.
 - c En el campo Servicios, busque el servicio de servidor DHCP y reinicie el servicio si no está en ejecución.

- 2 Si el servidor DHCP está en ejecución, vuelva a comprobar el ámbito de DHCP y las reservas de DHCP que configuró para sus hosts de destino.

Si el ámbito y reservas de DHCP están configurados de forma correcta, lo más probable es que el problema involucre al firewall.

- 3 Como solución alternativa temporal, apague el firewall para ver si eso resuelve el problema.
 - a Abra el símbolo del sistema haciendo clic en **Inicio > Programa > Accesorios > Símbolo del sistema**.
 - b Escriba el siguiente comando para apagar temporalmente el firewall. No apague el firewall en un entorno de producción.

```
netsh firewall set opmode disable
```

- c Intente aprovisionar el host con Auto Deploy.
- d Escriba el siguiente comando para volver a encender el firewall.

```
netsh firewall set opmode enable
```

- 4 Instale reglas para permitir tráfico de red DHCP hacia los hosts de destino.

Consulte la documentación del firewall para ver los detalles del DHCP y del sistema Windows en el cual se ejecuta el servidor DHCP.

El host Auto Deploy no puede ponerse en contacto con el servidor TFTP

El host que aprovisiona con Auto Deploy no puede contactar al servidor de TFTP.

Problema

Cuando intenta arrancar un host aprovisionado con Auto Deploy, el host realiza un arranque de red y el servidor DHCP le asigna una dirección, pero el host no puede contactar al servidor TFTP.

Causa

El servidor TFTP podría haber dejado de ejecutarse o un firewall podría bloquear el puerto TFTP.

Solución

- Si instaló el servidor TFTP de WinAgents, abra la consola de administración TFTP de TFTP y compruebe que el servicio esté en ejecución. Si el servicio se está ejecutando, compruebe las reglas de entrada del firewall de Windows para asegurarse de que el puerto TFTP no esté bloqueado. Desactive temporalmente el firewall para ver si este es el problema.
- Para todos los otros servidores TFTP, consulte la documentación para procedimientos de depuración.

El host de Auto Deploy no puede recuperar una imagen de ESXi del servidor Auto Deploy

El host que aprovisiona con Auto Deploy se detiene en la pantalla de arranque de iPXE.

Problema

Cuando intenta arrancar un host aprovisionado con Auto Deploy, el proceso de arranque se detiene en la pantalla de arranque de iPXE y el mensaje de estado indica que el host trata de obtener la imagen de ESXi del servidor Auto Deploy.

Causa

Puede que el servicio de Auto Deploy se detenga o que el servidor Auto Deploy quede inaccesible.

Solución

- 1 Inicie sesión en el sistema en el cual instaló el servidor Auto Deploy.
- 2 Compruebe que el servidor Auto Deploy esté en ejecución.
 - a Haga clic en **Inicio > Configuración > Panel de control > Herramientas administrativas**.
 - b Haga doble clic en **Servicios** para abrir el panel Administración de servicios.
 - c En el campo Servicios, busque el servicio VMware vSphere Auto Deploy Waiter y reinícielo si no está en ejecución.
- 3 Abra un navegador web, introduzca la siguiente URL y compruebe si es posible acceder al servidor Auto Deploy.

`https://Auto_Deploy_Server_IP_Address:Auto_Deploy_Server_Port/vmw/rdp`

Nota Use esta dirección solo para comprobar si se puede tener acceso al servidor.

- 4 Si no es posible hacerlo, probablemente hay un problema con el firewall.
 - a Pruebe configurando reglas de entrada de TCP permisivas para el puerto de servidor Auto Deploy.

El puerto es 6501 a menos que haya especificado uno diferente durante la instalación.

- b Como último recurso, deshabilite temporalmente el firewall y vuelva a habilitarlo después de que haya verificado si bloqueó el tráfico. No deshabilite el firewall en entornos de producción.

Para deshabilitar el firewall, ejecute **netsh firewall set opmode disable**. Para habilitar el firewall, ejecute **netsh firewall set opmode enable**.

Recuperarse de daños en la base de datos en el servidor Auto Deploy

En ciertas situaciones, es posible que experimente un problema con la base de datos de Auto Deploy. La opción de recuperación más eficaz es reemplazar el archivo de base de datos actual con la copia de seguridad más reciente.

Problema

Al usar Auto Deploy para aprovisionar los hosts ESXi del entorno, es posible que experimente un problema con la base de datos de Auto Deploy.

Importante Se trata de un problema poco frecuente. Siga todas las demás estrategias de solución de problemas de Auto Deploy antes de reemplazar el archivo de base de datos actual. Se perderán las reglas o las asociaciones que haya creado desde la copia de seguridad que elija.

Causa

Este problema ocurre únicamente en los hosts aprovisionados con Auto Deploy.

Solución

- 1 Detenga el servicio del servidor Auto Deploy.
- 2 Busque el registro de Auto Deploy desde la página de Auto Deploy en vSphere Web Client.
- 3 Busque el siguiente mensaje en los registros:

`DatabaseError: database disk image is malformed.`

Si ve este mensaje, reemplace el archivo de base de datos existente con la copia de seguridad más reciente.

4 Vaya al directorio de datos de Auto Deploy.

Sistema operativo	Ubicación del archivo
vCenter Server Appliance	/var/lib/rbd
Microsoft Windows	El directorio de datos que seleccionó durante la instalación. Para buscarlo, escriba el siguiente comando en un símbolo de la línea de comandos: <pre>reg.exe QUERY "HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware vSphere Auto Deploy" /v DataPath</pre>

El directorio contiene un archivo denominado `db` y los archivos de copia de seguridad denominados `db-yyy-mm-dd`.

5 Cambie el nombre del archivo `db` actual.

Si solicita asistencia, es posible que el servicio de soporte de VMware le pida ese archivo.

6 Cambie el nombre de la copia de seguridad más reciente a `db`.

7 Reinicie el servicio del servidor Auto Deploy.

8 Si el mensaje sigue apareciendo en el registro, repita los pasos para usar la siguiente copia de seguridad más reciente hasta que Auto Deploy funcione sin mostrar errores de la base de datos.

Configurar prueba de concepto de Auto Deploy

Una configuración de prueba de concepto de un entorno de Auto Deploy ayuda a los administradores a evaluar el producto y demostrar sus capacidades en lo que respecta a la administración. Cuando complete el flujo de trabajo de configuración de prueba de concepto, tendrá un entorno de Auto Deploy en funcionamiento que incluye un host de referencia y uno o más hosts de destino.

La configuración de prueba de concepto está diseñada para un entorno de desarrollo o prueba, pero su configuración completa puede representar la base para un entorno de producción. El conjunto de tareas comienza en un entorno en el que no hay componentes de Auto Deploy instalados. En las descripciones de las tareas se asume que va a utilizar una red común sin etiquetado de VLAN entre los hosts físicos y el resto de su entorno.

Para realizar las tareas, deberá tener los siguientes conocimientos y privilegios.

- Experiencia con vSphere (vCenter Server, ESX y ESXi).
- Conocimiento básico de Microsoft PowerShell y vSphere PowerCLI.
- Derechos de administrador en los sistemas Windows y vCenter Server de destino.

Siga las tareas en el orden presentado en este documento. Algunos pasos pueden realizarse en un orden diferente, pero el orden utilizado aquí limita las manipulaciones repetidas de algunos componentes.

Auto Deploy no es compatible con entornos que solo utilicen IPv6 de extremo a extremo. La infraestructura de arranque PXE no es compatible con IPv6. Después de la implementación, puede volver a configurar los hosts de forma manual de manera que utilicen IPv6 y agregarlos a vCenter Server por IPv6. Sin embargo, la configuración de IPv6 de un host sin estado se pierde al reiniciarlo.

Lista de verificación previa a la instalación de prueba de concepto

Antes de poder iniciar la configuración para la prueba de concepto, debe asegurarse de que el entorno cumpla con los requisitos de hardware y software, y de contar con los permisos necesarios para los componentes que se incluyen en la configuración.

Esta configuración de prueba de concepto está personalizada para vCenter Server 6.0 y versiones posteriores. Para las versiones anteriores de vCenter Server, diríjase al centro de documentación de VMware correspondiente.

Para la configuración para la prueba de concepto, el sistema debe cumplir con los requisitos específicos de software y hardware.

Tabla 4-13. Lista de verificación previa a la instalación

Software y hardware necesarios	Detalles
Sistema operativo	Un sistema Windows Server 2008 R2 u otro sistema Windows posterior compatible con Microsoft PowerShell instalado previamente. Para obtener una lista completa de los sistemas operativos compatibles, consulte Sistemas operativos de host compatibles para la instalación de VMware vCenter Server .
vCenter Server	La versión 6.0 o posterior que se va a instalar en un sistema Windows. También puede instalar vSphere PowerCLI en un sistema Windows diferente. El servidor Auto Deploy forma parte de vCenter Server. vSphere PowerCLI se instala en el mismo sistema Windows. Muchas de las tareas de configuración se realizan iniciando sesión en ese sistema, ya sea en forma directa en la consola o mediante Escritorio remoto (RDP).
Almacenamiento	<p>Al menos 4 GB de espacio libre en el sistema Windows en el que se ejecuta vCenter Server. De preferencia, debe ser un segundo volumen o disco duro.</p> <p>El almacenamiento para los almacenes de datos NFS, iSCSI o Fibre Channel de ESXi, con servidores y matrices de almacenamiento que se configuran de manera tal que los servidores puedan detectar los LUN.</p> <ul style="list-style-type: none"> ■ Una lista de las direcciones IP de destino para NFS o iSCSI. ■ Una lista con la información de los volúmenes de destino para NFS o iSCSI.

Tabla 4-13. Lista de verificación previa a la instalación (continuación)

Software y hardware necesarios	Detalles
Información de los hosts (para dos hosts o más)	<p>Una lista de las direcciones IP de destino para NFS o iSCSI.</p> <p>Una lista con la información de los volúmenes de destino para NFS o iSCSI.</p> <ul style="list-style-type: none"> ■ La ruta predeterminada, la máscara de red y las direcciones IP de los servidores DNS principales y secundarios. ■ La dirección IP y la máscara de red de la red de administración principal de VMkernel. ■ La dirección IP y la máscara de red de las demás redes de VMkernel, como el almacenamiento, vSphere FT o VMware vMotion. <p>Auto Deploy no sobrescribe las particiones existentes como opción predeterminada.</p>
vSphere PowerCLI	Los archivos binarios del instalador de vSphere PowerCLI obtenidos de la página de descargas del sitio web de VMware.
Almacén de software de ESXi	La ubicación del almacén de software de ESXi en la página de descargas del sitio web de VMware. Se debe usar una URL para apuntar al perfil de imagen que está almacenado en esa ubicación o se debe descargar un archivo .zip que funcione con un almacén local. No descargue la imagen de ESXi.
servidor TFTP	El software del instalador para TFTP, como un servidor TFTP de WinAgents. El servidor TFTP que se incluye en Windows Server 2008 está estrechamente ligado a la implementación de la red de Windows y no es adecuado.
Servidor DHCP	El servidor DHCP que se incluye con Windows Server 2008 es adecuado para esta configuración de prueba de concepto.

También necesitará información acerca de los privilegios de administrador necesarios para los servidores principales del entorno, entre ellos, el servidor de Active Directory, el servidor DNS, el servidor DHCP, el servidor NTP, etc.

Se debe tener control completo del dominio de difusión de la subred en la que se implementará la configuración. Asegúrese de que no haya otros servidores DHCP, DNS ni TFTP en esta subred.

Instalar el servidor TFTP

Auto Deploy depende de un servidor TFTP para enviar la imagen de arranque hacia los hosts que aprovisiona. Se debe instalar un servidor TFTP en el entorno.

Con esta tarea solo se instala el servidor TFTP. Después se descarga un archivo de configuración en el servidor. Consulte [Configurar Auto Deploy y el entorno de TFTP en vSphere Web Client](#).

Requisitos previos

Asegúrese de que el sistema cumpla con los requisitos en la lista de comprobación de instalación. Consulte [Lista de verificación previa a la instalación de prueba de concepto](#).

Procedimiento

- 1 Inicie sesión en la consola del sistema Windows en la que vCenter Server está instalado con privilegios de administrador, en forma directa o mediante RDP.
- 2 Descargue e instale el software del servidor TFTP.

En esta configuración de muestra se usa el servidor TFTP de WinAgents. El servidor TFTP que se incluye con Windows 2008 está estrechamente vinculado con la implementación de red Windows y no es adecuado para Auto Deploy.
- 3 Configure el directorio raíz de TFTP como D:*Drive* o una ubicación similar (por ejemplo, D:\TFTP_Root\).

Pasos siguientes

Instalación y configuración de vSphere PowerCLI. Para escribir las reglas que asignan perfiles de imagen y perfiles de host a los hosts se usan cmdlets de PowerCLI. Consulte [Instalar y configurar de vSphere PowerCLI](#).

Instalar y configurar de vSphere PowerCLI

Puede administrar Auto Deploy con reglas que crea con los cmdlets de vSphere PowerCLI.

Esta configuración de prueba de concepto instala vSphere PowerCLI en el mismo sistema que el sistema vCenter Server. También puede instalar vSphere PowerCLI en un sistema Windows diferente.

Requisitos previos

- Verifique que Microsoft .NET 4.5 SP2 esté instalado o instálelo desde el sitio web de Microsoft.
- Compruebe que Windows PowerShell 3.0 esté instalado o instálelo desde el sitio web de Microsoft.

Procedimiento

- 1 Inicie sesión con privilegios de administrador en la consola del sistema Windows en el cual está instalado vCenter Server, ya sea de forma directa o mediante RDP.
- 2 Descargue vSphere PowerCLI de la página de descargas del sitio web de VMware e instale el software vSphere PowerCLI.

- 3 Confirme que vSphere PowerCLI funciona correctamente.
 - a Haga doble clic en el icono vSphere PowerCLI en el escritorio para abrir una ventana de vSphere PowerCLI.
 - b (opcional) Si aparece un error de SSL, compruebe la huella digital e ignore el error y, a continuación, ejecute `Get-DeployCommand` y presione Intro.

vSphere PowerCLI muestra una lista de cmdlets y sus definiciones en la ventana vSphere PowerCLI.

Pasos siguientes

- Si no ve una lista de cmdlets cuando ejecuta `Get-DeployCommand`, compruebe su versión de vSphere PowerCLI y, a continuación, desinstale el software y vuelva a instalarlo si es necesario.
- Para obtener información de referencia sobre vSphere PowerCLI, consulte [Usar los cmdlets de Auto Deploy](#). Consulte la *Guía del usuario de vSphere PowerCLI* para obtener detalles.
- Prepare los hosts que desea aprovisionar con Auto Deploy. Consulte [Preparar hosts de destino de Auto Deploy](#).

Preparar hosts de destino de Auto Deploy

Debe preparar todos los hosts de destino para Auto Deploy.

Requisitos previos

Los hosts que desee aprovisionar con Auto Deploy deberán cumplir con los requisitos para ESXi.

Consulte [Requisitos de hardware de ESXi](#).

Nota No puede aprovisionar los hosts de EFI con Auto Deploy a menos que cambie el sistema EFI al modo de compatibilidad de BIOS.

Procedimiento

- 1 Cambie la configuración del BIOS de cada host físico para forzar el arranque del host desde el dispositivo de red principal.
- 2 Vuelva a confirmar la dirección MAC del dispositivo de red principal.

Pasos siguientes

Prepare el servidor DHCP. Consulte [Preparar el servidor DHCP](#).

Preparar el servidor DHCP

El servidor DHCP del entorno de prueba de concepto debe estar configurado para servir a cada host de destino con un archivo binario iPXE.

El entorno de prueba de concepto utiliza Active Directory con DNS y DHCP.

La prueba de concepto demuestra cómo utilizar reservas DHCP. La configuración de una dirección IP fija para cada host lleva mucho tiempo y no se recomienda.

Requisitos previos

- Compruebe que el sistema cumpla con los requisitos de la lista de comprobación previa a la instalación. Consulte [Lista de verificación previa a la instalación de prueba de concepto](#).
- Realice todas las tareas previas de configuración de prueba de concepto. Consulte [Configurar prueba de concepto de Auto Deploy](#) para obtener la lista completa.

Procedimiento

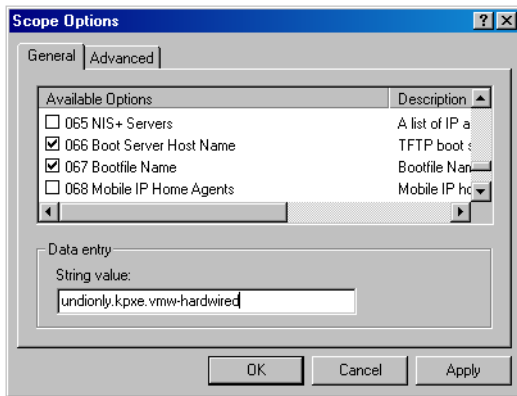
- 1 Inicie sesión en el servidor DHCP como usuario administrador.
- 2 Cree un ámbito DHCP para el intervalo de direcciones IP.
 - a Haga clic en **Inicio > Configuración > Panel de control > Herramientas administrativas** y seleccione **DHCP**.
 - b Desplácese hasta **DHCP > *hostname* > IPv4**.
 - c Haga clic con el botón derecho en **IPv4** y seleccione **Nuevo ámbito**.
 - d En la pantalla principal, haga clic en **Siguiente** y especifique un nombre y una descripción para el ámbito.
 - e Especifique un intervalo de direcciones IP y haga clic en **Siguiente**.
 - f Haga clic en **Siguiente** hasta llegar a la pantalla Configurar opciones DHCP. Allí, seleccione **No, configuraré esta opción más adelante**.
- 3 Si piensa usar reservas DHCP, cree una reserva DHCP para cada host ESXi de destino.
 - a En la ventana DHCP, vaya a **DHCP > *hostname* > IPv4 > Ámbito Auto Deploy > Reservas**.
 - b Haga clic con el botón derecho en **Reservas** y seleccione **Nueva reserva**.
 - c En la ventana Nueva reserva, especifique un nombre, una dirección IP y la dirección MAC de uno de los hosts. No incluya los dos puntos (:) en la dirección MAC.

- d Repita el procedimiento para cada uno de los otros hosts.

4 Configure el servidor DHCP para que apunte los hosts al servidor TFTP.

El procedimiento exacto depende del servidor DHCP que utilice. En este ejemplo se utiliza el servidor DHCP que se incluye con Windows 2008.

- a En la ventana DHCP, vaya a **DHCP > *hostname* > IPv4 > Ámbito Auto Deploy > Opciones de ámbito**.
- b Haga clic con el botón derecho en **Opciones de ámbito** y elija **Configurar opciones**.
- c En la ventana Opciones de ámbito, haga clic en la pestaña **General**.
- d Haga clic en **066 Nombre de host de servidor de arranque** y escriba la dirección del servidor TFTP que instaló, en el campo Valor de cadena, debajo de Opciones disponibles.



- e Haga clic en **067 Nombre de archivo de arranque** y escriba **undionly.kpxe.vmw-hardwired**.

El archivo binario iPXE `undionly.kpxe.vmw-hardwired` se utilizará para arrancar los hosts ESXi.

- f Haga clic en **Aplicar** y, a continuación, en **Aceptar** para cerrar la ventana.

- 5 En la ventana DHCP, haga clic con el botón derecho en **DHCP > *hostname* > IPv4 > Ámbito > Activar** y haga clic en **Activar**.
- 6 Si va a utilizar Active Directory para DHCP y DNS, no cierre la sesión del servidor DHCP. De lo contrario, cierre sesión.

Pasos siguientes

Prepare el servidor DNS. Consulte [Preparar el servidor DNS](#).

Preparar el servidor DNS

La preparación del servidor DNS involucra agregar información de DHCP al servidor DNS y comprobar que las entradas de DNS funcionen. Esta tarea es opcional.

El entorno de ejemplo utiliza Active Directory con DNS y DHCP.

Requisitos previos

Realice todas las tareas previas de configuración de prueba de concepto. Consulte [Configurar prueba de concepto de Auto Deploy](#) para obtener la lista completa.

Procedimiento

- 1 Inicie sesión en el servidor DNS.
- 2 Agregue las direcciones IP de reserva DHCP y los nombres de host asociados como entradas de DNS estáticas.
Asegúrese de agregar entradas en las zonas directa (registro A) e inversa (registro PTR).
- 3 Inicie sesión en la consola del sistema Windows en la que vCenter Server está instalado con privilegios de administrador, en forma directa o mediante RDP.
- 4 Abra un símbolo del sistema y ejecute el comando nslookup para buscar nombres de host ESXi para confirmar que las entradas de DNS estén funcionando.
Utilice las búsquedas directa (corta y de FQDN) e inversa.
- 5 Cierre la sesión del servidor DNS.

Configurar Auto Deploy y el entorno de TFTP en vSphere Web Client

Deberá descargar un archivo TFTP Boot ZIP desde su servidor Auto Deploy. El servidor FTP personalizado aloja las imágenes de arranque que proporciona Auto Deploy. Puede realizar la tarea en vSphere Web Client.

Requisitos previos

- Compruebe que el sistema cumpla con los requisitos de la lista de comprobación previa a la instalación. Consulte [Lista de verificación previa a la instalación de prueba de concepto](#).
- Realice todas las tareas previas de configuración de prueba de concepto. Consulte [Configurar prueba de concepto de Auto Deploy](#) para obtener la lista completa.

Procedimiento

- 1 Desde el explorador web, acceda a la dirección URL de vSphere Web Client que conecta con el sistema vCenter Server que administra el servidor Auto Deploy.
- 2 Cuando aparezca la advertencia de certificado, continúe hacia el sistema vCenter Server.
- 3 Inicie el servicio de Auto Deploy.
 - a En la página de inicio de vSphere Web Client, haga clic en **Administración**.
 - b En **Configuración del sistema**, haga clic en **Servicios**.
 - c Seleccione **Auto Deploy**, haga clic en el menú **Acciones** y seleccione **Iniciar**.
En Windows, se puede deshabilitar el servicio de Auto Deploy. Puede habilitar el servicio cambiando el tipo de ejecución del servicio de Auto Deploy.
- 4 En el inventario, desplácese al sistema vCenter Server.

- 5 En la pestaña Administración, seleccione **Configuración** y haga clic en **Auto Deploy**.
- 6 Haga clic en el vínculo **Descargar TFTP Boot Zip** para descargar el archivo de configuración de TFTP.
- 7 Guarde el archivo `Deploy-tftp.zip` en el directorio `TFTP_Root` que creó al instalar el servidor TFTP y descomprima el archivo.
- 8 Minimice el explorador web que está utilizando con vSphere Web Client.

Pasos siguientes

Prepare el almacén desde el que Auto Deploy recupera el software ESXi cuando aprovisiona los hosts. Consulte [Preparar el almacén de software de ESXi](#).

Preparar el almacén de software de ESXi

Auto Deploy aprovisiona hosts con imágenes descritas por perfiles de imágenes. Los perfiles de imágenes se almacenan en almacenes de software. Debe asegurarse de que esté disponible el perfil de imagen correcto antes de iniciar el aprovisionamiento de los hosts.

El almacén de software de ESXi contiene los perfiles de imágenes y paquetes de software (VIB) que se usan para ejecutar ESXi. Un perfil de imágenes es una lista de VIB. Esta configuración de prueba de concepto utiliza un almacén y perfil de imagen que proporciona VMware y no crea perfiles de imágenes personalizados.

Esta configuración de prueba de concepto descarga el archivo ZIP que contiene el perfil de imágenes. En su lugar, puede apuntar el servidor Auto Deploy hacia la dirección URL HTTP de un perfil de imágenes.

Si requiere VIB personalizados como controladores personalizados en su perfil de imágenes, puede crear un perfil de imágenes personalizado usando Image Builder PowerCLI.

Los pasos de esta tarea le indican que ejecute cmdlets de PowerCLI. Para obtener información adicional sobre cada cmdlet, escriba el `Help cmdlet de Ayuda` en la línea de comandos de PowerCLI o busque el centro de documentación de vSphere.

Requisitos previos

- Compruebe que el sistema cumpla con los requisitos de la lista de comprobación previa a la instalación. Consulte [Lista de verificación previa a la instalación de prueba de concepto](#).
- Realice todas las tareas previas de configuración de prueba de concepto. Consulte [Configurar prueba de concepto de Auto Deploy](#) para obtener la lista completa.

Procedimiento

- 1 Inicie sesión en la consola del sistema Windows en la que vCenter Server está instalado con privilegios de administrador, en forma directa o mediante RDP.

- 2 Descargue el archivo ZIP del almacén de ESXi desde el sitio web de VMware en una ubicación a la que el sistema PowerCLI Windows pueda acceder.

El archivo tiene un nombre que sigue este patrón: `VMware-Esxi-N.N.N-xxxxx-depot.zip`.

- 3 Guarde el archivo ZIP en su unidad D:\ local o cualquier volumen con suficiente espacio y anote la ubicación del archivo.
- 4 Inicie una sesión de PowerCLI y ejecute los siguientes cmdlets en la línea de comandos.

```
Connect-VIServer -Server your_vc_hostname -User username -Password password <Enter>
Add-EsxSoftwareDepot path:\VMware-Esxi-version-xxxxx-depot.zip <Enter>
```

Incluya la ruta de acceso y el nombre de archivo completos del archivo ZIP que descargó.

El almacén de software en línea de VMware se encuentra en <https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml>.

- 5 Confirme que haya agregado correctamente el archivo ZIP en el almacén marcando los contenidos del almacén con el cmdlet `Get-EsxImageProfile`.

```
Get-EsxImageProfile <Enter>
```

El cmdlet devuelve información sobre todos los perfiles de imágenes en el almacén.

Pasos siguientes

Configure Auto Deploy para aprovisionar el primer host y hacerlo con el perfil de imágenes en el almacén. Consulte [Configurar el primer host y aprovisionar con Auto Deploy](#).

Configurar el primer host y aprovisionar con Auto Deploy

Para configurar el primer host, es necesario comprender cómo escribir reglas de Auto Deploy con vSphere PowerCLI. Después de escribir las reglas y agregarlas al conjunto de reglas, puede encender el host para aprovisionarlo.

Puede usar la interfaz de la línea de comandos de PowerCLI para especificar la manera en que Auto Deploy aprovisiona los hosts de destino. Debe definir reglas y agregarlas al conjunto de reglas activo. El servidor Auto Deploy comprueba el conjunto de reglas para determinar qué perfil de imagen se debe enviar a cada host ESXi, qué perfil de host se debe enviar a cada host ESXi y en qué ubicación de vCenter Server se debe colocar el host.

Una regla permite especificar los siguientes parámetros.

Parámetro	Descripción
Nombre	Nombre de la regla, especificado mediante el parámetro <code>-Name</code> .
Elemento	Un elemento o más, especificados mediante el parámetro <code>-Item</code> . Un elemento puede ser un perfil de imagen que se debe usar, un perfil de host que se debe usar o una ubicación en el inventario de vCenter Server (centro de datos, carpeta o clúster) para el host de destino. Puede especificar varios elementos, separados por comas.
Patrón	<p>El patrón especifica el host o el grupo de hosts a los que se aplica la regla. Seleccione una de las siguientes opciones:</p> <p>vendor</p> <p>Nombre del proveedor de la máquina.</p> <p>model</p> <p>Nombre del modelo de la máquina.</p> <p>serie</p> <p>Número de serie de la máquina.</p> <p>hostname</p> <p>Nombre de host de la máquina.</p> <p>domain</p> <p>Nombre del dominio.</p> <p>ipv4</p> <p>Dirección IPv4 de la máquina.</p> <p>mac</p> <p>Dirección MAC de NIC de arranque.</p> <p>asset</p> <p>Etiqueta de recurso de la máquina.</p> <p>oemstring</p> <p>Cadenas específicas del fabricante del equipo original (OEM) en el SMBIOS.</p> <p>Especifique el parámetro <code>-AllHosts</code> para aplicar el elemento o los elementos a todos los hosts.</p>

Esta configuración de prueba de concepto primero usa el parámetro `-AllHosts` y, a continuación, usa una dirección IP para identificar los hosts que se deben aprovisionar.

Escribir reglas para el primer host

Si desea especificar el perfil de imagen que aprovisionará el host, utilice PowerCLI para escribir una regla y agregue la regla al conjunto de reglas activo.

Esta tarea supone que el usuario tiene conocimientos básicos de Microsoft PowerShell y vSphere PowerCLI.

Requisitos previos

- Compruebe que el sistema cumpla con los requisitos de la lista de comprobación previa a la instalación. Consulte [Lista de verificación previa a la instalación de prueba de concepto](#).
- Realice todas las tareas previas de configuración de prueba de concepto. Consulte [Configurar prueba de concepto de Auto Deploy](#) para obtener la lista completa.
- Asegúrese de que pueda acceder al software ESXi desde el sistema en el que ejecuta los cmdlets de PowerCLI.

Procedimiento

- 1 Inicie sesión en la consola del sistema Windows en la que vCenter Server está instalado con privilegios de administrador, en forma directa o mediante RDP.

Esta tarea supone que el usuario ha instalado PowerCLI en el sistema en el que se ejecuta vCenter Server.

- 2 Abra la ventana PowerCLI y despliegue una lista de los perfiles de imagen de ESXi.

Get-EsxImageProfile

- 3 Cree una nueva regla mediante el siguiente cmdlet, reemplazando ESXi-5.1.0-XXXXX-standard por el perfil de imagen que desea utilizar.

New-DeployRule -Name "InitialBootRule" -Item "Esxi-5.1.0-XXXXX-standard" -AllHosts

- 4 Agregue la nueva regla al conjunto de reglas activo con la finalidad de que la regla esté disponible para el servidor Auto Deploy.

Add-DeployRule -DeployRule "InitialBootRule"

Pasos siguientes

Arranque el host y compruebe que Auto Deploy aprovisione el host y lo agrega al inventario de vCenter Server. Consulte [Aprovisionar el primer host](#).

Aprovisionar el primer host

Puede aprovisionar el primer host y controlar su ubicación en vCenter Server para completar la comprobación del aprovisionamiento de imagen de la configuración.

Requisitos previos

- Compruebe que el sistema cumpla con los requisitos de la lista de comprobación previa a la instalación. Consulte [Lista de verificación previa a la instalación de prueba de concepto](#).
- Realice todas las tareas previas de configuración de prueba de concepto. Consulte [Configurar prueba de concepto de Auto Deploy](#) para obtener la lista completa.

Procedimiento

- 1 Abra una sesión de consola en el host físico que desee utilizar como el primer host ESXi de destino, arranque el host y busque mensajes que indiquen un arranque iPXE correcto.

Durante el proceso de arranque, DHCP asigna una dirección IP al host. La dirección IP coincide con uno de los nombres que especificó anteriormente en el servidor DNS. El host se pone en contacto con el servidor Auto Deploy y descarga los archivos binarios de ESXi desde la URL de HTTP indicada en el archivo tramp de iPXE que descargó al directorio TFTP_Root anteriormente. Cada instancia de Auto Deploy produce un conjunto de archivos personalizado para el servidor TFTP.

- 2 Conéctese al sistema vCenter Server con vSphere Web Client.

En esta configuración de prueba de concepto, el sistema vCenter Server es localhost.

- 3 Haga clic en **Hosts y clústeres**.

- 4 Compruebe que el host recién aprovisionado esté en el inventario de vCenter Server en el nivel del centro de datos.

De forma predeterminada, Auto Deploy agrega hosts en ese nivel cuando finaliza el proceso de arranque.

Pasos siguientes

Si tiene algún problema, consulte [Solucionar problemas de Auto Deploy](#).

Configure el primer host para utilizar como referencia y guarde su perfil de host para utilizar con otros hosts. Consulte [Configurar el host de referencia de prueba de concepto](#).

Configurar el host de referencia de prueba de concepto

Puede personalizar el primer host ESXi que arranque para su entorno y crear un perfil de host. Puede configurar Auto Deploy para aprovisionar otros hosts de destino con dicho perfil de host. El host ESXi desde el que crea el perfil de host se considera su host de referencia o host de plantilla.

La forma en la que configura el host de referencia depende de qué desea realizar.

Configuración compartida

Especifique la configuración que comparten todos los hosts y guarde un perfil de host para el host.

Configuración específica del host

Personalice los hosts configurando el perfil de host para solicitar al usuario la entrada de una cantidad limitada de opciones, como una dirección IP estática. Las personalizaciones del host se almacenan cuando se guarda el perfil de host. Consulte [Personalizar hosts en vSphere Web Client](#).

Auto Deploy se aplica a todas las configuraciones comunes desde el perfil de host en todos los hosts de destino. Si configura el perfil de host para solicitar la entrada del usuario, todos los hosts aprovisionados con dicho perfil de host aparecen en el modo de mantenimiento. Debe volver a aplicar el perfil de host o restablecer las personalizaciones del host para solicitar información específica del host.

Nota Los administradores no pueden acceder ni manipular directamente las personalizaciones del host. Utilice la interfaz de usuario de Host Profiles de vSphere Web Client para trabajar con personalizaciones del host.

Requisitos previos

- Compruebe que el sistema cumpla con los requisitos de la lista de comprobación previa a la instalación. Consulte [Lista de verificación previa a la instalación de prueba de concepto](#).
- Realice todas las tareas previas de configuración de prueba de concepto. Consulte [Configurar prueba de concepto de Auto Deploy](#) para obtener la lista completa.

Procedimiento

- 1 Utilice vSphere Web Client para conectarse al sistema vCenter Server.
En esta configuración de prueba de concepto, el sistema vCenter Server es localhost.
- 2 Haga clic en Hosts y clústeres y seleccione el host que Auto Deploy agregó al primer centro de datos.
- 3 Configure el host.

En el resto de la configuración de prueba de concepto se supone que configura al menos una configuración que es diferente para los distintos hosts.

Configuración	Descripción
Redes	Configure los siguientes componentes de conexión de red. <ul style="list-style-type: none"> ■ Conmutador virtual base y grupo de puertos de administración para VMkernel. ■ Grupo de puertos de red de almacenamiento para VMkernel. ■ Grupo de puertos de conexión de red de máquinas virtuales. ■ Cualquier conmutador virtual adicional y grupo de puertos. ■ Conmutadores distribuidos, si es necesario (transfiera grupos de puertos a conmutadores distribuidos si los utiliza).
Almacenamiento	Configure el almacenamiento compartido.
Configuración de hora	Ajuste la configuración de hora.
Seguridad	Configure el perfil de seguridad.
Autenticación	Configure la autenticación.
DNS y enrutamiento	Si es necesario, ajuste la configuración de DNS y enrutamiento.
Otro	Ajuste la configuración avanzada o cualquier otra configuración según se requiera en el entorno de destino.

Pasos siguientes

Cree el perfil de host desde el host de referencia para su uso con todos los demás hosts de destino. Consulte la documentación sobre *Host Profiles*.

Crear y aplicar un perfil de host con vSphere Web Client

La configuración que comparte un grupo de hosts se almacena en un perfil de host. Puede crear el perfil de host a partir de cualquier host de referencia. La configuración que varía en los distintos hosts, como la dirección IP estática, se puede administrar a través del mecanismo de personalización de host.

Auto Deploy puede aprovisionar todos los hosts con el mismo perfil. En algunos casos, Auto Deploy también utiliza personalizaciones de host que permiten especificar información diferente en los distintos hosts. Por ejemplo, si configura un puerto VMkernel para vMotion o para almacenamiento, puede especificar una dirección IP estática para el puerto mediante el mecanismo de personalización de host.

En este ejemplo, debe extraer un perfil de host de un host de referencia, asociar ese perfil con otro host y comprobar el cumplimiento del perfil de host. En la mayoría de los casos, no debe realizar estas tareas en forma manual sino que debe escribir una regla de Auto Deploy que aplique el perfil de host a todos los hosts que se aprovisionen con Auto Deploy. Consulte [Escribir una regla y asignar un perfil de host a hosts](#).

Requisitos previos

- Compruebe que el sistema cumpla con los requisitos de la lista de comprobación previa a la instalación. Consulte [Lista de verificación previa a la instalación de prueba de concepto](#).
- Realice todas las tareas previas de configuración de prueba de concepto. Consulte [Configurar prueba de concepto de Auto Deploy](#) para obtener la lista completa.

Procedimiento

- 1 Inicie sesión en vSphere Web Client conectado al sistema vCenter Server con privilegios de administrador.
- 2 Haga clic en **Reglas y perfiles** y seleccione **Perfiles de host**.
- 3 Haga clic en el icono Extraer perfil del host y responda las solicitudes del asistente.

Opción	Descripción
Seleccionar host	Seleccione el nombre del host de referencia que configuró anteriormente.
Nombre y descripción	Asigne el nombre ESXiGold al perfil y agregue una descripción.
Listo para finalizar	Revise la información y haga clic en Finalizar .

- 4 Haga clic con el botón derecho en el perfil de host ESXiGold, seleccione **Asociar o separar hosts y clústeres**.

- 5 Seleccione el host ESXi con el que desea asociar el perfil y haga clic en **Asociar** y, a continuación, en **Siguiente**.

El asistente cargará la personalización del host.

- 6 Proporcione la información sobre personalización y haga clic en **Finalizar**.

Pasos siguientes

Cree una regla que asigne el perfil de imagen y el perfil de host recién creado a todos los hosts que desee aprovisionar con Auto Deploy. Consulte [Crear una regla para otros hosts de destino](#).

Crear una regla para otros hosts de destino

Puede crear una regla que aplique el perfil de imagen previamente comprobado y el perfil de host que acaba de crear a todos los hosts de destino.

Esta tarea supone que el usuario tiene conocimientos básicos de Microsoft PowerShell y vSphere PowerCLI.

Requisitos previos

- Compruebe que el sistema cumpla con los requisitos de la lista de comprobación previa a la instalación. Consulte [Lista de verificación previa a la instalación de prueba de concepto](#).
- Realice todas las tareas previas de configuración de prueba de concepto. Consulte [Configurar prueba de concepto de Auto Deploy](#) para obtener la lista completa.

Procedimiento

- 1 Inicie sesión en la consola del sistema Windows en la que vCenter Server está instalado con privilegios de administrador, en forma directa o mediante RDP.
- 2 Inicie una sesión de PowerCLI e introduzca en el símbolo del sistema los siguientes comandos seguidos de Intro.

```
Connect-VIServer -Server your_vc_hostname -User username -Password password
Add-EsxSoftwareDepot path:\VMware-Esxi-version-xxxxx-depot.zip
```

Incluya la ruta completa y el nombre del archivo ZIP que descargó previamente. Se requiere agregar el almacén de software cada vez que inicie una sesión nueva de PowerCLI.

- 3 (Opcional) Para mostrar las reglas del tipo de conjunto de reglas activo, introduzca el siguiente cmdlet en el símbolo del sistema y presione Intro.

```
Get-DeployRuleset
```

- Para crear una regla que haga que Auto Deploy aprovisione el conjunto de hosts en el rango de IP especificado con la imagen seleccionada y con el perfil de host creado a partir del host de referencia, introduzca el siguiente comando y presione Intro.

```
New-DeployRule -name "Production01Rule" -item "image_profile",  
ESXiGold,target_cluster -Pattern "ipv4=IP_range"
```

Opción	Descripción
image_profile	El perfil de imagen de ESXi que utilizó en la primera regla de implementación.
target_cluster	El nombre del clúster en vCenter Server al que desea agregar todos los hosts.
IP_range	Introduzca una sola dirección IP o un rango de direcciones IP para los hosts que desea aprovisionar con el perfil de imagen y el perfil de host.

Cuando especifique un clúster de destino, el perfil de host se aplica a todos los hosts del clúster. No se requiere la aplicación del perfil de host a cada host.

- Agregue la nueva regla al conjunto de reglas activo.

```
Add-DeployRule -DeployRule "Production01Rule" <Enter>
```

- (Opcional) Elimine la regla de implementación que ha creado para la operación de arranque inicial.

```
Remove-DeployRule -DeployRule InitialBootRule <Enter>
```

- Compruebe el conjunto de reglas activo.

```
Get-DeployRuleset<Enter>
```

PowerCLI muestra información similar al siguiente ejemplo.

```
Name:                Production01Rule
PatternList:         {ipv4=address_range}
ItemList:            {ESXi-version-XXXXXX-standard, Compute01, ESXiGold}
```

Pasos siguientes

Aprovisione todos los hosts y configure las personalizaciones del host para cada host. Consulte [Aprovisionar todos los hosts y configurar personalizaciones de host](#).

Aprovisionar todos los hosts y configurar personalizaciones de host

Con la regla que aprovisiona los hosts mediante un perfil de imagen y con el perfil de host creado desde el host de referencia disponible, puede aprovisionar todos los hosts de destino. Si algún elemento del perfil de host está configurado para solicitar la intervención del usuario, el host se activa en modo de mantenimiento. Debe aplicar el perfil de host o comprobar el cumplimiento de host para que se le pida la información. El sistema asocia la personalización del host con el host.

Requisitos previos

- Compruebe que el sistema cumpla con los requisitos de la lista de comprobación previa a la instalación. Consulte [Lista de verificación previa a la instalación de prueba de concepto](#).
- Realice todas las tareas previas de configuración de prueba de concepto. Consulte [Configurar prueba de concepto de Auto Deploy](#) para obtener la lista completa.
- Abra una consola para cada host que desee aprovisionar a fin de supervisar el progreso del arranque.

Procedimiento

- 1 Arranque los hosts restantes.

Auto Deploy arranca los hosts, aplica el perfil de host y agrega los hosts al inventario de vCenter Server. Los hosts permanecen en el modo de mantenimiento, dado que el perfil de host de referencia está configurado para solicitar la intervención del usuario para cada host.

- 2 Conéctese al sistema vCenter Server con vSphere Web Client.
- 3 Haga clic en **Inicio** y seleccione **Perfiles de host**.
- 4 En el panel de la izquierda, seleccione el perfil ESXiGold y agregue los hosts recién arrancados en ese perfil.
- 5 Aplique el perfil de host a cada uno de los hosts, proporcione la información de intervención del usuario y reinicie cada host.

Una vez finalizado el progreso de reinicio, todos los hosts están en ejecución con la imagen que especifica y utiliza la configuración del perfil de host de referencia. El clúster muestra que todos los hosts son totalmente compatibles.

Resultados

Ahora todos los hosts están configurados con información compartida a través del perfil de host de referencia y con la información específica del host a través del mecanismo de personalización de host. La próxima vez que arranque los hosts, estos recuperarán la información y arrancarán completamente.

Pasos siguientes

Una vez finalizada la implementación de prueba de concepto correctamente, puede comenzar a planificar la configuración de producción.

Usar vSphere ESXi Image Builder

vSphere ESXi Image Builder es un conjunto de cmdlets de vSphere PowerCLI que pueden usarse para administrar paquetes de VIB y perfiles de imagen de vSphere, como VIB de controladores y VIB de actualización. También puede usar cmdlets de vSphere ESXi Image Builder para exportar un perfil de imagen a un archivo ZIP de almacén sin conexión o un archivo ISO que puede usar para instalar ESXi con un conjunto personalizado de actualizaciones, revisiones y controladores.

Información sobre vSphere ESXi Image Builder

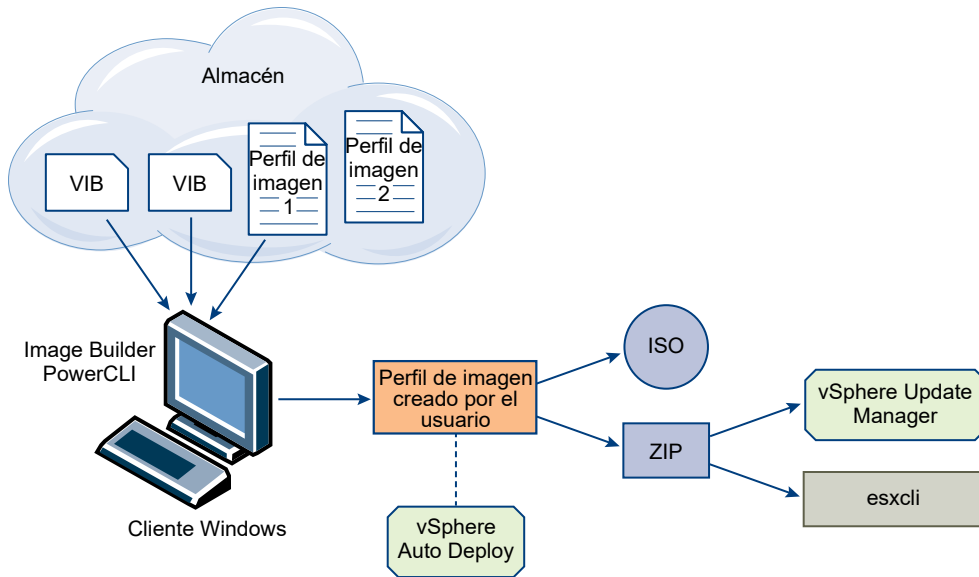
Puede utilizar VMware vSphere® ESXi™ Image Builder CLI para administrar almacenes de software, perfiles de imagen y paquetes de software (VIB). Los perfiles de imagen y los VIB especifican el software que desea utilizar durante la instalación o actualización de un host ESXi.

Descripción general de vSphere ESXi Image Builder

vSphere ESXi Image Builder permite administrar perfiles de imágenes y VIB de vSphere.

Los VIB son paquetes de software; los perfiles de imágenes contienen un conjunto de paquetes de software. Consulte [Almacenes de software y sus componentes](#).

Figura 4-6. Arquitectura de Image Builder



Puede usar cmdlets de vSphere ESXi Image Builder a fin de administrar el software para implementar en los hosts ESXi en varias situaciones diferentes.

Tabla 4-14. Casos en los que se puede utilizar vSphere ESXi Image Builder

Caso de uso para vSphere ESXi Image Builder	Descripción
Crear perfiles de imágenes para que use vSphere Auto Deploy	Use vSphere ESXi Image Builder para crear un perfil de imagen que defina los VIB que vSphere Auto Deploy emplea para aprovisionar hosts.
Agregar controladores de terceros personalizados a un perfil de imagen existente y exportarlos a un ISO o paquete	Quando agregue un controlador de terceros o VIB personalizados de extensión a sus hosts ESXi, use vSphere ESXi Image Builder para clonar la imagen base que proporcione VMware, agregue los VIB personalizados y expórtelos a un archivo ISO o un archivo ZIP en paquete sin conexión.

Tabla 4-14. Casos en los que se puede utilizar vSphere ESXi Image Builder (continuación)

Caso de uso para vSphere ESXi Image Builder	Descripción
Realización de actualizaciones	Si actualiza desde un sistema 4.0 o 4.1 que incluye extensiones o controladores personalizados, puede usar vSphere ESXi Image Builder para crear un perfil de imagen que incluya el VIB base de vSphere 5. Puede crear VIB de vSphere 5 para las extensiones personalizadas y agregar dichos VIB al VIB base. Exporte el perfil de imagen personalizado a un archivo ISO que puede instalar o un archivo ZIP que puede usar con vSphere Update Manager.
Creación de imágenes personalizadas con tamaño reducido	Si requiere una imagen de tamaño mínimo, puede clonar el perfil de imagen base de ESXi y quitar VIB mediante vSphere ESXi Image Builder.

Los cmdlets de vSphere ESXi Image Builder toman perfiles de imágenes y VIB como archivo de entrada y producen diversos archivos de salida.

Tabla 4-15. Archivos de entrada y salida de los cmdlets de vSphere ESXi Image Builder

Parámetro	Descripción
Archivo de entrada	Los perfiles de imágenes y los VIB se encuentran ubicados en un almacén de software y se usan como archivos de entrada para cmdlets de vSphere PowerCLI que se ejecutan en un cliente de Windows.
Archivos de salida	Los cmdlets de vSphere PowerCLI crean perfiles de imágenes personalizados que se pueden exportar a un archivo de imagen ISO o un archivo ZIP de almacén sin conexión. Para la instalación se usan imágenes ISO. El almacén de ZIP puede usarse mediante Update Manager o a través de comandos <code>esxcli software</code> para actualizar o instalar imágenes. Los perfiles de imágenes también se usan en reglas de vSphere Auto Deploy para personalizar el software con que se aprovisionan los hosts ESXi.

Vea el vídeo *Uso de Image Builder CLI* para obtener información sobre vSphere ESXi Image Builder:



Using Image Builder CLI

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vvb0gt3i/uiConfId/49694343/)

Almacenes de software y sus componentes

Comprender cómo están estructurados los almacenes, perfiles y VIB y dónde puede utilizarlos es un requisito previo para la instalación en la memoria de una imagen ISO personalizada de ESXi, para el aprovisionamiento de hosts ESXi con vSphere Auto Deploy y para determinadas operaciones de actualización personalizadas.

Los siguientes términos técnicos se utilizan en toda la documentación de vSphere en asuntos relacionados con tareas de instalación y actualización.

VIB

Un VIB es un paquete de software de ESXi. VMware y sus soluciones de paquetes de partners, controladores, proveedores de CIM y aplicaciones que extienden la plataforma de ESXi como VIB. Los VIB están disponibles en almacenes de software. Puede usar VIB para crear y personalizar imágenes ISO o para actualizar hosts ESXi mediante la instalación de VIB de forma asincrónica en los hosts.

Consulte [Propiedades del objeto SoftwarePackage](#).

Perfil de imagen

Un perfil de imagen define una imagen de ESXi y consta de VIB. Un perfil de imagen incluye un VIB base y también podría incluir más VIB. Es posible analizar y definir un perfil de imagen mediante vSphere ESXi Image Builder.

Consulte [Propiedades del objeto ImageProfile](#).

Almacén de software

Un almacén de software es una colección de VIB y perfiles de imagen. El almacén de software es una jerarquía de archivos y carpetas, y puede estar disponible a través de una URL HTTP (almacén en línea) o un archivo ZIP (almacén sin conexión). Los partners VMware y VMware se encargan de que los almacenes estén disponibles. Las compañías con instalaciones de VMware grandes podrían crear almacenes internos para aprovisionar hosts ESXi con vSphere Auto Deploy o para exportar un imagen ISO para la instalación de ESXi.

Descripción general de cmdlets de vSphere ESXi Image Builder

Los cmdlets de vSphere ESXi Image Builder permiten administrar perfiles de imagen y VIB.

vSphere ESXi Image Builder incluye los siguientes cmdlets.

Nota Durante la ejecución de cmdlets de vSphere ESXi Image Builder, al invocar el cmdlet, proporcione todos los parámetros en la línea de comandos. No se recomienda proporcionar parámetros en modo interactivo.

Ejecute `Get-Help cmdlet_name` en el símbolo de vSphere PowerCLI para obtener información de referencia detallada.

Tabla 4-16. Cmdlets de vSphere ESXi Image Builder

Cmdlet	Descripción
Add-EsxSoftwareDepot	Agregar el almacén de software o el archivo ZIP en la ubicación especificada del entorno actual. Descarga metadatos del almacén y analiza los VIB para comprobar si tienen dependencias.
Remove-EsxSoftwareDepot	Se desconecta del almacén de software especificado.

Tabla 4-16. Cmdlets de vSphere ESXi Image Builder (continuación)

Cmdlet	Descripción
Get-EsxSoftwareDepot	Devuelve una lista de almacenes de software que se encuentran en el entorno actual. Si desea examinar y administrar perfiles de imagen y VIB, primero debe agregar el almacén de software correspondiente al entorno.
Get-EsxSoftwarePackage	Devuelve una lista de objetos de paquete de software (VIB). Utilice estas opciones del cmdlet para filtrar los resultados.
Get-EsxImageProfile	Devuelve una matriz de objetos ImageProfile de todos los almacenes agregados actualmente.
New-EsxImageProfile	Crea un nuevo perfil de imagen. En la mayoría de los casos, se recomienda crear un nuevo perfil mediante la clonación de un perfil existente. Consulte Clonar un perfil de imagen .
Set-EsxImageProfile	Modifica un objeto ImageProfile local y realiza pruebas de validación en el perfil modificado. El cmdlet devuelve el objeto modificado pero no lo conserva.
Export-EsxImageProfile	Exporta un perfil de imagen como una imagen ISO de ESXi para instalar ESXi, o bien como un archivo ZIP.
Compare-EsxImageProfile	Devuelve una estructura ImageProfileDiff que muestra si dos perfiles tienen la misma lista de VIB y el mismo nivel de aceptación. Consulte Niveles de aceptación .
Remove-EsxImageProfile	Elimina el perfil de imagen del almacén de software.
Add-EsxSoftwarePackage	Agrega uno o más paquetes (VIB) nuevos a un perfil de imagen existente.
Remove-EsxSoftwarePackage	Elimina uno o más paquetes (VIB) de un perfil de imagen.

Perfiles de imagen

Los perfiles de imagen definen el conjunto de VIB que utiliza un proceso de instalación o actualización de ESXi. Los perfiles de imagen se aplican a hosts aprovisionados con vSphere Auto Deploy y a otros hosts ESXi 5.x. El usuario define y manipula los perfiles de imagen con vSphere ESXi Image Builder.

Requisitos de los perfiles de imagen

Puede crear un perfil de imagen personalizado desde cero o clonar uno existente y agregarle o quitarle VIB. Para que sean válidos, los perfiles deben cumplir los siguientes requisitos.

- Cada perfil de imagen debe tener una combinación de nombre y proveedor única.
- Además, cada uno tiene un nivel de aceptación. Cuando agrega un VIB a un perfil de imagen con un cmdlet de vSphere ESXi Image Builder, este programa comprueba que el VIB coincida con el nivel de aceptación definido para el perfil.
- No puede quitar VIB que son necesarios para otros VIB.
- Tampoco puede incluir dos versiones del mismo VIB en un perfil de imagen. Cuando se agrega una nueva versión de un VIB, esta reemplaza a la versión existente.

Validar un perfil de imagen

Para que sean válidos, los perfiles de imagen y sus VIB deben cumplir varios criterios.

- Los perfiles de imagen deben contener al menos un VIB de base y un módulo de kernel de arranque.
- Si algún VIB del perfil de imagen depende de otro VIB, este otro también tendrá que estar incluido en el perfil de imagen. Los creadores de VIB almacenan esa información en la propiedad Depends del objeto SoftwarePackage.
- Los VIB no deben entrar en conflicto entre sí. Los creadores de VIB almacenan la información sobre conflictos en la propiedad Conflicts del objeto SoftwarePackage.
- Dos VIB con el mismo nombre, pero de dos versiones diferentes, no pueden coexistir. Cuando se agrega una nueva versión de un VIB, esta reemplaza a la versión existente.
- Hay problemas de falta de validación del nivel de aceptación.

Cuando se realiza un cambio en un perfil de imagen, vSphere ESXi Image Builder comprueba que el cambio no invalide el perfil.

Validación de dependencias

Cuando se agrega o se quita un VIB, vSphere ESXi Image Builder comprueba que se cumplan las dependencias del paquete. Cada objeto SoftwarePackage incluye una propiedad Depends que especifica una lista de otros VIB de los que depende ese VIB. Consulte [Estructura de los objetos ImageProfile, SoftwarePackage e ImageProfileDiff](#)

Validación del nivel de aceptación

vSphere ESXi Image Builder realiza una validación del nivel de aceptación cada vez que se crea o se modifica un perfil de imagen. vSphere ESXi Image Builder comprueba el nivel de aceptación de los VIB del perfil de imagen con el nivel de aceptación mínimo permitido del perfil. El nivel de aceptación del VIB también se valida cada vez que se valida la firma de un VIB.

Validar VIB durante la exportación

Cuando se exporta un perfil de imagen a una imagen ISO, vSphere ESXi Image Builder valida todos los VIB mediante las siguientes acciones.

- Comprueba que no haya conflictos mediante la comprobación de la propiedad Conflicts de todos los objetos SoftwarePackage.
- Realiza una validación de firma de VIB. La validación de la firma evita que se realicen modificaciones no autorizadas a los paquetes de VIB. La firma es una suma de comprobación criptográfica que garantiza que un determinado autor produjo el VIB. La validación de la firma también se lleva a cabo durante la instalación de VIB en un host ESXi y cuando el servidor vSphere Auto Deploy utiliza VIB.

- Comprueba que los VIB respeten las reglas de uso de rutas de archivo. VMware prueba los VIB VMwareCertified y VMwareAccepted para garantizar que estos respeten siempre las reglas de uso de rutas de archivo.

Niveles de aceptación

Cada VIB se lanza con un nivel de aceptación que no se puede cambiar. El nivel de aceptación del host determina qué VIB pueden instalarse en un host. Puede cambiar los niveles de aceptación del host mediante los comandos de `esxcli`.

VMware admite los siguientes niveles de aceptación.

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.

Estructura de los objetos ImageProfile, SoftwarePackage e ImageProfileDiff

Conocer la estructura de los objetos `ImageProfile`, `SoftwarePackage` y `ImageProfileDiff` ayuda a administrar los procesos de implementación y actualización.

Propiedades del objeto ImageProfile

El objeto `ImageProfile`, al que se puede acceder con el cmdlet de `Get-
EsxImageProfilevSphere` PowerCLI, posee las siguientes propiedades.

Nombre	Tipo	Descripción
<code>AcceptanceLevel</code>	<code>AcceptanceLevel</code>	Determina qué VIB se pueden agregar al perfil. Los niveles son <code>VMwareCertified</code> , <code>VMwareAccepted</code> , <code>PartnerSupported</code> y <code>CommunitySupported</code> . Consulte Niveles de aceptación .
<code>Author</code>	<code>System.String</code>	La persona que creó el perfil. 60 caracteres o menos.
<code>CreationTime</code>	<code>System.DateTime</code>	Marca de hora de creación.
<code>Description</code>	<code>System.String</code>	La descripción de texto completo del perfil. Sin límite de longitud.
<code>GUID</code>	<code>System.String</code>	Identificador único global del perfil de imagen.
<code>ModifiedTime</code>	<code>System.DateTime</code>	Marca de hora de la última modificación.
<code>Name</code>	<code>System.String</code>	Nombre del perfil de imagen. 80 caracteres o menos.
<code>ReadOnly</code>	<code>System.Boolean</code>	Cuando se establece en <code>true</code> , el perfil no se puede editar. Utilice <code>Set- EsxImageProfile -ReadOnly</code> para lograr que los perfiles de imagen personalizados sean de solo lectura.
<code>Rules</code>	<code>ImageProfileRule[]</code>	Cualquier restricción o requisito de hardware OEM que el perfil de imagen podría tener. vSphere Auto Deploy verifica el valor de esta propiedad al implementar un perfil de imagen, e implementa el perfil si se encuentra disponible hardware coincidente.
<code>Vendor</code>	<code>System.String</code>	La organización que publica el perfil. 40 caracteres o menos.
<code>VibList</code>	<code>SoftwarePackage[]</code>	La lista de identificadores de VIB que la imagen contiene.

Propiedades del objeto SoftwarePackage

Al preparar un perfil de imagen, puede examinar los paquetes de software para decidir qué paquetes son adecuados para la inclusión. El objeto `SoftwarePackage` posee las siguientes propiedades.

Nombre	Tipo	Descripción
AcceptanceLevel	AcceptanceLevel	El nivel de aceptación de este VIB.
Conflicts	SoftwareConstraint[]	Una lista de VIB que no se pueden instalar al mismo tiempo que este VIB. Cada limitación utiliza el siguiente formato: package-name[<< < = > = >> >>version]
Depends	SoftwareConstraint[]	Una lista de VIB que deben instalarse al mismo tiempo que este VIB. Mismo formato de limitación que la propiedad Conflicts.
Description	System.String	La descripción extensa de VIB.
Guid	System.String	El identificador único del VIB.
LiveInstallOk	System.Boolean	Valor "True" si se admiten las instalaciones activas en este VIB.
LiveRemoveOk	System.Boolean	Valor "True" si se admiten las eliminaciones activas en este VIB.
MaintenanceMode	System.Boolean	Valor "True" si los hosts deben estar en el modo de mantenimiento para la instalación de este VIB.
Name	System.String	Nombre del VIB. Generalmente describe de forma exclusiva al paquete en un sistema ESXi en ejecución.
Provides	SoftwareProvides	La lista de paquetes virtuales o interferencias que este VIB proporciona. Consulte Propiedades del objeto SoftwareProvide .
ReferenceURLs	SupportReference[]	La lista de objetos SupportReference con información de apoyo exhaustiva. El objeto SupportReference posee dos propiedades, Title y URL, ambas del tipo System.String.
Replaces	SoftwareConstraint[]	La lista de objetos SoftwareConstraint que identifica a los VIB que reemplazan a este VIB o lo vuelven obsoleto. Los VIB reemplazan automáticamente a los VIB con el mismo nombre, pero de versiones anteriores.
ReleaseDate	System.DateTime	Fecha y hora de publicación o lanzamiento del VIB.
SourceUrls	System.String[]	La lista de URL de origen desde la que se puede descargar este VIB.

Nombre	Tipo	Descripción
StatelessReady	System.Boolean	Valor "True" si el paquete es compatible con perfiles de host u otras tecnologías que permiten que sea adecuado para la utilización en conjunto con vSphere Auto Deploy.
Summary	System.String	Resumen de una línea del VIB.
Tags	System.String[]	Matriz de etiquetas de cadenas para este paquete definido por el proveedor o editor. Las etiquetas pueden utilizarse para identificar características del paquete.
Vendor	System.String	Proveedor o editor del VIB.
Version	System.String	Versión del VIB.
VersionObject	Software.Version	La propiedad VersionObject es del tipo SoftwareVersion. La clase SoftwareVersion implementa un método Compare estático para comparar dos versiones de cadenas. Consulte Propiedades del objeto SoftwareVersion

Propiedades del objeto ImageProfileDiff

Cuando ejecute el cmdlet `Compare-EsxImageProfile`, puede transferir dos parámetros, primero el perfil de referencia y, a continuación, el perfil de comparación. El cmdlet devuelve un objeto `ImageProfileDiff`, que posee las siguientes propiedades.

Nombre	Tipo	Descripción
CompAcceptanceLevel	System.String	El nivel de aceptación para el segundo perfil que se transfirió a <code>Compare-EsxImageProfile</code> .
DowngradeFromRef	System.String[]	La lista de VIB en el segundo perfil que son degradaciones de los VIB del primer perfil.
Equal	System.Boolean	Valor <code>True</code> si los dos perfiles de imagen poseen paquetes y niveles de aceptación idénticos.
OnlyInComp	System.String	La lista de VIB encontrados solo en el segundo perfil que se transfirió a <code>Compare-EsxImageProfile</code> .
OnlyInRef	System.String[]	La lista de VIB encontrados solo en el primer perfil que se transfirió a <code>Compare-EsxImageProfile</code> .

Nombre	Tipo	Descripción
PackagesEqual	System.Boolean	True si los perfiles de imagen poseen conjuntos idénticos de paquetes de VIB.
RefAcceptanceLevel	System.String	El nivel de aceptación para el primer perfil que se transfirió a Compare-ExsImageProfile.
UpgradeFromRef	System.String[]	La lista de VIB en el segundo perfil que son actualizaciones de los VIB del primer perfil.

Propiedades del objeto SoftwareVersion

El objeto `SoftwareVersion` permite comparar dos cadenas de versión. El objeto incluye un método `Compare` estático que acepta dos cadenas como entrada y devuelve 1 si la primera cadena de versión es un número superior a la segunda cadena de versión. `Compare` devuelve 0 si las dos cadenas de versión son iguales. `Compare` devuelve -1 si la segunda cadena de versión es un número superior al de la primera cadena. El objeto posee las siguientes propiedades.

Nombre	Tipo	Descripción
Version	System.String	La parte de la versión antes del guión. Esta parte indica la versión principal.
Release	System.String	La parte de la versión después del guión. Esta parte indica la versión de la revisión.

Propiedades del objeto SoftwareConstraint

El objeto `SoftwareConstraint` implementa un método `MatchesProvide`. El método acepta un objeto `SoftwareProvides` o `SoftwarePackage` como entrada y devuelve `True` si la limitación coincide con `SoftwareProvide` o `SoftwarePackage` o, de lo contrario, devuelve `False`.

El objeto `SoftwareConstraint` posee las siguientes propiedades.

Nombre	Tipo	Descripción
Name	System.String	Nombre de la limitación. Este nombre debe coincidir con una propiedad <code>SoftwareProvideName</code> correspondiente.
Relation	System.String	Una enumeración o uno de los siguientes indicadores de comparación: <<, <=, =, >=, >>. Esta propiedad puede ser \$null si la limitación no posee una propiedad <code>Relation</code> y <code>Version</code> .

Nombre	Tipo	Descripción
Version	System.String	La versión para hacer coincidir la limitación. Esta propiedad puede ser \$null si la limitación no posee una propiedad Relation y Version.
VersionObject	SoftwareVersion	La versión representada por un objeto SoftwareVersion.

Propiedades del objeto SoftwareProvide

El objeto `SoftwareProvide` posee las siguientes propiedades.

Nombre	Tipo	Descripción
Name	System.String	Nombre del suministro.
Version	System.String	Versión del suministro. Puede ser \$null si el suministro no especifica una versión.
Release	System.String	La versión del suministro tal como se representa a través de un objeto <code>SoftwareVersion</code> . Consulte Propiedades del objeto SoftwareVersion .

Instalar y usar vSphere ESXi Image Builder

vSphere ESXi Image Builder está compuesto por el servidor de vSphere ESXi Image Builder y los cmdlets de PowerShell de vSphere ESXi Image Builder. El servidor de vSphere ESXi Image Builder se inicia cuando se ejecuta el primer cmdlet de vSphere ESXi Image Builder.

Instalar vSphere ESXi Image Builder y software de requisito previo

Antes de que pueda ejecutar los cmdlets de vSphere ESXi Image Builder, deberá instalar vSphere PowerCLI y todo el software de requisito previo. El complemento vSphere ESXi Image Builder se incluye con la instalación de vSphere PowerCLI.

Instale vSphere ESXi Image Builder y el software de requisito previo en un sistema Microsoft Windows.

Procedimiento

- 1 Instale Microsoft .NET 2.0 desde el sitio web de Microsoft siguiendo las instrucciones de dicho sitio web.
- 2 Instale Microsoft PowerShell 2.0 desde el sitio web de Microsoft siguiendo las instrucciones de dicho sitio web.
- 3 Instale vSphere PowerCLI, que incluye los cmdlets de vSphere ESXi Image Builder.

Consulte la *Guía de instalación de vSphere PowerCLI* para obtener instrucciones detalladas.

Pasos siguientes

Consulte [Usar los cmdlets de vSphere ESXi Image Builder](#) . Si son sus primeros pasos con vSphere PowerCLI, consulte la documentación de vSphere PowerCLI.

Utilice los cmdlets de vSphere ESXi Image Builder y otros cmdlets de vSphere PowerCLI y cmdlets de PowerShell para administrar los perfiles de imagen y VIB. Utilice `Get-Help cmdlet_name` en cualquier momento para obtener ayuda en la línea de comandos.

Usar los cmdlets de vSphere ESXi Image Builder

Los cmdlets de vSphere ESXi Image Builder se implementan como cmdlets de Microsoft PowerShell y se incluyen en vSphere PowerCLI. Los usuarios de los cmdlets de vSphere ESXi Image Builder pueden aprovechar todas las funciones de vSphere PowerCLI.

Los usuarios experimentados de PowerShell pueden utilizar los cmdlets de vSphere ESXi Image Builder al igual que otros cmdlets de PowerShell. Si estos son sus primeros pasos con PowerShell y vSphere PowerCLI, siga estos consejos.

Puede escribir cmdlets, parámetros y valores de parámetros en el shell de vSphere PowerCLI.

- Obtenga ayuda para cualquier cmdlet a través de `Get-Help cmdlet_name`.
- Recuerde que PowerShell no distingue mayúsculas de minúsculas.
- Utilice la opción de finalización con tabulación para los nombres de cmdlets y parámetros.
- Formatee cualquier variable y salida de cmdlet utilizando `Format-List` o `Format-Table` o sus formas cortas `fl` o `ft`. Consulte `Get-Help Format-List`.
- Utilice caracteres comodín para la búsqueda y filtrado de VIB y perfiles de imagen. Son compatibles todas las expresiones con comodines.

Transmitir parámetros por nombre

Puede transmitir parámetros por nombre en la mayoría de los casos y rodear los valores de parámetros que contienen espacios o caracteres especiales con comillas dobles.

```
Add-ESXSoftwarePackage -ImageProfile profile42 -SoftwarePackage "partner package 35"
```

Transmitir parámetros como objetos

Puede pasar los parámetros como objetos si desea realizar el scripting y automatización. Puede utilizar la técnica con cmdlets que devuelven varios objetos o con cmdlets que devuelven un solo objeto.

- 1 Asocie la salida de un cmdlet que devuelve varios objetos a una variable.

```
$profs = Get-ESXImageProfile
```

- 2 Cuando ejecute el cmdlet que necesita el objeto como entrada, acceda al objeto por posición, con la lista comenzando con 0.

```
Add-EsxSoftwarePackage -ImageProfile $profs[4] -SoftwarePackage partner-pkg
```

El ejemplo agrega el paquete de software especificado al quinto perfil de imagen de la lista devuelto por `Get-EsxImageProfile`.

La mayoría de los ejemplos de la documentación *Instalación y configuración de vSphere* pasan los parámetros por nombre. [Flujos de trabajo de vSphere ESXi Image Builder](#) incluye ejemplos que pasan parámetros como objetos.

Tareas comunes de vSphere ESXi Image Builder

Los cmdlets de vSphere ESXi Image Builder permiten manipular almacenes de software, perfiles de imagen y VIB.

Clonar un perfil de imagen

La clonación de un perfil publicado es la manera más sencilla de crear un perfil de imagen personalizado. La clonación de un perfil resulta especialmente útil si desea eliminar algunos VIB puntuales de un perfil, o si desea usar hosts de diferentes proveedores y quiere usar el mismo perfil básico, pero también agregar VIB de proveedores específicos. Las grandes instalaciones o los partners de VMware pueden considerar la posibilidad de crear un nuevo perfil.

Requisitos previos

- Instalar vSphere PowerCLI y todo el software necesario como requisito previo. Consulte [Instalar y usar vSphere ESXi Image Builder](#).
- Compruebe que tenga acceso al almacén de software que contiene el perfil de imagen que desea clonar.

Procedimiento

- 1 En una sesión de vSphere PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute <code>Add-EsxSoftwareDepot -DepotUrl depot_url</code> .
Archivo ZIP	<ol style="list-style-type: none"> a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code>.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

- 2 (opcional) Ejecute el cmdlet `Get-EsxImageProfile` para buscar el nombre del perfil que desea clonar.

Puede utilizar opciones de filtros con `Get-EsxImageProfile`.

- 3 Ejecute el cmdlet `New-EsxImageProfile` para crear un nuevo perfil y use el parámetro `-CloneProfile` para especificar el perfil que desea clonar.

```
New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42"
```

En este ejemplo, se clona el perfil denominado *My_Profile* y se asigna el nombre Test Profile 42. Debe especificar una combinación exclusiva de nombre y proveedor para el perfil clonado.

Pasos siguientes

Consulte [Revisar contenido de almacenes](#) para ver algunos ejemplos de filtros.

Personalice el perfil de imagen agregando o eliminando VIB. Consulte [Agregar VIB a un perfil de imagen](#).

Agregar VIB a un perfil de imagen

Puede agregar uno o más VIB a un perfil de imagen si dicho perfil de imagen no está configurado en solo lectura. Si el nuevo VIB depende de otros VIB o entra en conflicto con otros VIB del perfil, aparecerá un mensaje en el símbolo del sistema de PowerShell y no se agregará el VIB.

Puede agregar VIB desde VMware o desde partners de VMware a un perfil de imagen. Si agrega VIB de VMware, vSphere ESXi Image Builder realiza la validación. Si agrega VIB desde uno o más partners OEM de forma simultánea, no se informa de errores, pero el perfil de imagen resultante podría no funcionar. Instale los VIB desde solo un proveedor OEM al mismo tiempo.

Si aparece un error sobre problemas con el nivel de aceptación, cambie el nivel de aceptación del perfil de imagen y el nivel de aceptación del host. Considere meticulosamente si es apropiado el cambio del nivel de aceptación del host. Los niveles de aceptación de VIB se establecen durante la creación del VIB y no se pueden cambiar.

Puede agregar los VIB incluso si el perfil de imagen resultante no es válido.

Nota VMware solo puede admitir entornos y configuraciones que hayan demostrado ser estables y totalmente funcionales a través de pruebas rigurosas y exhaustivas. Utilice solo aquellas configuraciones compatibles. Puede utilizar VIB personalizados si reduce el nivel de aceptación del host y, como resultado, la compatibilidad. En dicho caso, registre los cambios realizados, a fin de que pueda revertirlos en caso de que desee eliminar los VIB personalizados y restaurar posteriormente el nivel de aceptación del host al valor predeterminado (Partner Supported). Consulte [Trabajar con niveles de aceptación](#).

Requisitos previos

Instalar vSphere PowerCLI y todo el software necesario como requisito previo. Consulte [Instalar vSphere ESXi Image Builder y software de requisito previo](#)

Procedimiento

- 1 En una sesión de vSphere PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute <code>Add-EsxSoftwareDepot -DepotUrl depot_url</code> .
Archivo ZIP	<ol style="list-style-type: none"> a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code>.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

- 2 Ejecute el cmdlet `Get-EsxImageProfile` para mostrar todos los perfiles de imagen de todos los almacenes actualmente visibles.

El cmdlet devuelve todos los perfiles disponibles. Puede limitar la búsqueda utilizando los argumentos opcionales para filtrar la salida.

- 3 Clone el perfil.

```
New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42" -Vendor "My Vendor"
```

Los perfiles de imagen publicados por VMware y sus partners son de solo lectura. Para realizar cambios, deberá clonar el perfil de imagen. Se requiere el parámetro `vendor`.

- 4 Ejecute el cmdlet `Add-EsxSoftwarePackage` para agregar un paquete nuevo a uno de los perfiles de imagen.

```
Add-EsxSoftwarePackage -ImageProfile My_Profile -SoftwarePackage partner-package
```

El cmdlet ejecuta las pruebas de validación estándares en el perfil de imagen. Si la validación es correcta, el cmdlet devuelve un perfil de imagen modificado y validado. Si el VIB que desea agregar depende de un VIB diferente, el cmdlet muestra dicha información e incluye el VIB que resolvería la dependencia. Si el nivel de aceptación del VIB que desea agregar es inferior al nivel de aceptación del perfil de imagen, ocurrirá un error.

Exportar un perfil de imagen a ISO o ZIP de paquete sin conexión

Puede exportar un perfil de imagen a una imagen ISO o un archivo ZIP que contenga archivos y carpetas de componentes. No puede crear los dos si ejecuta el cmdlet una sola vez. Puede utilizar una imagen ISO como el instalador de ESXi o cargar la imagen ISO a vSphere Update Manager para actualizaciones. Puede utilizar el archivo ZIP, que contiene metadatos y los VIB especificados en el perfil de imagen, para actualizar a ESXi 5.0 y posterior.

Requisitos previos

Instalar vSphere PowerCLI y todo el software necesario como requisito previo. Consulte [Instalar vSphere ESXi Image Builder y software de requisito previo](#).

Procedimiento

- 1 En una sesión de vSphere PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute <code>Add-EsxSoftwareDepot -DepotUrl depot_url</code> .
Archivo ZIP	<ol style="list-style-type: none"> a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code>.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

- 2 Ejecute `Export-EsxImageProfile` para exportar el perfil de imagen.

Formato de exportación	Cmdlet
Imágenes ISO	<code>Export-EsxImageProfile</code> con el parámetro <code>-ExportToIso</code>
Archivos ZIP de almacén sin conexión	<code>Export-EsxImageProfile</code> con el parámetro <code>-ExportToBundle</code>

Resultados

Para la imagen ISO, vSphere ESXi Image Builder valida firmas de VIB, agrega archivos binarios de VIB a la imagen y descarga la imagen a la ubicación especificada. Para el archivo ZIP, vSphere ESXi Image Builder valida firmas de VIB y descarga los archivos binarios de VIB a la ubicación especificada.

Ejemplo: Exportar un perfil de imagen a ISO

Ejemplo: Exportar un perfil de imagen a un paquete sin conexión

Siga estos pasos para exportar un perfil de imagen a una imagen ISO o un archivo ZIP que contenga archivos y carpetas de componentes.

- 1 Agregue el almacén de software.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```

- 2 Observe todos los perfiles de imagen disponibles para encontrar el nombre del perfil de imagen que desea exportar.

```
Get-EsxImageProfile
```

- 3 Exporte el perfil de imagen.

```
Export-EsxImageProfile -ImageProfile "myprofile" -ExportToIso -FilePath iso_name
```

- 1 Agregue el almacén de software.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```


- 2 Observe todos los perfiles de imagen disponibles para encontrar el nombre del perfil de imagen que desea exportar.

```
Get-EsxImageProfile
```

- 3 Exporte el perfil de imagen.

```
Export-EsxImageProfile -ImageProfile "myprofile" -ExportToBundle -FilePath C:\my_bundle.zip
```

Pasos siguientes

Utilice la imagen ISO en una instalación de ESXi o cargue la imagen ISO a vSphereUpdate Manager para realizar actualizaciones.

Utilice el archivo ZIP para actualizar una instalación de ESXi.

- Importe el archivo ZIP a vSphere Update Manager para utilizarlo con líneas base de revisión.
- Descargue el archivo ZIP a un host ESXi o un almacén de datos, y ejecute los comandos `esxcli software vib` para importar los VIB del archivo ZIP.

Consulte la documentación de *Actualización de vSphere*.

Mantenimiento de perfiles de imagen entre sesiones

Cuando se crea un perfil de imagen y se sale de la sesión de vSphere PowerCLI, el perfil de imagen ya no está disponible cuando se inicia una nueva sesión. Puede exportar el perfil de imagen a un almacén de software de archivos zip y agregar ese depósito en la siguiente sesión.

Requisitos previos

Instalar vSphere PowerCLI y todo el software necesario como requisito previo. Consulte [Instalar vSphere ESXi Image Builder y software de requisito previo](#).

Procedimiento

- 1 En una sesión de vSphere PowerCLI, cree un perfil de imagen, por ejemplo, clonando un perfil de imagen existente y agregando un VIB.
- 2 Exporte el perfil de imagen a un archivo ZIP llamando a `Export-EsxImageProfile` con el parámetro `ExportToBundle`.

```
Export-EsxImageProfile -ImageProfile "my_profile" -ExportToBundle -FilePath  
"C:\isos\temp-base-plus-vib25.zip"
```

- 3 Salga de la sesión de vSphere PowerCLI.
- 4 Cuando inicie una nueva sesión de vSphere PowerCLI, agregue el almacén que contiene su perfil de imagen para poder acceder a él.

```
Add-EsxSoftwareDepot "C:\isos\temp-base-plus-vib25.zip"
```

Comparar perfiles de imagen

Puede comparar dos perfiles de imagen a través del cmdlet `Compare-EsxImageProfile`, por ejemplo, para comprobar si poseen la misma lista de VIB o nivel de aceptación. También es posible la comparación de perfiles de imagen o sus propiedades utilizando los operadores de comparación de PowerShell.

Requisitos previos

Instalar vSphere PowerCLI y todo el software necesario como requisito previo. Consulte [Instalar vSphere ESXi Image Builder y software de requisito previo](#).

Procedimiento

- 1 En una sesión de vSphere PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute <code>Add-EsxSoftwareDepot -DepotUrl depot_url</code> .
Archivo ZIP	<ol style="list-style-type: none"> a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code>.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

- 2 (opcional) Ejecute el cmdlet `Get-EsxImageProfile` para visualizar una lista de todos los perfiles de imagen en todos los almacenes disponibles.

En la lista, puede encontrar los nombres de los perfiles de imagen que desea comparar.

- 3 Antes de comparar los perfiles de imagen, asígnelos a variables.

Por ejemplo, puede crear las variables `$imageProfile1` y `$imageProfile2` para conservar los nombres de los perfiles de imagen comparados.

```
$imageProfile1
= Get-EsxImageProfile -Name "ImageProfile1"
$imageProfile2
= Get-EsxImageProfile -Name "ImageProfile2"
```

- 4 Compare los dos perfiles de imagen a través del cmdlet `Compare-EsxImageProfile` o el operador de comparación `-eq`, que devuelve un valor booleano.

- Compare los dos perfiles de imagen para obtener una descripción completa de las diferencias a través del cmdlet `Compare-EsxImageProfile`.

```
Compare-EsxImageProfile -ReferenceProfile
    $imageProfile1 -ComparisonProfile $imageProfile2
```

- Compare los dos perfiles de imagen por lista de VIB y nivel de aceptación a través del operador de comparación `-eq`.

```
if ($imageProfile1 -eq $imageProfile2) {
    Write-host "Successfully verified that both image profiles are equal."
} else {
    Write-host "Failed to verify that the image profiles are equal."
}
```

- Compare los dos perfiles de imagen por una propiedad específica a través del operador de comparación `-eq`.

```
if ($imageProfile1.vendor -eq $imageProfile2.vendor) {
    Write-host "Successfully verified that both image profiles are equal."
} else {
    Write-host "Failed to verify that the image profiles are equal."
}
```

Comparar VIB

Puede comparar dos VIB o sus propiedades usando los operadores de comparación de PowerShell.

Requisitos previos

Instalar vSphere PowerCLI y todo el software necesario como requisito previo. Consulte [Instalar vSphere ESXi Image Builder y software de requisito previo](#).

Procedimiento

- 1 En una sesión de vSphere PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute <code>Add-EsxSoftwareDepot -DepotUrl depot_url</code> .
Archivo ZIP	<ol style="list-style-type: none"> a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code>.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

- 2 (opcional) Ejecute el cmdlet `Get-EsxSoftwarePackage` para ver todos los VIB disponibles.

En la lista, puede encontrar los nombres de los VIB que desea comparar.

- 3 Antes de comparar los VIB, asígnelos a variables.

Por ejemplo, puede crear las variables `$vib1` y `$vib2` para mantener los nombre de los VIB comparados.

```
$vib1 = Get-EsxSoftwarePackage -Name "ReferenceVIB"
$vib2 = Get-EsxSoftwarePackage -Name "ComparisonVIB"
```

- 4 Use un operador de comparación para comparar los VIB por contenido y nivel de aceptación, o por una propiedad específica.

- Compare los dos VIB según su contenido y nivel de aceptación.

```
if ($vib1 -eq $vib2) {
    Write-host "Successfully verified that both VIBs are equal."
} else {
    Write-host "Failed to verify that the VIBs are equal."
}
```

- Compare una propiedad específica de los VIB usando un operador de comparaciones, como `-eq`, `-lt`, `-le`, `-gt` o `-ge`.

```
if ($vib1.VersionObject -lt $vib2.VersionObject) {
    Write-host "Successfully verified that both the VIBs are equal."
} else {
    Write-host "Failed to verify that the VIBs are equal."
}
```

Trabajar con niveles de aceptación

Los hosts, los perfiles de imagen y los VIB individuales tienen niveles de aceptación. Los niveles de aceptación de VIB muestran cómo se probó el VIB. Como parte importante de los procedimientos de instalación y actualización, es necesario que comprenda lo que significa cada nivel de aceptación, cómo cambiar los niveles y qué implica cada cambio.

Los niveles de aceptación se configuran para hosts, perfiles de imagen y VIB individuales. El nivel de aceptación predeterminado para una imagen o un perfil de imagen de ESXi es `PartnerSupported`.

Niveles de aceptación de host

El nivel de aceptación de host determina qué VIB puede instalar en un host. Puede cambiar el nivel de aceptación de un host mediante los comandos `ESXCLI`. De forma predeterminada, los hosts ESXi tienen el nivel de aceptación `PartnerSupported` para permitir que se realicen actualizaciones fácilmente con los VIB `PartnerSupported`.

Nota VMware admite hosts con el nivel de aceptación `PartnerSupported`. Para conocer los problemas que podrían surgir con los VIB individuales con nivel de aceptación `PartnerSupported`, póngase en contacto con la organización de soporte del partner.

Niveles de aceptación de perfil de imagen

El nivel de aceptación de perfil de imagen se establece en el nivel de aceptación de VIB más bajo que haya en el perfil. Si desea agregar un VIB con un nivel de aceptación bajo a un perfil de imagen, puede cambiar el nivel de aceptación del perfil con el cmdlet `Set-EsxImageProfile`. Consulte [Establecer el nivel de aceptación del perfil de imagen](#).

vSphere Update Manager no muestra el nivel de aceptación real. Utilice cmdlets de vSphere ESXi Image Builder para recuperar la información de nivel de aceptación para VIB y perfiles de imagen.

Niveles de aceptación de VIB

El nivel de aceptación de un VIB se establece cuando este se crea. Solo el creador del VIB puede establecer el nivel de aceptación.

Si intenta aprovisionar un host con un perfil de imagen o un VIB que tiene un nivel de aceptación más bajo que el host, se produce un error. Debe modificar el nivel de aceptación del host para instalar el perfil de imagen o el VIB. Consulte [Cambiar nivel de aceptación del host](#). Al cambiar el nivel de aceptación del host, se modifica también su nivel de soporte.

El nivel de aceptación de un host, perfil de imagen o VIB permite determinar quién probó el VIB y quién lo admite. VMware admite los siguientes niveles de aceptación.

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.

Cambiar nivel de aceptación del host

Es posible disminuir el nivel de aceptación del host para que coincida con el de un VIB o un perfil de imagen que desea instalar.

El nivel de aceptación de cada VIB en un host debe ser por lo menos tan elevado como el nivel de aceptación del host. Por ejemplo, no es posible instalar un VIB con nivel de aceptación PartnerSupported en un host con nivel de aceptación VMwareAccepted. Primero debe disminuir el nivel de aceptación del host. Para obtener más información sobre los niveles de aceptación, consulte [Niveles de aceptación](#).

Advertencia El cambio del nivel de aceptación del host a CommunitySupported afecta la compatibilidad del host y podría perjudicar su seguridad.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

- 1 Recupere el nivel de aceptación del VIB o el perfil de imagen.

Opción	Descripción
Ver información para todos los VIB	<pre>esxcli --server=server_name software sources vib list --depot=depot_URL</pre>
Ver información para un VIB específico	<pre>esxcli --server=server_name software sources vib list --viburl=vib_URL</pre>
Ver información para todos los perfiles de imagen	<pre>esxcli --server=server_name software sources profile list -- depot=depot_URL</pre>
Ver información para un perfil de imagen específico	<pre>esxcli --server=server_name software sources profile get --depot=depot_URL --profile=profile_name</pre>

- 2 Vea el nivel de aceptación del host.

```
esxcli --server=server_name software acceptance get
```

- 3 Cambie el nivel de aceptación del host.

```
esxcli
--server=server_name software acceptance set --level=acceptance_level
```

El valor de *acceptance_level* puede ser `VMwareCertified`, `VMwareAccepted`, `PartnerSupported` o `CommunitySupported`. Los valores para *acceptance_level* distinguen mayúsculas de minúsculas.

Nota Si el host tiene un nivel de aceptación más elevado que el VIB o el perfil de imagen que desea agregar, puede ejecutar comandos en el espacio de nombres `esxcli software vib` o `esxcli software profile` con la opción `--force`. Cuando utiliza la opción `--force`, aparece un mensaje de advertencia, ya que exige un VIB o un perfil de imagen con un nivel de aceptación más bajo que el del host y la configuración deja de ser coherente. La advertencia también aparece cuando instala VIB, elimina VIB o realiza ciertas otras operaciones en el host que tiene niveles de aceptación incoherentes.

Establecer el nivel de aceptación del perfil de imagen

Si desea agregar un VIB a un perfil de imagen, y el nivel de aceptación del VIB es menor al del perfil de imagen, puede clonar el perfil de imagen con un nivel de aceptación menor o cambiar el nivel de aceptación del perfil de imagen.

Puede especificar `VMwareCertified`, `VMwareAccepted`, `PartnerSupported` o `CommunitySupported` como un nivel de aceptación de un perfil de imagen. Si disminuye el nivel de aceptación, se cambiará el nivel de compatibilidad para el perfil de imagen y los hosts que aprovisiona con él. Para obtener más información, consulte [Niveles de aceptación](#).

Requisitos previos

Instale vSphere PowerCLI y todas las herramientas de software que constituyan un requisito previo. Consulte [Instalar vSphere ESXi Image Builder y software de requisito previo](#).

Procedimiento

- 1 En una sesión de vSphere PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute <code>Add-EsxSoftwareDepot -DepotUrl depot_url</code> .
Archivo ZIP	<ol style="list-style-type: none"> a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code>.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

- 2 Obtenga el nivel de aceptación para el perfil de imagen.

```
Get-EsxImageProfile -Name string
```

- 3 Establezca el nivel de aceptación del perfil de imagen.

```
Set-EsxImageProfile -Name string -AcceptanceLevel level
```

Flujos de trabajo de vSphere ESXi Image Builder

Los flujos de trabajo de vSphere ESXi Image Builder son ejemplos del uso de cmdlets. Los flujos de trabajo no representan tareas reales, sino que ilustran cómo se pueden explorar diferentes maneras de usar un cmdlet. Los administradores que prueban los flujos de trabajo se benefician mediante una experiencia con vSphere PowerCLI, con Microsoft PowerShell o con ambos.

Revisar contenido de almacenes

Puede examinar los VIB y los almacenes de software con los cmdlets de vSphere ESXi Image Builder. Puede utilizar comodines para examinar el contenido de los almacenes. Son compatibles todas las expresiones con comodines.

El propio flujo de trabajo transmite los parámetros por nombre. No obstante, es posible acceder a variables para transmitir parámetros como objetos.

Puede utilizar opciones de filtros y expresiones con comodines para examinar el contenido de los almacenes.

Requisitos previos

Compruebe que vSphere PowerCLI y el software requerido estén instalados. Consulte [Instalar vSphere ESXi Image Builder y software de requisito previo](#).

Procedimiento

- 1 En una sesión de vSphere PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute <code>Add-EsxSoftwareDepot -DepotUrl depot_url</code> .
Archivo ZIP	<ol style="list-style-type: none"> a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code>.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

- 2 Recupere los perfiles de imagen.

Puede filtrarlos por proveedor, nombre y nivel de aceptación.

■ `Get-EsxImageProfiles`

Devuelve una matriz de objetos de `ImageProfile` provenientes de todos los almacenes que se agregaron a la sesión.

■ `Get-EsxImageProfile -Vendor "C*"`

Devuelve todos los perfiles de imagen creados por un proveedor cuyo nombre comienza con la letra C.

3 Recupere los paquetes de software mediante el cmdlet `Get-EsxSoftwarePackage`.

Puede filtrarlos (por ejemplo, por proveedor o versión) y puede usar los caracteres comodín estándar de PowerShell.

- `Get-EsxSoftwarePackage -Vendor "V*"`

Devuelve todos los paquetes de software de un proveedor cuyo nombre comienza con la letra V.

- `Get-EsxSoftwarePackage -Vendor "V*" -Name "*scsi*"`

Devuelve todos los paquetes de software cuyo nombre contiene la cadena `scsi` y que pertenecen a un proveedor cuyo nombre comienza con la letra V.

- `Get-EsxSoftwarePackage -Version "2.0*"`

Devuelve todos los paquetes de software con una cadena de versión que comienza con 2.0.

4 Use `-Newest` para buscar el paquete más reciente.

- `Get-EsxSoftwarePackage -Vendor "V*" -Newest`

Devuelve el paquete más reciente para los proveedores cuyo nombre comienza con la letra V y muestra la información mediante una tabla.

- `Get-EsxSoftwarePackage -Vendor "V*" -Newest | format-list`

Devuelve información detallada acerca de cada paquete de software, mediante un canal que permite enlazar el resultado de la solicitud de paquetes de software emitida al cmdlet `format-list` de PowerShell.

5 Vea la lista de VIB en el perfil de imagen.

```
(Get-EsxImageProfile -Name "Robin's Profile").VibList
```

`VibList` es una propiedad del objeto `ImageProfile`.

6 Recupere los paquetes de software lanzados antes o después de una fecha determinada, mediante los parámetros `CreatedBefore` o `CreatedAfter`.

```
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

Ejemplo: Revisar el contenido de almacenes mediante variables

En este ejemplo de flujo de trabajo, se examina el contenido de un almacén mediante la transmisión de parámetros como objetos a los que se accede por posición en una variable, no mediante la transmisión de parámetros por nombre. Puede ejecutar los comandos siguientes en una secuencia desde la línea de comandos de vSphere PowerCLI. Reemplace los nombres por nombres que resulten adecuados para la instalación correspondiente.

```
Get-ESXSoftwarePackage -Vendor "v*"
Get-ESXSoftwarePackage -Vendor "v*" -Name "r*"
Get-ESXSoftwarePackage -Version "2.0*"
$ip1 = Get-ESXImageProfile -name ESX-5.0.0-123456-full
$ip1.VibList
Get-ESXSoftwarePackage -CreatedAfter 7/1/2010
```

Crear perfiles de imagen a través de un flujo de trabajo de clonación

Puede utilizar los cmdlets de vSphere ESXi Image Builder para comprobar los almacenes que están disponibles, agregar un almacén, visualizar la información de un perfil de imagen y crear un perfil de imagen nuevo mediante la clonación de uno de los perfiles de imagen disponibles.

Los perfiles publicados generalmente son de solo lectura y no pueden modificarse. Incluso si un perfil publicado no es de solo lectura, clonar en lugar de modificar el perfil es la práctica recomendada, debido a que la modificación de un perfil original elimina el original. No podrá revertir al perfil original no modificado, excepto si realiza una reconexión con un almacén.

Un flujo de trabajo de clonación de perfiles podría incluir comprobar el estado actual del sistema, agregar un almacén de software y clonar el perfil.

Requisitos previos

Compruebe que vSphere PowerCLI y el software requerido estén instalados. Consulte [Instalar vSphere ESXi Image Builder y software de requisito previo](#).

Procedimiento

- 1 En una ventana de PowerShell, compruebe si se ha definido algún almacén de software para la sesión actual.

```
$DefaultSoftwareDepots
```

PowerShell devuelve los almacenes definidos actualmente o nada si se acaba de iniciar PowerShell.

- 2 Si el almacén que contiene el perfil que desea clonar no aparece en los resultados, agréguelo a la sesión actual.

Opción	Acción
Almacén remoto	Ejecute <code>Add-ESXSoftwareDepot -DepotUrl depot_url</code> .
Archivo ZIP	<ol style="list-style-type: none"> a Descargue el archivo ZIP en la ruta de acceso de archivo local. b Ejecute <code>Add-ESXSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code>

PowerShell agregará el almacén especificado a la sesión actual y mostrará todos los almacenes actuales.

- 3 (opcional) Compruebe la variable `$DefaultSoftwareDepots`, que ahora devuelve el almacén recientemente agregado.
- 4 Vea todos los perfiles de imagen disponibles.

```
Get-ESXImageProfile
```

- 5 Para clonar un perfil de imagen, introduzca su nombre, un nombre nuevo para el perfil nuevo y un nombre para el proveedor.

```
$ip = New-ESXImageProfile -CloneProfile base-tbd-v1 -Name "Test Profile 42" -Vendor "Vendor20"
```

- 6 (opcional) Visualice el perfil de imagen recientemente creado, `$ip`.

PowerShell devuelve la información sobre el perfil de imagen en formato tabular.

Name	Vendor	Last Modified	Acceptance Level
----	-----	-----	-----
Test Profile 42	Vendor20	9/15/2010 5:45:43...	PartnerSupported

Ejemplo: Crear un perfil de imagen mediante la clonación con variables

En este ejemplo de flujo de trabajo, se repiten los pasos de este flujo de trabajo mediante la transmisión de parámetros como objetos a los que se accede por posición en una variable, no mediante la transmisión de parámetros por nombre. Puede ejecutar los siguientes cmdlets en secuencia desde la línea de comandos de vSphere PowerCLI.

```
$DefaultSoftwareDepots
Add-ESXSoftwareDepot -DepotUrl depot_url
$DefaultSoftwareDepots
$profs = Get-ESXImageProfile
$profs
$ip = New-ESXImageProfile -CloneProfile $profs[2] -Name "new_profile_name" -Vendor "my_vendor"
$ip
```

Crear flujos de trabajo de nuevos perfiles de imagen

En la mayoría de las situaciones, se crea un perfil de imagen clonando un perfil existente. Es posible que algunos clientes o partners de VMware necesiten crear un nuevo perfil de imagen. Ponga mucha atención a las dependencias y a los niveles de aceptación en caso de que se cree un perfil de imagen desde cero.

El sistema espera que el nivel de aceptación de los VIB que se agregan a la imagen de base sea igual de alto que el nivel de la imagen de base. Si se tiene que agregar un VIB con un nivel de aceptación menor al perfil de imagen, se debe bajar el nivel de aceptación del perfil de imagen. Para obtener más información, consulte [Establecer el nivel de aceptación del perfil de imagen](#).

Como alternativa a la especificación de los parámetros en la línea de comandos, se puede usar el mecanismo de introducción de información de PowerShell para especificar parámetros de cadena. La introducción de información no funciona para otros parámetros, como objetos.

Requisitos previos

- vSphere PowerCLI y el software de requisito previo están instalados. Consulte [Instalar vSphere ESXi Image Builder y software de requisito previo](#).
- Tiene acceso a un almacén que incluye una imagen base y uno o más VIB. Los partners de VMware y VMware tienen almacenes públicos a los que se accede mediante URL. Los partners de VMware o VMware pueden crear un archivo ZIP que se puede descomprimir en el entorno local y al que se puede acceder mediante una ruta de acceso de archivo.

Procedimiento

- 1 En una sesión de vSphere PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute <code>Add-EsxSoftwareDepot -DepotUrl depot_url</code> .
Archivo ZIP	<ol style="list-style-type: none"> a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code>.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

- 2 Ejecute el cmdlet `Get-EsxImageProfile` para mostrar todos los perfiles de imagen de todos los almacenes actualmente visibles. Puede limitar la búsqueda utilizando los argumentos opcionales para filtrar la salida.

```
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

- 3 Cree un nuevo perfil, asígnele un nombre y proveedor y agregue un paquete base.

```
New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage esx-base[0],esx-xlibs[0]
```

El ejemplo usa el paquete `esx-base`. En la mayoría de los casos, cuando se crea un nuevo perfil de imagen se incluye el paquete `esx-base`. Los nombres que contienen espacios van con comillas.

- 4 Use un proceso para pasar el nuevo perfil de imagen a `format-list` para obtener información detallada sobre el nuevo paquete.

```
(Get-EsxImageProfile -Name "Test #2").VibList | format-list
```

Ejemplo: Crear perfiles de imagen desde cero utilizando variables

Esta secuencia de comandos repite los pasos del flujo de trabajo, pero pasa parámetros como objetos, a los que se accede mediante posición en una variable, en lugar de pasar parámetros por nombre. Se pueden ejecutar los siguientes comandos en secuencia en el mensaje vSphere PowerCLI.

```
Add-EsxSoftwareDepot depoturl
$pkgs = Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
$ip2 = New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage
$pkgs[0]
$ip2.VibList | format-list
```

Editar flujo de trabajo de perfiles de imagen

Puede crear una imagen personalizada mediante la clonación y edición de un perfil de imagen. Puede agregar o reemplazar uno o más VIB en el perfil existente. Si agregar o reemplazar VIB podría no permitir que el perfil de imagen funcione de forma correcta, se generará un error.

Requisitos previos

- vSphere PowerCLI y el software de requisito previo están instalados. Consulte [Instalar vSphere ESXi Image Builder y software de requisito previo](#).
- Tiene acceso a un almacén que incluye una imagen base y uno o más VIB. VMware y partners de VMware permiten que estén disponibles almacenes públicos a los que se puede acceder a través de una dirección URL. VMware o partners de VMware pueden crear un archivo ZIP que puede descargar a su entorno local y acceder a través de una ruta de archivo.

Procedimiento

- 1 En una sesión de vSphere PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute <code>Add-EsxSoftwareDepot -DepotUrl <i>depot_url</i></code> .
Archivo ZIP	<ol style="list-style-type: none"> a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute <code>Add-EsxSoftwareDepot -DepotUrl C:\file_path\offline-bundle.zip</code>.

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

- 2 Utilice una canalización para pasar el perfil de imagen que desea editar a `format-list` para acceder a información detallada.

En este ejemplo, el perfil de imagen creado en [Crear flujos de trabajo de nuevos perfiles de imagen](#) contiene solo la imagen base. No se incluye en el almacén un perfil de imagen nuevo creado. En cambio, puede acceder al perfil de imagen por el nombre o mediante la asociación con una variable.

```
Get-ExsImageProfile "Test #2" | format-list
```

PowerShell devuelve la información.

```
Name           : Test #2
Vendor         : Vendor42
...
VibList        : {esx-base 5.0.0.-...,}
```

- 3 (opcional) Si va a agregar un VIB con un nivel de aceptación inferior que aquel del perfil de imagen, cambie el nivel de aceptación del perfil de imagen.

```
Set-ExsImageProfile -ImageProfile "Test #2" -AcceptanceLevel VMwareAccepted
```

PowerShell devuelve la información sobre el perfil cambiado en formato tabular.

Name	Vendor	Last Modified	Acceptance Level
----	-----	-----	-----
Test #2	Vendor42	9/22/2010 12:05:...	VMwareAccepted

- 4 Agregue un paquete de software (VIB) al perfil de imagen. Puede agregar el paquete por nombre.

```
Add-ExsSoftwarePackage -ImageProfile "Test #2"
                        -SoftwarePackage NewPack3
```

PowerShell devuelve la información sobre el perfil de imagen en formato tabular.

Name	Vendor	Last Modified	Acceptance Level
----	-----	-----	-----
Test #2	Vendor42	9/22/2010 12:05:...	VMwareAccepted

Nota Si ocurre un error cuando agrega el paquete de software, es posible que tenga un problema con los niveles de aceptación. Consulte [Trabajar con niveles de aceptación](#)

- 5 Vuelva a visualizar el perfil de imagen.

```
Get-ExsImageProfile "Test #2" | format-list
```

La lista de VIB se actualiza para incluir el paquete de software nuevo y se muestra la información.

```
Name           : Test #2
Vendor         : Vendor42
...
VibList        : {esx-base 5.0.0.-..., NewPack3}
```

Ejemplo: Editar perfiles de imagen a través de variables

Esta secuencia de cmdlet repite los pasos del flujo de trabajo, pero pasa los parámetros como objetos, a los que se accede a través de una posición en una variable, en lugar de pasar los parámetros por nombre. Puede ejecutar los siguientes cmdlets en secuencia desde la línea de comandos de vSphere PowerCLI.

```
Add-EsxSoftwareDepot -DepotUrl depot_url
$ip2 = Get-EsxImageProfile -name "Test #2"
$ip2 | format-list
Set-EsxImageProfile -ImageProfile $ip2 -AcceptanceLevel VMwareAccepted
Add-EsxImageSoftwarePackage -ImageProfile $ip2 -SoftwarePackage NewPack3
$ip2 | format-list
```

Configurar ESXi

5

Estos temas proporcionan información sobre el uso de la interfaz de usuario de la consola directa y la configuración de los valores predeterminados de ESXi.

Este capítulo incluye los siguientes temas:

- [Configurar ESXi automáticamente](#)
- [Acerca de la interfaz de ESXi de la consola directa](#)
- [Configurar la contraseña de la cuenta de administrador](#)
- [Configuración de arranque del BIOS](#)
- [El host no arranca después de instalar ESXi en modo UEFI](#)
- [Acceso de red a un host ESXi](#)
- [Configurar la red en un host que no se haya adjuntado a la red](#)
- [Administrar ESXi de forma remota](#)
- [Configuración de las opciones de red](#)
- [Comportamiento de almacenamiento](#)
- [Habilitar el acceso a ESXi Shell y SSH con la interfaz de usuario de la consola directa](#)
- [Ver registros del sistema](#)
- [Configurar Syslog en hosts ESXi](#)
- [Configurar el filtrado de registros en hosts ESXi](#)
- [Configurar el nivel de aceptación del perfil de imagen de host](#)
- [Restablecer la configuración del sistema](#)
- [Quitar todos los paquetes personalizados en ESXi](#)
- [Deshabilitación de la compatibilidad con caracteres no ASCII en los nombres de directorios y archivos de máquinas virtuales](#)
- [Desinstalar un host ESXi](#)

Configurar ESXi automáticamente

Cuando enciende el host ESXi por primera vez o después de restablecer los valores predeterminados de configuración, el host pasa a la fase de autoconfiguración. En esta fase se configuran dispositivos de red y de almacenamiento del sistema con opciones predeterminadas.

De manera predeterminada, el protocolo de configuración dinámica de host (DHCP) configura IP y todos los discos internos visibles que están en blanco se formatean con el sistema de archivos de la máquina virtual (VMFS). De este modo, las máquinas virtuales pueden almacenarse en los discos.

Acerca de la interfaz de ESXi de la consola directa

Use la consola directa para la configuración inicial y solución de problemas de ESXi.

Conecte un teclado y monitor al host para usar la consola directa. Una vez que el host concluye la fase de configuración automática, aparece la consola directa en el monitor. Puede examinar la configuración de red predeterminada y cambiar cualquier configuración que no sea compatible con el entorno de red.

Las operaciones clave disponibles en la consola directa incluyen:

- Configuración de hosts
- Configuración de acceso administrativo
- Solucionar problemas

También puede usar vSphere Web Client para administrar el host mediante vCenter Server.

Tabla 5-1. Buscar en la consola directa

Acción	Clave
Ver y cambiar la configuración	F2
Cambiar la interfaz de usuario a modo de alto contraste	F4
Apagar o reiniciar el host	F12
Ver el registro de VMkernel	Alt+F12
Cambiar a la consola del shell	Alt+F1
Cambiar a la interfaz de usuario de la consola directa	Alt+F2
Mover la selección entre campos	Teclas de flecha
Seleccionar un elemento de menú	Intro
Alternar un valor	Barra espaciadora

Tabla 5-1. Buscar en la consola directa (continuación)

Acción	Clave
Confirmar comandos sensibles, como restablecimiento de valores predeterminados de la configuración	F11
Guardar y salir	Intro
Salir sin guardar	Esc
Salir de registros del sistema	q

Configuración de la distribución del teclado para la consola directa

Puede configurar la distribución del teclado que desea usar con la consola directa.

Procedimiento

- 1 Desde la consola directa, seleccione **Configurar teclado** y presione Intro.
- 2 Seleccione la distribución que desea usar.
- 3 Presione la barra espaciadora para habilitar y desactivar las selecciones.
- 4 Presione Intro.

Crear un mensaje emergente de seguridad para la consola directa

Un banner de seguridad es un mensaje que se muestra en la pantalla **Principal** de la consola directa.

Procedimiento

- 1 Desde vSphere Web Client, conéctese a vCenter Server.
- 2 Seleccione el host en el inventario.
- 3 Haga clic en la pestaña **Administrar**.
- 4 Haga clic en **Configuración**.
- 5 En Sistema, seleccione **Configuración avanzada del sistema**.
- 6 Seleccione **Anotaciones**.
- 7 Haga clic en el icono de edición.
- 8 Introduzca un mensaje de seguridad.

Resultados

El mensaje se muestra en la pantalla **Principal** de la consola directa.

Redirigir la consola directa a un puerto serie

Para administrar de forma remota el host ESXi desde una consola serie, puede redirigir la consola directa hacia un puerto serie.

vSphere admite el tipo de terminal VT100 y el emulador de terminal PuTTY para ver la consola directa a través del puerto serie.

Puede redirigir la consola directa hacia un puerto serie de varias formas.

- [Redireccionar la consola directa a un puerto serie mediante la configuración manual de las opciones de arranque](#)

Cuando se redirige la consola directa a un puerto serie mediante la configuración de opciones de arranque, el cambio no persiste en los arranques subsiguientes.

- [Redirigir la consola directa a un puerto serie desde vSphere Web Client](#)

Puede administrar de forma remota el host ESXi desde una consola que esté conectada al puerto serie redirigiendo la consola directa a los puertos serie com1 o com2. Cuando se utiliza vSphere Web Client para redirigir la consola directa a un puerto serie, la opción de arranque que se configura continúa después de los arranques posteriores.

- [Redireccionar la consola directa a un puerto serie en un host implementado con Auto Deploy](#)

Después de redireccionar la consola directa a un puerto serie, puede determinar que esa configuración forme parte del perfil de host que se conserva cuando se reaprovisiona el host con Auto Deploy.

Redireccionar la consola directa a un puerto serie mediante la configuración manual de las opciones de arranque

Cuando se redirige la consola directa a un puerto serie mediante la configuración de opciones de arranque, el cambio no persiste en los arranques subsiguientes.

Requisitos previos

Compruebe que el puerto serie no esté en uso para la generación de registros y la depuración serie.

Procedimiento

- 1 Inicie el host.
- 2 Cuando aparezca la ventana Cargando el hipervisor de VMware, presione las teclas Mayús + O para editar las opciones de arranque.
- 3 Deshabilite logPort y gdbPort en com1 y establezca tty2Port en com1 introduciendo las siguientes opciones de arranque:

```
"gdbPort=none logPort=none tty2Port=com1";
```

Para utilizar com2, reemplace com1 por com2.

Resultados

La consola directa se redirecciona al puerto serie hasta que reinicie el host. Para redireccionar la consola directa para los arranque subsiguientes, consulte [Redirigir la consola directa a un puerto serie desde vSphere Web Client](#)

Redirigir la consola directa a un puerto serie desde vSphere Web Client

Puede administrar de forma remota el host ESXi desde una consola que esté conectada al puerto serie redirigiendo la consola directa a los puertos serie com1 o com2. Cuando se utiliza vSphere Web Client para redirigir la consola directa a un puerto serie, la opción de arranque que se configura continúa después de los arranques posteriores.

Requisitos previos

- Compruebe que puede acceder al host desde vSphere Web Client.
- Compruebe que el puerto serie no esté en uso para registro y depuración seriales o para shell ESX (tty1Port).

Procedimiento

- 1 Desde vSphere Web Client, conéctese a vCenter Server.
- 2 Seleccione el host en el inventario.
- 3 Haga clic en la pestaña **Administrar**.
- 4 Haga clic en **Configuración**.
- 5 En Sistema, seleccione **Configuración avanzada del sistema**.
- 6 Asegúrese de que los campos **VMkernel.Boot.logPort** y **VMkernel.Boot.gdbPort** no estén establecidos para usar el puerto com al que desea redirigir la consola directa.
- 7 Configure **VMkernel.Boot.tty2Port** al puerto serie para redireccionar la consola directa a: **com1** o **com2**.
- 8 Reinicie el host.

Resultados

Ahora puede administrar de forma remota el host ESXi desde una consola que esté conectada al puerto serie.

Redireccionar la consola directa a un puerto serie en un host implementado con Auto Deploy

Después de redireccionar la consola directa a un puerto serie, puede determinar que esa configuración forme parte del perfil de host que se conserva cuando se reaprovisiona el host con Auto Deploy.

Requisitos previos

El puerto serie no deberá estar en uso para el registro y la depuración en serie.

Procedimiento

- 1 Desde vSphere Web Client, conéctese a vCenter Server.
- 2 Seleccione el host en el inventario.
- 3 Haga clic en la pestaña **Administrar**.
- 4 Seleccione **Configuración**.
- 5 Seleccione **Configuración avanzada del sistema**.
- 6 Asegúrese de que los campos **VMkernel.Boot.logPort** y **VMkernel.Boot.gdbPort** no estén establecidos para usar el puerto com al que desea redirigir la consola directa.
- 7 Configure **VMkernel.Boot.tty2Port** al puerto serie para redireccionar la consola directa a: **com1** o **com2**.
- 8 Haga clic en **Aceptar**.
- 9 Guarde el perfil de host y conecte el host al perfil. Consulte la documentación de *Perfiles de host de vSphere*.

Resultados

La configuración para redireccionar la consola directa a un puerto serie es almacenada por vCenter Server y se conserva cuando se reaprovisiona el host con Auto Deploy.

Configurar la contraseña de la cuenta de administrador

Puede usar la consola directa para establecer la contraseña para la cuenta de administrador (raíz).

El nombre de usuario del administrador para el host ESXi es root. De forma predeterminada, la contraseña del administrador no está establecida.

Procedimiento

- 1 En la consola directa, seleccione **Configurar contraseña**.
- 2 (opcional) Si ya hay una contraseña configurada, escríbala en la línea **Contraseña antigua** y presione Intro.
- 3 En la línea **Contraseña nueva**, introduzca una nueva contraseña y presione Intro.
- 4 Vuelva a introducir la nueva contraseña y presione Intro.

Configuración de arranque del BIOS

Si el servidor tiene varias unidades, es posible que deba configurar las opciones del BIOS.

La configuración de arranque del BIOS determina la manera en que se arranca el servidor. Por lo general, el dispositivo de CD-ROM se muestra primero en la lista.

Nota Si usa ESXi integrado, la configuración de arranque del BIOS determina si el servidor se inicia desde un dispositivo de arranque de ESXi o desde otro dispositivo de arranque. Por lo general, el dispositivo flash USB se muestra primero en la lista de la configuración de arranque del BIOS en la máquina que aloja ESXi.

Es posible cambiar la configuración de arranque configurando el orden de arranque en el BIOS durante el inicio o seleccionado un dispositivo de arranque desde el menú selección de dispositivos de arranque. Cuando se cambia el orden de arranque en el BIOS, la nueva configuración afecta todos los reinicios posteriores. Cuando se selecciona un dispositivo de arranque desde el menú selección de dispositivos de arranque, la selección afecta únicamente el arranque actual.

Algunos servidores no incluyen un menú selección de dispositivos de arranque, en cuyo caso se debe cambiar el orden de arranque en el BIOS incluso para los arranques únicos y, a continuación, se debe volver a cambiar durante un reinicio posterior.

Cómo cambiar la configuración de arranque del BIOS para ESXi

Ajuste la configuración de arranque del BIOS para ESXi si desea que el servidor arranque en ESXi de forma predeterminada.

Las versiones ESXi Instalable y ESXi Integrada, no pueden existir en el mismo host.

Procedimiento

- 1 Mientras se enciende el host ESXi, presione la tecla necesaria para entrar en la configuración del BIOS del host.

En función del hardware del servidor, la tecla podría ser una tecla de función o Suprimir. La opción para entrar a la configuración del BIOS podría ser diferente para su servidor.

- 2 Seleccione la configuración de arranque del BIOS.

Opción	Descripción
Si está utilizando la versión instalable de ESXi	Seleccione el disco en el que instaló el software ESXi y muévelo a la primera posición de la lista. El host arrancará en ESXi.
Si está utilizando la versión integrada de ESXi	Seleccione el dispositivo flash USB y muévelo a la primera posición de la lista. El host arrancará en el modo ESXi.

Configuración de la opción de arranque para medios virtuales

Si usa software de administración remota para configurar ESXi, es posible que deba configurar la opción de arranque para medios virtuales.

Los medios virtuales son una manera de conectar un medio de almacenamiento remoto como CD-ROM, dispositivo de almacenamiento USB, imagen ISO y disquete con un servidor de destino que puede estar en cualquier lado de la red. El servidor de destino tiene acceso al medio remoto, y puede leerlo y escribir en él como si estuviera conectado físicamente al puerto USB del servidor.

Requisitos previos

Las versiones ESXi Instalable y ESXi Integrada, no pueden existir en el mismo host.

Procedimiento

- 1 Conecte el medio al dispositivo virtual.

Por ejemplo, si utiliza un servidor Dell, inicie sesión en Dell Remote Access Controller (DRAC) o una interfaz de administración remota similar y seleccione una unidad de disquete o CD-ROM física, o bien proporcione una ruta de acceso a una imagen de disquete o de CD-ROM.

- 2 Reinicie el servidor.

- 3 Mientras se enciende el servidor, entre al menú de selección de dispositivos.

En función del hardware del servidor, la tecla podría ser una tecla de función o Suprimir.

- 4 Siga las instrucciones para seleccionar el dispositivo virtual.

Resultados

El servidor arranca desde el dispositivo configurado una vez y vuelve al orden de arranque predeterminado en los arranques subsiguientes.

El host no arranca después de instalar ESXi en modo UEFI

Cuando instala ESXi en un equipo host en modo UEFI, la máquina podría producir un error al arrancar.

Problema

Cuando reinicia después de instalar ESXi en un equipo host en modo UEFI, el reinicio podría producir un error. Este problema viene acompañado de un mensaje de error similar a `Unexpected network error. No hay dispositivo de arranque disponible.`

Causa

El sistema host no reconoce el disco que ESXi instaló como disco de arranque.

Solución

- 1 Mientras aparece el mensaje de error en la pantalla, presione F11 para visualizar las opciones de arranque.
- 2 Seleccione una opción similar a **Agregar opción de arranque**.

La redacción de la opción podría variar, según el sistema.

- 3 Seleccione el archivo `\EFI\BOOT\BOOTx64.EFI` en el disco en el que instaló ESXi.
- 4 Cambie el orden de arranque de manera que el host arranque desde la opción que haya agregado.

Acceso de red a un host ESXi

El comportamiento predeterminado es configurar la red de administración ESXi con DHCP. Puede anular el comportamiento predeterminado y utilizar una configuración de IP estática para la red de administración después de que se complete la instalación.

Tabla 5-2. Situaciones de configuración de red compatibles con ESXi

Situación	Enfoque
Debe aceptar la configuración de IP ajustada por DHCP.	En la consola directa de ESXi, puede buscar la dirección IP asignada a través de DHCP a la interfaz de administración de ESXi. Puede utilizar esa dirección IP para conectarse al host desde vSphere Web Client y personalizar la configuración, incluido el cambio de la dirección IP de administración.
Una de las siguientes situaciones es real: <ul style="list-style-type: none"> ■ No tiene un servidor DHCP. ■ El host ESXi no está conectado a un servidor DHCP. ■ El servidor DHCP conectado no funciona de forma correcta. 	<p>Durante la fase de configuración automática, el software asigna la dirección IP local de vínculo, que se encuentra en la subred 169.254.x.x/16. La dirección IP asignada aparece en la consola directa.</p> <p>Puede anular la dirección IP local de vínculo mediante la configuración de una dirección IP estática a través de la consola directa.</p>
El host ESXi se conecta a un servidor DHCP en funcionamiento, pero no desea utilizar la dirección IP configurada por DHCP.	<p>Durante la fase de configuración automática, el software asigna una dirección IP configurada por DHCP.</p> <p>Puede realizar la conexión inicial a través de la dirección IP configurada por DHCP. A continuación, puede configurar una dirección IP estática.</p> <p>Si posee un acceso físico al host ESXi, puede anular la dirección IP configurada por DHCP mediante la configuración de una dirección IP estática a través de la consola directa.</p>
Sus directivas de implementación de seguridad no permiten que se enciendan hosts sin configuración en la red.	Siga el procedimiento de configuración en Configurar la red en un host que no se haya adjuntado a la red .

Configurar la red en un host que no se haya adjuntado a la red

Algunos entornos altamente seguros no permiten que se enciendan hosts no configurados en la red. Puede configurar el host antes de conectarlo a la red.

Requisitos previos

Compruebe que no existan cables de red conectados al host.

Procedimiento

- 1 Encienda el host.
- 2 Utilice la interfaz de usuario de la consola directa para configurar la contraseña para la cuenta de administrador (raíz).
- 3 Utilice la interfaz de usuario de la consola directa para configurar una dirección IP estática.
- 4 Conecte un cable de red al host.
- 5 (opcional) Utilice vSphere Web Client para conectarse a un sistema vCenter Server.
- 6 (opcional) Agregue el host al inventario de vCenter Server.

Administrar ESXi de forma remota

Puede usar vSphere Client, vSphere Web Client y vCenter Server para administrar los hosts ESXi.

Para obtener instrucciones sobre cómo descargar e instalar vCenter Server y los componentes de vCenter Server, o sobre cómo descargar e implementar vCenter Server Appliance, consulte [Capítulo 8 Instalar vCenter Server en un servidor físico o una máquina virtual de Windows](#) e [Capítulo 9 Implementar vCenter Server Appliance](#). Para ver instrucciones sobre la instalación de vSphere Client, consulte [Instalar vSphere Client](#).

Configuración de las opciones de red

ESXi requiere una dirección IP para la red de administración. Para configurar las opciones de red básicas, utilice vSphere Web Client o la consola directa.

Utilice vSphere Web Client si está conforme con la dirección IP asignada por el servidor DHCP.

Utilice la consola directa para la configuración de red en los casos siguientes:

- Si no está conforme con la dirección IP asignada por el servidor DHCP.
- Si no está autorizado para emplear la dirección IP asignada por el servidor DHCP.
- Si ESXi no tiene una dirección IP. Esta situación puede darse si la fase de configuración automática no configuró DHCP correctamente.
- Si se seleccionó el adaptador de red incorrecto durante la fase de configuración automática.

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.

Selección de los adaptadores de red para la red de administración

El tráfico entre un host ESXi y cualquier software de administración externo se transmite por medio de un adaptador de red Ethernet en el host. Puede usar la consola directa para elegir los adaptadores de red que utiliza la red de administración.

El software de administración externo incluye, entre otros, vCenter Server y el cliente SNMP. A los adaptadores de red en el host se les asigna el nombre `vmnicN`, donde N es un número único que identifica el adaptador de red (por ejemplo, `vmnic0`, `vmnic1` y así sucesivamente).

Durante la fase de configuración automática, el host ESXi selecciona `vmnic0` para el tráfico de administración. Puede anular la opción predeterminada seleccionando manualmente el adaptador de red que transmite el tráfico de administración para el host. En algunos casos, se recomienda usar un adaptador de red Gigabit Ethernet para el tráfico de administración. Otra manera de ayudar a garantizar la disponibilidad es seleccionar varios adaptadores de red. El uso de varios adaptadores de red permite las funcionalidades de equilibrio de la carga y conmutación por error.

Procedimiento

- 1 Desde la consola directa, seleccione **Configurar red de administración** y presione Intro.
- 2 Seleccione **Adaptadores de red** y presione Intro.
- 3 Seleccione un adaptador de red y presione Intro.

Resultados

Una vez que la red esté en funcionamiento, puede usar vSphere Web Client para conectar ESXi al host mediante vCenter Server.

Configurar el id. de VLAN

Puede establecer el número de identificador de LAN virtual (VLAN) del host ESXi.

Procedimiento

- 1 Desde la consola directa, seleccione **Configurar red de administración** y presione Intro.
- 2 Seleccione **VLAN** y presione Intro.
- 3 Introduzca un número de identificador de VLAN del 1 al 4094.

Configurar IP para ESXi

De forma predeterminada, DHCP establece la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

Para futuras referencias, anote la dirección IP.

Para que DHCP funcione, el entorno de red debe tener un servidor DHCP. Si DHCP no está disponible, el host asigna la dirección IP local del vínculo, que se encuentra en la subred 169.254.x.x/16. La dirección IP asignada aparece en la consola directa. Si no cuenta con acceso al host a través de monitor físico, puede acceder a la consola directa mediante una aplicación de administración remota. Consulte [Usar aplicaciones de administración remota](#)

Si tiene acceso a la consola directa, cuenta con la opción de configurar una dirección de red estática. La máscara de red predeterminada es 255.255.0.0.

Configurar IP desde la consola directa

Si tiene acceso físico al host o acceso remoto a la consola directa, puede usar la consola directa para configurar la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

Procedimiento

- 1 Seleccione **Configurar red de administración** y presione Intro.
- 2 Seleccione **Configuración IP** y presione Intro.
- 3 Seleccione **Establecer dirección IP estática y configuración de red**.
- 4 Introduzca la dirección IP, la máscara de subred y la puerta de enlace predeterminada y presione Intro.

Configurar IP desde vSphere Web Client

Si no tiene acceso físico al host, puede utilizar vSphere Web Client para establecer la configuración de IP estática.

Procedimiento

- 1 Inicie sesión en vCenter Server desde vSphere Web Client.
- 2 Seleccione el host en el inventario.
- 3 En la pestaña **Administrar**, seleccione **Redes**.
- 4 Seleccione **Adaptadores virtuales**.
- 5 Seleccione **Red de administración vmk0** y haga clic en el icono de edición.
- 6 Seleccione **Configuración de IPv4**.
- 7 Seleccione **Usar configuración de IPv4 estática**.
- 8 Introduzca o modifique la configuración de la dirección IPv4 estática.
- 9 (opcional) Configure direcciones IPv6 estáticas.
 - a Seleccione **Configuración de IPv6**.
 - b Seleccione **Direcciones IPv6 estáticas**.
 - c Haga clic en el icono de adición.
 - d Escriba la dirección IPv6 y haga clic en **Aceptar**.
- 10 Haga clic en **Aceptar**.

Configurar DNS para ESXi

Puede seleccionar una configuración de DNS manual o automática del host ESXi.

El valor predeterminado es automático. Para que el DNS funcione, su entorno de red debe tener un servidor DHCP y un servidor DNS.

En entornos de red donde no hay DNS automático o no se desea que haya uno, puede configurar información de DNS estático, incluidos un nombre de host, un servidor de nombres principal, un servidor de nombres secundario y sufijos DNS.

Configurar DNS desde la consola directa

Si tiene acceso físico al host o acceso remoto a la consola directa, puede usar la consola directa para configurar información de DNS.

Procedimiento

- 1 Seleccione **Configurar red de administración** y presione Intro.
- 2 Seleccione **Configuración del DNS** y presione Intro.
- 3 Seleccione **Usar las siguientes direcciones de servidor DNS y nombre de host**.
- 4 Introduzca el servidor principal, el servidor alternativo (opcional) y el nombre de host.

Configurar sufijos DNS

Si tiene acceso físico al host, puede utilizar la consola directa para configurar la información del DNS. De forma predeterminada, DHCP adquiere los sufijos DNS.

Procedimiento

- 1 Desde la consola directa, seleccione **Configurar la red de administración**.
- 2 Seleccione **Personalizar sufijos DNS** y presione Intro.
- 3 Introduzca los nuevos sufijos DNS.

Probar la red de administración

Puede usar la consola directa para realizar pruebas de conectividad de red sencillas.

La consola directa realiza las siguientes pruebas.

- Hace ping en la puerta de enlace predeterminada
- Hace ping en el servidor de nombre del DNS principal
- Hace ping en el servidor de nombre del DNS secundario
- Resuelve el nombre de host configurado

Procedimiento

- 1 Desde la consola directa, seleccione **Probar red de administración** y presione Intro.
- 2 Presione Intro para comenzar la prueba.

Reiniciar los agentes de administración

Los agentes de administración sincronizan los componentes de VMware y permiten acceder al host ESXi mediante vSphere Web Client y vCenter Server. Se instalan con el software vSphere. Es posible que necesite reiniciar los agentes de administración si se interrumpe el acceso remoto.

Al reiniciar los agentes de administración, se reinician todos los agentes de administración y los servicios que están instalados y se ejecutan en `/etc/init.d` en el host ESXi. Generalmente, estos agentes incluyen `hostd`, `ntpd`, `sfcdbd`, `slpd`, `wsman` y `vobd`. El software también reinicia Fault Domain Manager (FDM) si está instalado.

Los usuarios que accedan a este host a través de vSphere Web Client y vCenter Server perderán la conectividad cuando reinicie los agentes de administración.

Procedimiento

- 1 Desde la consola directa, seleccione **Opciones de solución de problemas** y presione Intro.
- 2 Seleccione **Reiniciar agentes de administración** y presione Intro.
- 3 Presione F11 para confirmar el reinicio.

Resultados

El host ESXi reiniciará los servicios y los agentes de administración.

Reiniciar la red de administración

Puede que sea necesario reiniciar la interfaz de red de administración para restaurar la red o renovar una concesión de DHCP.

Si se reinicia la red de administración, se produce una breve interrupción de red que puede afectar temporalmente a las máquinas virtuales en ejecución.

Si una concesión de DHCP renovada provoca una nueva identidad de red (dirección IP o nombre de host), se desconecta el software de administración remota.

Procedimiento

- 1 Desde la consola directa, seleccione **Reiniciar red de administración** y presione Intro.
- 2 Presione F11 para confirmar el reinicio.

Restauración del conmutador estándar

vSphere Distributed Switch funciona como un único conmutador virtual en todos los hosts asociados. Las máquinas virtuales pueden mantener una configuración de red coherente cuando se migran a varios hosts. Si migra un conmutador estándar existente o un adaptador virtual a Distributed Switch, y este deja de ser necesario o deja de funcionar, puede restaurar el conmutador estándar para asegurarse de que el host siga estando accesible.

Cuando restaura el conmutador estándar, se crea un nuevo adaptador virtual y el vínculo superior de red de administración conectado actualmente a Distributed Switch se migra al nuevo conmutador virtual.

Es posible que necesite restaurar el conmutador estándar por las siguientes razones:

- Distributed Switch no se necesita o no funciona.
- Es necesario reparar Distributed Switch para restaurar la conectividad con vCenter Server y los hosts deben permanecer accesibles.
- No es deseable que vCenter Server administre el host. Cuando el host no está conectado a vCenter Server, la mayoría de las características de Distributed Switch no están disponibles para el host.

Requisitos previos

Compruebe que la red de administración esté conectada a un conmutador distribuido.

Procedimiento

- 1 En la consola directa, seleccione **Restaurar conmutador estándar** y presione Intro.

Si el host se encuentra en un conmutador estándar, la opción aparece atenuada y no puede seleccionarla.

- 2 Presione F11 para confirmar.

Prueba de la conectividad con los dispositivos y las redes

Puede utilizar la consola directa para realizar algunas pruebas simples de conectividad de red. Además de la red de administración, se pueden especificar otros dispositivos y otras redes.

Procedimiento

- 1 Desde la consola directa, seleccione **Probar red de administración** y presione Intro.
- 2 Escriba las direcciones a las que desee emitir un ping u otro nombre de host DNS que desee resolver.
- 3 Presione Intro para comenzar la prueba.

Comportamiento de almacenamiento

Al iniciar ESXi, el host entra en una fase de autoconfiguración durante la que se configuran los dispositivos de almacenamiento del sistema con los valores predeterminados.

Cuando reinicie el host ESXi después de instalar la imagen de ESXi, el host configura los dispositivos de almacenamiento del sistema con la configuración predeterminada. De forma predeterminada, todos los discos internos vacíos visibles se formatean con VMFS a fin de que sea posible almacenar máquinas virtuales en los discos. En ESXi Embedded, todos los discos internos vacíos visibles con VMFS también se formatean de forma predeterminada.

Precaución ESXi sobrescribe cualquier disco que parezca estar vacío. Los discos se consideran vacíos si no poseen una tabla de particiones o particiones válidas. Si usa software que utiliza dichos discos, en particular si está utilizando un administrador de volúmenes lógicos (LVM) en lugar de o además de esquemas tradicionales de particionamiento, ESXi podría causar un reformato del LVM local. Realice una copia de seguridad de los datos del sistema antes de habilitar ESXi por primera vez.

En el disco duro o dispositivo USB desde el que arranca el host ESXi, el software de formateo de discos conserva las particiones de diagnóstico existentes que el proveedor de hardware crea. En el espacio restante, el software crea las particiones descritas en [Tabla 5-3. Particiones creadas por ESXi en la unidad del host](#).

Tabla 5-3. Particiones creadas por ESXi en la unidad del host

Versión de ESXi	Particiones creadas
ESXi Installable	<p>Para instalaciones desde cero, se crean varias particiones nuevas para los bancos de arranque, la partición de trabajo y el bloqueador. Las instalaciones desde cero de ESXi utilizan las tablas de particiones GUID (GPT) en lugar del particionamiento basado en MSDOS. La tabla de particiones en sí se establece como parte de la imagen binaria y se escribe en el disco en el mismo momento que se instala el sistema. El instalador de ESXi deja las particiones de trabajo y de VMFS vacías, y ESXi las crea cuando el host se reinicia por primera vez después de la instalación o actualización. Solo se crea una partición de trabajo VFAT de 4 GB para el intercambio de sistema. Consulte Acerca de la partición desde cero. La partición de trabajo VFAT se crea solo en el disco desde el que se arranca el host ESXi.</p> <hr/> <p>Nota Para crear el volumen VMFS y una partición de trabajo con la instalación, el instalador de ESXi requiere un mínimo de 5,2 GB de espacio libre en el disco de instalación.</p> <hr/> <p>El instalador afecta solamente al disco de instalación. El instalador no afecta a otros discos del servidor. Cuando se realiza la instalación en un disco, el instalador sobrescribe el disco completo. Cuando el instalador configura automáticamente el almacenamiento, no sobrescribe las particiones del proveedor de hardware. Durante la instalación de ESXi, el instalador crea una partición de diagnóstico de 110 MB para los volcados de memoria.</p>
ESXi Embedded	<p>Una partición de diagnóstico de 110 MB para los volcados de memoria, si la partición no está presente en otro disco. Las particiones de trabajo y diagnóstico VFAT se crean solo en el disco desde el que se arranca el host ESXi. En otros discos, el software crea una partición VMFS5 por disco vacío, utilizando todo el disco. Solo se formatean los discos vacíos.</p>
ESXi Installable y ESXi Embedded	<p>Una partición VMFS5 en el espacio libre restante.</p>

Es posible que desee anular este comportamiento predeterminado si, por ejemplo, utiliza dispositivos de almacenamiento compartido en lugar de almacenamiento local. A fin de evitar un formateo automático de discos, desconecte los dispositivos de almacenamiento local del host en las siguientes circunstancias:

- Antes de ejecutar el host por primera vez.
- Antes de ejecutar el host después de restablecerlo a los valores predeterminados de configuración.

Para anular el formateo VMFS, si ya se realizó el formateo automático de discos, puede eliminar el almacén de datos. Consulte la documentación de *Administración de vCenter Server y hosts*.

Acerca de la partición desde cero

Para nuevas instalaciones de ESXi, durante la fase de configuración automática se crea una partición desde cero VFAT de 4 GB si la partición no esté presente en otro disco.

Nota La creación de particiones de los hosts que se actualizan a ESXi 5.x desde versiones de ESXi anteriores a la 5.0 se diferencia en gran medida de la creación de particiones para nuevas instalaciones de ESXi 5.x. Consulte la documentación de *Actualización de vSphere*.

Cuando ESXi arranca, el sistema intenta buscar una partición adecuada en un disco local para crear una partición desde cero.

No se requiere la partición desde cero. Se usa para almacenar la salida de vm-support que se necesita cuando se crea un paquete compatible. Si no hay una partición desde cero, la salida de vm-support se almacena en un ramdisk. En situaciones con poca memoria, sería conveniente crear una partición desde cero si no hay una presente.

Para la versión instalable de ESXi, la partición se crea durante la instalación y se selecciona. VMware recomienda que no modifique la partición.

Nota Para crear el volumen y la partición desde cero de VMFS, el instalador de ESXi necesita un mínimo de 5,2 GB de espacio disponible en el disco de instalación.

Para ESXi Embedded, si no se encuentra una partición pero hay un disco local vacío, el sistema lo formatea y crea una partición desde cero. Si no se crea una partición desde cero, se puede configurar una, pero no es necesario que esta exista. También puede anular la configuración predeterminada. Sería conveniente crear la partición desde cero en un directorio remoto instalado de NFS.

Nota El instalador puede crear varias particiones de VFAT. La designación de VFAT no siempre indica que la partición sea desde cero. En algunos casos, una partición de VFAT simplemente puede quedar inactiva.

Establecer la partición desde cero de vSphere Web Client

Si no hay ninguna partición desde cero configurada, es posible que quiera configurar una, especialmente si le preocupa la memoria insuficiente. Si no hay una partición desde cero, el resultado de vm-support se almacena en un disco RAM.

Requisitos previos

El directorio que se usará para la partición temporal debe existir en el host.

Procedimiento

- 1 Desde vSphere Web Client, conéctese a vCenter Server.
- 2 Seleccione el host en el inventario.
- 3 Haga clic en la pestaña **Administrar**.

4 Seleccione **Configuración**.

5 Seleccione **Configuración avanzada del sistema**.

El parámetro **ScratchConfig.CurrentScratchLocation** muestra la ubicación actual de la partición desde cero.

6 En el campo **ScratchConfig.ConfiguredScratchLocation**, introduzca una ruta de acceso de directorio que sea exclusiva para este host.

Por ejemplo, `/vmfs/volumes/DatastoreUUID/DatastoreFolder`.

7 Reinicie el host para que se apliquen los cambios.

El host se detiene inesperadamente durante el arranque cuando comparte un disco de arranque con otro host

Cuando dos hosts o más, ya sean físicos o virtuales, arrancan desde el mismo LUN o desde el mismo disco físico compartido, no pueden usar la misma partición temporal.

Problema

El host se detiene en el arranque cuando comparte un disco de arranque con otro host.

Causa

Dos hosts ESXi o más pueden compartir el mismo LUN o el mismo disco físico. Cuando hay dos hosts de este tipo que, además, tienen configurada la misma partición temporal, cualquiera de los dos hosts puede experimentar un error en el arranque.

Solución

1 Establezca los hosts para que arranquen de manera secuencial y, a continuación, arránquelos.

Esta configuración permite iniciar los hosts de manera tal que pueda cambiar la partición temporal para uno de ellos.

2 Desde vSphere Web Client, conéctese a vCenter Server.

3 Seleccione el host en el inventario.

4 Haga clic en la pestaña **Administrar**.

5 Haga clic en **Configuración**.

6 En Sistema, seleccione **Configuración avanzada del sistema**.

7 Seleccione **ScratchConfig**.

El campo **ScratchConfig.CurrentScratchLocation** muestra la ubicación actual de la partición temporal.

8 En el campo **ScratchConfig.ConfiguredScratchLocation**, introduzca una ruta de acceso de directorio que sea exclusiva para este host.

Por ejemplo, `/vmfs/volumes/DatastoreUUID/DatastoreFolder`.

- 9 Reinicie el host para que se apliquen los cambios.

Habilitar el acceso a ESXi Shell y SSH con la interfaz de usuario de la consola directa

Use la interfaz de usuario de la consola directa para habilitar ESXi Shell.

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 (opcional) Establezca el tiempo de espera de ESXi Shell.

De manera predeterminada, el tiempo de espera de ESXi Shell es 0 (deshabilitado).

La configuración del tiempo de espera de disponibilidad es la cantidad de minutos que pueden transcurrir antes de que deba iniciar sesión después de que se habilite ESXi Shell. Después del período de tiempo de espera, si no se ha iniciado sesión, el shell se deshabilita.

Nota Si inicia sesión y se agota el tiempo de espera, la sesión se mantiene activa. Sin embargo, ESXi Shell se deshabilitará, lo que impide que otros usuarios inicien sesión.

- a En el menú Opciones del modo de solución de problemas, seleccione **Modificar tiempos de espera de SSH y ESXi Shell** y presione Intro.
- b Introduzca el tiempo de espera de disponibilidad en minutos.

El tiempo de espera de disponibilidad es la cantidad de minutos que pueden transcurrir antes de que deba iniciar sesión después de que se habilite ESXi Shell.
- c Presione Intro.
- d Introduzca el tiempo de espera de inactividad.

El tiempo de inactividad es la cantidad de minutos que pueden transcurrir antes de que el usuario cierre sesión en 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.
- 6 Presione Esc hasta que vuelva al menú principal de la interfaz de usuario de la consola directa.

Ver registros del sistema

Los registros del sistema proporcionan información detallada sobre los eventos operativos del sistema.

Procedimiento

- 1 En la consola directa, seleccione **Ver registros del sistema**.
- 2 Presione la tecla numérica que corresponda para ver un registro.
Si agrega el host a vCenter Server, aparecen los registros de vCenter Server Agent (vpxa).
- 3 Presione Intro o la barra espaciadora para desplazarse por los mensajes.
- 4 Realice una búsqueda de expresiones regulares.
 - a Presione la tecla de barra diagonal (/).
 - b Escriba el texto que desea buscar.
 - c Presione Intro.El texto que se encontró aparece resaltado en la pantalla.
- 5 Presione q para volver a la consola directa.

Pasos siguientes

Consulte también [Configurar Syslog en hosts ESXi](#).

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
Syslog.global.defaultRotate	Establece el número máximo de archivos que se van a mantener. Puede configurar este número en forma global y para subregistradores individuales.
Syslog.global.defaultSize	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.
Syslog.global.LogDir	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> .
Syslog.global.logDirUnique	Al seleccionar esta opción, se crea un subdirectorio con el nombre del host ESXi del directorio especificado por Syslog.global.LogDir . Un directorio único es útil si varios hosts ESXi utilizan el mismo directorio NFS.
Syslog.global.LogHost	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.
 - a Haga clic en el nombre del registro que desea personalizar.
 - b 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.

Configurar el filtrado de registros en hosts ESXi

Las capacidades de filtrado de registros permiten modificar la directiva de registro del servicio de Syslog que se ejecuta en un host ESXi. Puede crear filtros de registros para reducir la cantidad de entradas repetidas en los registros de ESXi y agregar a la lista de no permitidos eventos de registros específicos en su totalidad.

Los filtros de registros afectan a todos los eventos de registros que el daemon `vm syslogd` del host ESXi procesa, ya sea que se registren en un directorio de registro o en un servidor remoto de Syslog.

Al crear un filtro de registro, se establece una cantidad máxima de entradas de registro para los mensajes de registro. Los mensajes de registros son generados por uno o más componentes del sistema especificado y coinciden con una frase especificada. Debe habilitar la capacidad de filtrado de registros y volver a cargar el daemon de Syslog para activar los filtros de registros en el host ESXi.

Importante Al establecer un límite para la cantidad de información de registro, se restringe la capacidad para solucionar correctamente los posibles errores del sistema. Si ocurre una rotación de registros después de que se alcance la cantidad máxima de entradas de registro, es posible que pierda todas las instancias de un mensaje filtrado.

Procedimiento

- 1 Inicie sesión en ESXi Shell como raíz.
- 2 En el archivo `/etc/vmware/logfilters`, agregue la siguiente entrada para crear un filtro de registro.

```
numLogs | ident | logRegex
```

donde:

- `numLogs` establece la cantidad máxima de entradas de registro para los mensajes de registro especificados. Una vez alcanzado este número, se filtran y se omiten los mensajes de registro especificados. Utilice `0` para filtrar y omitir todos los mensajes de registro especificados.
- `ident` especifica uno o más componentes del sistema para aplicar el filtro a los mensajes de registro que generan estos componentes. Para obtener información sobre los componentes del sistema que generan los mensajes de registro, consulte los valores de los parámetros de `idents` en los archivos de configuración de syslog. Los archivos se encuentran en el directorio `/etc/vmsyslog.conf.d`. Utilice una lista separada por comas para aplicar un filtro a varios componentes del sistema. Utilice `*` para aplicar un filtro a todos los componentes del sistema.
- `logRegex` especifica una frase que distingue mayúsculas de minúsculas con la sintaxis de la expresión regular Python para filtrar los mensajes de registro según su contenido.

Por ejemplo, para establecer un límite máximo de dos entradas de registro desde el componente `hostd` para mensajes que se asemejen a la frase `SOCKET connect failed`, error 2: No such file or directory con cualquier número de error, agregue la siguiente entrada:

```
2 | hostd | SOCKET connect failed, error .*: No such file or directory
```

Nota Una línea que comienza con `#` indica un comentario y se omite el resto de la línea.

- 3 En el archivo `/etc/vmsyslog.conf`, agregue la siguiente entrada para habilitar la capacidad de filtrado de registros.

```
enable_logfilters = true
```

- 4 Ejecute el comando `esxcli system syslog reload` para volver a cargar el daemon Syslog y aplicar los cambios de configuración.

Configurar el nivel de aceptación del perfil de imagen de host

El nivel de aceptación del perfil de imagen del host determina qué paquetes de instalación de vSphere (VIB) se aceptan para la instalación.

Las firmas de VIB se comprueban y se aceptan para la instalación según una combinación del nivel de aceptación de VIB y nivel de aceptación del perfil de imagen del host. Los VIB se etiquetan con un nivel de aceptación que depende del estado de la firma.

Consulte [Niveles de aceptación](#).

Requisitos previos

Privilegios requeridos: **Host.Configuration.Security Profile** and **Host.Configuration.Firewall**

Procedimiento

- 1 Desde vSphere Web Client, conéctese a vCenter Server.
- 2 Seleccione el host en el inventario.
- 3 Haga clic en la pestaña **Administrar**.
- 4 Haga clic en **Configuración**.
- 5 En Sistema, seleccione **Perfil de seguridad**.
- 6 Desplácese hacia abajo hasta Nivel de aceptación del perfil de imagen del host y haga clic en **Editar**.

- 7 Seleccione el nivel de aceptación y haga clic en **Aceptar**.

Tabla 5-4. Niveles de aceptación del perfil de imagen del host

Nivel de aceptación del perfil de imagen del host	Niveles aceptados de los VIB
Certificado por VMware	Certificado por VMware
Aceptado por VMware	Certificado por VMware, Aceptado por VMware
Creado por los partners	Certificado por VMware, Aceptado por VMware, Creado por los partners
Creado por la comunidad	Certificado por VMware, Aceptado por VMware, Creado por los partners, Creado por la comunidad

Restablecer la configuración del sistema

Si tiene problemas para determinar el origen de un problema con su host ESXi, puede restablecer la configuración del sistema.

Los cambios en la configuración del sistema pueden estar relacionados con diferentes problemas, incluidos los problemas de conectividad con la red y dispositivos. Restablecer la configuración del sistema podría resolver estos problemas. Si restablecer la configuración del sistema no resuelve el problema, puede descartar los cambios en la configuración realizados desde la configuración inicial como el origen del problema.

Cuando restablezca la configuración, el software anula todos los cambios en la configuración, elimina la contraseña de la cuenta de administrador (raíz) y reinicia el host. También podrían eliminarse los cambios en la configuración realizados por el proveedor del hardware, como la configuración de direcciones IP y la configuración de licencias.

El restablecimiento de la configuración no elimina las máquinas virtuales del host ESXi. Después de restablecer los valores predeterminados de configuración, las máquinas virtuales no aparecen visibles, pero puede volver a lograr que estén visibles reconfigurando el almacenamiento y volviendo a registrar las máquinas virtuales.

Precaución Cuando restablezca los valores predeterminados de configuración, los usuarios que están accediendo al host pierden conectividad.

Requisitos previos

Antes de restablecer la configuración, realice una copia de seguridad de su configuración de ESXi en caso de que desee restaurar su configuración.

Procedimiento

- 1 Realice una copia de seguridad de la configuración utilizando el comando `vicfg-cfgbackup` de vSphere CLI.
- 2 Desde la consola directa, seleccione **Restablecer la configuración del sistema** y presione Intro.

- 3 Presione F11 para confirmar.

Resultados

El sistema se reiniciará después de que la configuración se restablezca a los valores predeterminados.

Quitar todos los paquetes personalizados en ESXi

Después de agregar paquetes personalizados, puede que se decida quitarlos.

Requisitos previos

Antes de quitar paquetes personalizados, apague o migre las máquinas virtuales en ejecución fuera del host ESXi.

Procedimiento

- 1 Reinicie el host ESXi.
- 2 En la consola directa, seleccione **Quitar extensiones personalizadas** y presione F11 para confirmar.
- 3 Reinicie el host.

Resultados

Se quitan todos los paquetes personalizados.

Deshabilitación de la compatibilidad con caracteres no ASCII en los nombres de directorios y archivos de máquinas virtuales

De forma predeterminada, ESXi admite el uso de caracteres no ASCII para los nombres de directorios y archivos de máquinas virtuales. Para deshabilitar esto, modifique el archivo `/etc/vmware/hostd/config.xml`.

Después de deshabilitar esto, aún se puede introducir caracteres no ASCII para los nombres de las máquinas virtuales. Las interfaces de usuario de vSphere mostrarán los nombres de las máquinas virtuales con los caracteres no ASCII, pero ESXi convertirá los nombres de directorios y archivos reales a cadenas ASCII.

Procedimiento

- 1 Mediante un editor de texto, abra el archivo `/etc/vmware/hostd/config.xml` para el host ESXi.
- 2 En la etiqueta `<config></config>`, agregue el código siguiente.

```
<g11nSupport>false</g11nSupport>
```

- 3 Guarde y cierre el archivo.
- 4 Reinicie el host.

Desinstalar un host ESXi

Si no desea que el servidor sea un host ESXi, puede desinstalar el equipo host ESXi.

Procedimiento

- 1 Quite los almacenes de datos de VMFS en los discos internos para que los discos internos ya no se configuren para almacenar máquinas virtuales.
- 2 Cambie la configuración de arranque en el BIOS para que el host ya no arranque en ESXi.
- 3 Instale otro sistema operativo en su lugar.

Después de instalar y configurar ESXi

6

Una vez que ESXi está instalado y configurado, puede administrar el host mediante vSphere Web Client y vCenter Server, aplicar una licencia al host y crear una copia de seguridad de la configuración de ESXi.

También puede usar vSphere Client para conectarse directamente al host ESXi y administrarlo.

Este capítulo incluye los siguientes temas:

- [Administrar el host ESXi](#)
- [Licencias de hosts ESXi](#)
- [Instalar vSphere Client](#)

Administrar el host ESXi

vSphere Client ofrece la forma más sencilla de administrar su host ESXi y controlar sus máquinas virtuales.

También puede utilizar vSphere Web Client para conectarse y administrar vCenter Server a través de un explorador web. vSphere Web Client se instala junto con vCenter Server y vCenter Server Appliance, y puede utilizarlo para administrar sus hosts ESXi.

Licencias de hosts ESXi

Después de instalar ESXi, el software ofrece un período de evaluación de 60 días durante el cual se puede explorar el conjunto completo de funciones de vSphere que se obtienen con una licencia de vSphere Enterprise Plus. Debe asignar al host una licencia adecuada antes de que caduque el período de evaluación.

Los hosts ESXi incluyen licencias de vSphere que proporcionan capacidad por CPU. Para proporcionar las licencias correctas a los hosts, debe asignarles una licencia de vSphere que cuente con capacidad de CPU suficiente para abarcar todos los CPU de los hosts. La licencia debe admitir todas las funciones que utilizan los hosts. Por ejemplo, si los hosts están conectados a vSphere Distributed Switch, debe asignarles una licencia que incluya la característica vSphere Distributed Switch.

Puede emplear uno de los métodos siguientes para asignar licencias a los hosts ESXi:

- Asignar licencias a varios hosts a la vez mediante la función de administración de licencias de vSphere Web Client. Los hosts deben estar conectados a un sistema vCenter Server. Para obtener más información, consulte *Administración de vCenter Server y hosts*.
- Configurar licencias masivas mediante los comandos de PowerCLI. Las licencias masivas funcionan para todos los hosts ESXi, pero son especialmente útiles para los hosts aprovisionados con Auto Deploy. Consulte [Configurar licencias masivas](#)
- Asignar licencias individuales a los hosts ESXi por medio de una conexión directa con vSphere Client. Para obtener más información, consulte *Administración de vSphere con vSphere Client*.

Acerca de los modos de evaluación y con licencia de ESXi

Puede utilizar el modo de evaluación para explorar el conjunto completo de funciones para los hosts ESXi. El modo de evaluación proporciona un conjunto de funciones equivalente a una licencia de vSphere Enterprise Plus. Antes de que finalice el modo de evaluación, debe asignar a sus hosts una licencia que admita todas las funciones en uso.

Por ejemplo, en el modo de evaluación, puede utilizar la tecnología vSphere vMotion, la función vSphere HA, la característica vSphere DRS y otras características. Si desea continuar utilizando estas funciones, debe asignar una licencia que las admita.

La versión de los hosts ESXi Installable se instala siempre en el modo de evaluación. ESXi Embedded se ofrece preinstalado en el dispositivo de almacenamiento interno por parte de cada proveedor de hardware. Podría estar en el modo de evaluación o con licencia previa.

El período de evaluación es de 60 días y comienza cuando se enciende el host ESXi. En cualquier momento durante el período de evaluación de 60 días, se puede realizar la conversión de un modo con licencia a un modo de evaluación. El tiempo disponible en el modo de evaluación se resta del tiempo ya consumido.

Por ejemplo, supongamos que se utiliza un host ESXi en el modo de evaluación durante 20 días y, a continuación, se asigna una clave de licencia de vSphere Standard Edition al host. Si se vuelve a establecer el host en el modo de evaluación, se podrá explorar el conjunto completo de funciones para el host durante el período de evaluación restante de 40 días.

Para obtener información sobre la administración de licencias para los hosts ESXi, consulte la documentación *Administración de vCenter Server y hosts*.

Registro de la clave de licencia de un host ESXi

Si no es posible acceder a un host o arrancarlo, deberá tener un registro de su clave de licencia. Puede escribir la clave de licencia y pegarla con cinta en el servidor o colocar la clave de licencia en una ubicación segura. Puede acceder a la clave de licencia desde la interfaz de usuario de la consola directa o vSphere Web Client.

Ver las claves de licencia de los hosts ESXi desde vSphere Web Client

Puede ver las claves de licencia de los hosts que están conectados a un sistema vCenter Server a través de vSphere Web Client.

Procedimiento

- 1 En vSphere Web Client, seleccione **Administración**.
- 2 En Licencias, seleccione **Licencias**.
- 3 En la pestaña **Activos**, seleccione **Hosts**.
- 4 En la columna Licencia, haga clic en una licencia.

Resultados

Verá información sobre la licencia, como su uso y la clave de licencia.

Acceder a la clave de licencia de ESXi desde la consola directa

Si tiene acceso físico al host o acceso remoto a la consola directa, puede utilizar la consola directa para acceder a la clave de licencia de ESXi.

Procedimiento

- ◆ En la consola directa, seleccione **Ver información de soporte**.
La clave de licencia aparece con el formato XXXXX-XXXXX-XXXXX-XXXXX-XXXXX, etiquetada como Número de serie de la licencia.

Nota También aparece el número de serie del equipo físico, etiquetado como Número de serie. No confunda la clave de licencia con el número de serie del equipo físico.

Instalar vSphere Client

vSphere Client permite conectarse a un host ESXi.

Requisitos previos

- Compruebe si tiene el instalador de vCenter Server o el de vSphere Client.
- Compruebe si es miembro del grupo Administradores en el sistema.
- Compruebe si el sistema tiene conexión a Internet.

Procedimiento

- 1 Ejecute el instalador de vSphere Client de una de las siguientes maneras.

Opción	Descripción
Si va a realizar la instalación desde el instalador de vCenter Server	a En el directorio del instalador del software, haga doble clic en el archivo <code>autorun.exe</code> .
	b Seleccione vSphere™ Client .
	c Haga clic en Instalar .
Si descargó vSphere Client	Haga doble clic en el archivo <code>VMware-viclient-build number.exe</code> .

- 2 Siga las instrucciones del asistente para completar la instalación.

Resultados

Puede utilizar vSphere Client para conectarse a un host ESXi o a un sistema vCenter Server.

Antes de instalar vCenter Server o implementar vCenter Server Appliance

7

Puede instalar vCenter Server en un sistema físico o en una máquina virtual que esté ejecutándose en un host ESXi. También puede descargar e implementar vCenter Server Appliance en un host ESXi 5.0 o posteriores, o en una instancia de vCenter Server 5.0 o posteriores.

Este capítulo incluye los siguientes temas:

- Preparar las bases de datos de vCenter Server para la instalación
- Cómo influye vCenter Single Sign-On en la instalación
- Sincronizar los relojes en la red de vSphere
- Usar una cuenta de usuario para ejecutar vCenter Server
- Instalar vCenter Server en máquinas IPv6
- Ejecutar el instalador de vCenter Server desde una unidad de red
- Información obligatoria para instalar vCenter Server
- Información necesaria para la implementación de vCenter Server Appliance

Preparar las bases de datos de vCenter Server para la instalación

vCenter Server requiere una base de datos para almacenar y organizar datos de servidor. Es posible utilizar la base de datos en paquete de PostgreSQL que se puede instalar y configurar en el momento de la implementación, o se puede configurar una base de datos externa.

vCenter Server para Windows admite las bases de datos de Oracle y Microsoft SQL, mientras que vCenter Server Appliance solamente admite las bases de datos de Oracle como bases de datos externas.

Puede configurar una base de datos externa manualmente o mediante un script. Además, el usuario del nombre del origen de datos debe tener una lista específica de permisos.

Las contraseñas de las bases de datos se almacenan en texto no cifrado en el host físico o la máquina virtual de Windows en los que se instalan vCenter Server y vCenter Server Appliance. Los archivos que contienen las contraseñas están protegidos mediante la protección del sistema operativo, lo que significa que debe ser usuario raíz de Linux o administrador local de Windows para acceder a estos archivos y leerlos.

Las instancias de vCenter Server no pueden compartir el mismo esquema de base de datos. Varias bases de datos de vCenter Server pueden residir en el mismo servidor de bases de datos o pueden distribuirse entre varios servidores de bases de datos. Para las bases de datos de Oracle, que se basan en el concepto de objetos de esquema, se pueden ejecutar varias instancias de vCenter Server en un mismo servidor de bases de datos si se tiene un propietario de esquema diferente para cada instancia de vCenter Server. También se puede usar un servidor de bases de datos dedicado de Oracle para cada instancia de vCenter Server.

No se puede instalar vCenter Server y apuntar a una base de datos externa anterior de vCenter Server. Se puede actualizar la antigua base de datos de vCenter Server a la versión más reciente actualizando solo la instancia de vCenter Server que está conectada a la base de datos. Para obtener información sobre la actualización de vCenter Server, consulte *Actualización de vSphere*.

Notas sobre la configuración de la base de datos de vCenter Server

Después de seleccionar un tipo de base de datos compatible, asegúrese de comprender los requisitos de configuración especiales.

[Tabla 7-1. Notas sobre la configuración de bases de datos compatibles con vCenter Server](#) no es una lista completa de bases de datos compatibles con vCenter Server y vCenter Server Appliance. Para obtener información sobre las versiones de bases de datos y las configuraciones de service pack específicas compatibles con vCenter Server, consulte las [matrices de interoperabilidad de productos VMware](#). vCenter Server Appliance admite las mismas versiones de bases de datos de Oracle que vCenter Server. En [Tabla 7-1. Notas sobre la configuración de bases de datos compatibles con vCenter Server](#) solo se proporcionan notas de configuración de bases de datos especiales que no se enumeran en las matrices de interoperabilidad de productos.

Las bases de datos de vCenter Server requieren un conjunto de códigos UTF.

Póngase en contacto con su administrador de base de datos para obtener las credenciales de base de datos adecuadas.

Tabla 7-1. Notas sobre la configuración de bases de datos compatibles con vCenter Server

Tipo de base de datos	Notas sobre la configuración
PostgreSQL	<p>En vCenter Server 6.0, la base de datos incluida de PostgreSQL es adecuada para entornos con hasta 20 hosts y 200 máquinas virtuales. En vCenter Server Appliance, puede usar la base de datos integrada de PostgreSQL para entornos con hasta 1.000 hosts y 10.000 máquinas virtuales.</p> <p>Importante Si utiliza la base de datos integrada de PostgreSQL, al desinstalar vCenter Server en Windows, se desinstalará la base de datos integrada y se perderán todos los datos.</p>
Microsoft SQL Server 2008 R2 SP2 o superior	<p>Asegúrese de que el equipo tenga una entrada de DSN de ODBC válida.</p> <p>Nota Esta base de datos no es compatible con vCenter Server Appliance.</p>
Microsoft SQL Server 2012	<p>Asegúrese de que el equipo tenga una entrada de DSN de ODBC válida.</p> <p>Nota Esta base de datos no es compatible con vCenter Server Appliance.</p>

Tabla 7-1. Notas sobre la configuración de bases de datos compatibles con vCenter Server (continuación)

Tipo de base de datos	Notas sobre la configuración
Microsoft SQL Server 2014	<p>Asegúrese de que el equipo tenga una entrada de DSN de ODBC válida.</p> <p>Nota Esta base de datos no es compatible con vCenter Server Appliance.</p>
Oracle 11g y Oracle 12c	<p>Asegúrese de que el equipo tenga una entrada de DSN de ODBC válida.</p> <p>Después de completar la instalación de vCenter Server, aplique la última revisión al cliente y el servidor de Oracle.</p>

Configurar bases de datos de Microsoft SQL Server

Si desea usar una base de datos de Microsoft SQL para su repositorio de vCenter Server, configure la base de datos que funcionará con vCenter Server.

Puede instalar y configurar la base de datos Microsoft SQL Server en el mismo equipo en el que instalará vCenter Server. Puede instalar y configurar la base de datos Microsoft SQL Server en otro equipo.

Procedimiento

1 Preparar la base de datos de SQL Server de vCenter Server

Primero debe crear una base de datos y un usuario para vCenter Server. A continuación, podrá asignar permisos al usuario de base de datos de vCenter Server mediante el esquema de dbo y la función dbo_owner existentes, o mediante la creación de un esquema y unas funciones de base de datos personalizados.

2 (opcional) Usar un script para crear manualmente objetos de base de datos de Microsoft SQL Server

En este tema se describe la creación de objetos de base de datos de forma manual, en vez de permitir la creación automática de los mismos por parte del instalador de vCenter Server.

3 Configurar una conexión de ODBC de SQL Server

Tras crear y configurar una base de datos de SQL Server y un usuario para vCenter Server, debe crear un DSN de 64 bits en el equipo en el que instalará vCenter Server. Durante la instalación de vCenter Server, usará el DSN para establecer una conexión entre vCenter Server y la base de datos.

4 Configurar TCP/IP de Microsoft SQL Server para JDBC

Si la base de datos de Microsoft SQL Server posee TCP/IP deshabilitado y no se configuran los puertos dinámicos, la conexión JDBC permanece cerrada. La conexión cerrada provoca un funcionamiento incorrecto de las estadísticas de vCenter Server. Puede configurar TCP/IP del servidor para JDBC.

Preparar la base de datos de SQL Server de vCenter Server

Primero debe crear una base de datos y un usuario para vCenter Server. A continuación, podrá asignar permisos al usuario de base de datos de vCenter Server mediante el esquema de dbo y la función dbo_owner existentes, o mediante la creación de un esquema y unas funciones de base de datos personalizados.

Requisitos previos

Inicie sesión en Microsoft SQL Server Management Studio como sysadmin (SA) o con una cuenta de usuario con privilegios sysadmin.

Preparar la base de datos de vCenter Server mediante el esquema dbo y la función de base de datos db_owner

El modo más sencillo de asignar permisos a un usuario de la base de datos de vCenter Server es mediante la función de base de datos db_owner.

Primero debe crear una base de datos y un usuario para vCenter Server. A continuación, podrá usar la función de base de datos db_owner y permitir que el instalador de vCenter Server cree el esquema de dbo predeterminado que asigna los permisos de usuario de base de datos a dicha función. También debe habilitar la supervisión de la base de datos del usuario antes de instalar vCenter Server. Consulte [Requisitos de permisos de base de datos para vCenter Server](#).

Para realizar el siguiente procedimiento, puede usar la interfaz de usuario gráfica o ejecutar scripts. El paquete del instalador de vCenter Server contiene scripts de ejemplo en el archivo vCenter-Server\dbschema\DB_and_schema_creation_scripts_PostgreSQL.txt.

Procedimiento

- 1 Cree una base de datos y un usuario para vCenter Server.
 - a En la base de datos principal, cree una base de datos para vCenter Server.
 - b Cree un usuario de base de datos para vCenter Server y asígnelo a las bases de datos de vCenter Server y msdb.

Por ejemplo, para crear el VCDB de la base de datos y el usuario vpxuser, puede ejecutar el siguiente script:

```
use master
go
CREATE DATABASE VCDB ON PRIMARY
(NAME = N'vcdb', FILENAME = N'C:\database_path\VCDB.mdf', SIZE = 10MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\database_path\VCDB.ldf', SIZE = 1000KB, FILEGROWTH = 10%)
COLLATE SQL_Latin1_General_CP1_CI_AS
go
use VCDB
go
CREATE LOGIN vpxuser WITH PASSWORD=N'vpxuser!0', DEFAULT_DATABASE=VCDB,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
```

```
CREATE USER vpxuser for LOGIN vpxuser
go
use MSDB
go
CREATE USER vpxuser for LOGIN vpxuser
go
```

Ahora tiene una base de datos Microsoft SQL Server que puede utilizar con vCenter Server.

- 2 Asigne la función db_owner al usuario de la base de datos de vCenter Server en las bases de datos de vCenter Server y msdb.

Por ejemplo, para asignar la función db_owner al usuario vpxuser, puede ejecutar el siguiente script:

```
use VCDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
go
use MSDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
go
```

- 3 Habilite la supervisión de la base de datos para el usuario de base de datos de vCenter Server.

Por ejemplo, para conceder permisos de supervisión de tamaño del disco de la base de datos, puede ejecutar el siguiente script:

```
use master
go
grant VIEW SERVER STATE to vpxuser
go
GRANT VIEW ANY DEFINITION TO vpxuser
go
```

Resultados

Cuando se instala vCenter Server, el instalador usa el esquema dbo predeterminado para asignar permisos a la función db_owner.

Preparar la base de datos de vCenter Server mediante la creación de un esquema y unas funciones de base de datos personalizados

Como alternativa al uso de la función de base de datos db_owner, los administradores de bases de datos con experiencia pueden establecer permisos mediante la creación del esquema y las funciones de base de datos de forma manual, lo que permite un mayor control sobre los permisos de la base de datos.

Primero debe crear una base de datos y un usuario para vCenter Server. A continuación, podrá crear un esquema personalizado y nuevas funciones de base de datos para el usuario de la base de datos. También debe habilitar la supervisión de la base de datos del usuario antes de instalar vCenter Server. Consulte [Requisitos de permisos de base de datos para vCenter Server](#).

Para realizar el siguiente procedimiento, puede usar la interfaz de usuario gráfica o ejecutar scripts. El paquete del instalador de vCenter Server contiene scripts de ejemplo en el archivo `vCenter-Server\dbschema\DB_and_schema_creation_scripts_PostgreSQL.txt`.

Procedimiento

- 1 Cree una base de datos y un usuario para vCenter Server.
 - a En la base de datos principal, cree una base de datos para vCenter Server.
 - b Cree un usuario de base de datos para vCenter Server y asígnelo a las bases de datos de vCenter Server y msdb.

Por ejemplo, para crear el VCDB de la base de datos y el usuario vpxuser, puede ejecutar el siguiente script:

```
use master
go
CREATE DATABASE VCDB ON PRIMARY
(NAME = N'vcdb', FILENAME = N'C:\database_path\VCDB.mdf', SIZE = 10MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\database_path\VCDB.ldf', SIZE = 1000KB, FILEGROWTH = 10%)
COLLATE SQL_Latin1_General_CP1_CI_AS
go
use VCDB
go
CREATE LOGIN vpxuser WITH PASSWORD=N'vpxuser!0', DEFAULT_DATABASE=VCDB,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
CREATE USER vpxuser for LOGIN vpxuser
go
use MSDB
go
CREATE USER vpxuser for LOGIN vpxuser
go
```

Ahora tiene una base de datos Microsoft SQL Server que puede utilizar con vCenter Server.

- 2 En la base de datos de vCenter Server, cree un esquema de base de datos y asígnelo al usuario de base de datos de vCenter Server.

Por ejemplo, para crear el esquema VMW en VCDB y asignarlo al usuario vpxuser, puede ejecutar el siguiente script:

```
use VCDB
CREATE SCHEMA VMW
go
ALTER USER vpxuser WITH DEFAULT_SCHEMA =VMW
```

- 3 En la base de datos de vCenter Server, cree privilegios y asígneles a las funciones de base de datos VC_ADMIN_ROLE y VC_USER_ROLE; a continuación, asigne dichas funciones al usuario de base de datos de vCenter Server.

Por ejemplo, para crear las funciones de VCDB y asignarlas al usuario vpxuser, puede ejecutar el siguiente script:

```
use VCDB
go
if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
CREATE ROLE VC_ADMIN_ROLE;
GRANT ALTER ON SCHEMA :: VMW to VC_ADMIN_ROLE;
GRANT REFERENCES ON SCHEMA :: VMW to VC_ADMIN_ROLE;
GRANT INSERT ON SCHEMA :: VMW to VC_ADMIN_ROLE;

GRANT CREATE TABLE to VC_ADMIN_ROLE;
GRANT CREATE VIEW to VC_ADMIN_ROLE;
GRANT CREATE Procedure to VC_ADMIN_ROLE;

if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_USER_ROLE')
CREATE ROLE VC_USER_ROLE
go
GRANT SELECT ON SCHEMA :: VMW to VC_USER_ROLE
go
GRANT INSERT ON SCHEMA :: VMW to VC_USER_ROLE
go
GRANT DELETE ON SCHEMA :: VMW to VC_USER_ROLE
go
GRANT UPDATE ON SCHEMA :: VMW to VC_USER_ROLE
go
GRANT EXECUTE ON SCHEMA :: VMW to VC_USER_ROLE
go
sp_addrolemember VC_USER_ROLE , vpxuser
go
sp_addrolemember VC_ADMIN_ROLE , vpxuser
go
```

- 4 En la base de datos de msdb, cree privilegios y asígneles a la función de base de datos VC_ADMIN_ROLE; a continuación, asigne dicha función al usuario de base de datos de vCenter Server.

Por ejemplo, para crear las funciones y asignarlas al usuario vpxuser, puede ejecutar el siguiente script:

```
use MSDB
go
if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
CREATE ROLE VC_ADMIN_ROLE;
go
GRANT SELECT on msdb.dbo.syscategories to VC_ADMIN_ROLE
go
GRANT SELECT on msdb.dbo.sysjobsteps to VC_ADMIN_ROLE
go
GRANT SELECT ON msdb.dbo.sysjobs to VC_ADMIN_ROLE
```

```
go
GRANT SELECT ON msdb.dbo.sysjobs_view to VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE
go
sp_addrolemember VC_ADMIN_ROLE , vpxuser
go
```

Nota La función VC_ADMIN_ROLE de la base de datos de msdb solo es necesaria durante la instalación y la actualización de vCenter Server. Tras la instalación o la actualización, puede retirar la función y desactivarla para futuras actualizaciones, o puede quitarla para mejorar la seguridad.

- 5 Habilite la supervisión de la base de datos para el usuario de base de datos de vCenter Server. Por ejemplo, para conceder permisos de supervisión de tamaño del disco de la base de datos, puede ejecutar el siguiente script:

```
use master
go
grant VIEW SERVER STATE to vpxuser
go
GRANT VIEW ANY DEFINITION TO vpxuser
go
```

Usar un script para crear manualmente objetos de base de datos de Microsoft SQL Server

En este tema se describe la creación de objetos de base de datos de forma manual, en vez de permitir la creación automática de los mismos por parte del instalador de vCenter Server.

Procedimiento

- 1 Inicie sesión en Microsoft SQL Server Management Studio con la cuenta de usuario de base de datos de vCenter Server que creó en las bases de datos de vCenter Server y msdb.
- 2 En el paquete de instalación de vCenter Server, busque los scripts de dbschema en el directorio vCenter-Server/dbschema.

- 3 Abra los archivos `VCDB_mssql.SQL` y `TopN_DB_mssql.sql` con Microsoft SQL Server Management Studio y reemplace todas las ocurrencias de `$schema` con el nombre del esquema.
- 4 Abra el archivo `VCDB_views_mssql.sql` con Microsoft SQL Server Management Studio y, tras cada una de las ocurrencias de `;`, inserte una nueva línea y escriba `go`.
- 5 Ejecute los scripts en una secuencia en la base de datos.

El usuario de DBO debe ser el propietario de los objetos que se crearon con estos scripts. Abra los scripts uno a uno en Microsoft SQL Server Management Studio y pulse F5 para ejecutar cada script en el siguiente orden:

- a `VCDB_mssql.SQL`
- b `insert_stats_proc_mssql.sql`
- c `load_stats_proc_mssql.sql`
- d `purge_stat2_proc_mssql.sql`
- e `purge_stat3_proc_mssql.sql`
- f `purge_usage_stats_proc_mssql.sql`
- g `stats_rollup1_proc_mssql.sql`
- h `stats_rollup2_proc_mssql.sql`
- i `stats_rollup3_proc_mssql.sql`
- j `cleanup_events_mssql.sql`
- k `delete_stats_proc_mssql.sql`
- l `upsert_last_event_proc_mssql.sql`
- m `load_usage_stats_proc_mssql.sql`
- n `TopN_DB_mssql.sql`
- o `calc_topn1_proc_mssql.sql`
- p `calc_topn2_proc_mssql.sql`
- q `calc_topn3_proc_mssql.sql`
- r `calc_topn4_proc_mssql.sql`
- s `clear_topn1_proc_mssql.sql`
- t `clear_topn2_proc_mssql.sql`
- u `clear_topn3_proc_mssql.sql`
- v `clear_topn4_proc_mssql.sql`
- w `rule_topn1_proc_mssql.sql`

```
x rule_topn2_proc_mssql.sql
y rule_topn3_proc_mssql.sql
z rule_topn4_proc_mssql.sql
aa process_license_snapshot_mssql.sql
ab l_stats_rollup3_proc_mssql.sql
ac l_purge_stat2_proc_mssql.sql
ad l_purge_stat3_proc_mssql.sql
ae l_stats_rollup1_proc_mssql.sql
af l_stats_rollup2_proc_mssql.sql
ag VCDB_views_mssql.sql
```

6 (opcional) Ejecute los scripts para habilitar la supervisión del estado de la base de datos.

```
a job_dbm_performance_data_mssql.sql
b process_performance_data_mssql.sql
```

7 Para todas las ediciones compatibles de Microsoft SQL Server, excepto Microsoft SQL Server Express, ejecute los scripts para configurar trabajos programados en la base de datos.

Estos scripts aseguran que el servicio de SQL Server Agent esté en ejecución.

```
a job_schedule1_mssql.sql
b job_schedule2_mssql.sql
c job_schedule3_mssql.sql
d job_cleanup_events_mssql.sql
e job_topn_past_day_mssql.sql
f job_topn_past_week_mssql.sql
g job_topn_past_month_mssql.sql
h job_topn_past_year_mssql.sql
```

8 Para todos los procedimientos que creó en [Paso 5](#), otorgue el privilegio de ejecución al usuario de base de datos de vCenter Server en la base de datos vCenter Server.

Por ejemplo, para conceder el permiso de ejecución de los procedimientos al usuario y vpxuser, puede ejecutar el siguiente script.

```
grant execute on insert_stats_proc to vpxuser
grant execute on purge_stat2_proc to vpxuser
grant execute on purge_stat3_proc to vpxuser
grant execute on purge_usage_stat_proc to vpxuser
grant execute on stats_rollup1_proc to vpxuser
grant execute on stats_rollup2_proc to vpxuser
```



```

grant execute on stats_rollup3_proc to vpxuser
grant execute on cleanup_events_tasks_proc to vpxuser
grant execute on delete_stats_proc to vpxuser
grant execute on upsert_last_event_proc to vpxuser
grant execute on load_usage_stats_proc to vpxuser
grant execute on load_stats_proc to vpxuser
grant execute on calc_topn1_proc to vpxuser
grant execute on calc_topn2_proc to vpxuser
grant execute on calc_topn3_proc to vpxuser
grant execute on calc_topn4_proc to vpxuser
grant execute on clear_topn1_proc to vpxuser
grant execute on clear_topn2_proc to vpxuser
grant execute on clear_topn3_proc to vpxuser
grant execute on clear_topn4_proc to vpxuser
grant execute on rule_topn1_proc to vpxuser
grant execute on rule_topn2_proc to vpxuser
grant execute on rule_topn3_proc to vpxuser
grant execute on rule_topn4_proc to vpxuser
grant execute on process_license_snapshot_proc to vpxuser
grant execute on l_stats_rollup3_proc to vpxuser
grant execute on l_purge_stat2_proc to vpxuser
grant execute on l_purge_stat3_proc to vpxuser
grant execute on l_stats_rollup1_proc to vpxuser
grant execute on l_stats_rollup2_proc to vpxuser

```

Si se ejecutó el script `process_performance_data_mssql.sql` en [Paso 5](#), otorgue el siguiente privilegio de ejecución a la base de datos de vCenter Server.

```

grant execute on process_performance_data_proc to vpxuser

```

Resultados

Ha creado las tablas de vCenter Server de forma manual.

Nota Durante la instalación de vCenter Server, cuando aparezca el mensaje de advertencia de reinicialización, seleccione **No sobrescribir, dejar la base de datos existente como está** y continúe con la instalación.

Configurar una conexión de ODBC de SQL Server

Tras crear y configurar una base de datos de SQL Server y un usuario para vCenter Server, debe crear un DSN de 64 bits en el equipo en el que instalará vCenter Server. Durante la instalación de vCenter Server, usará el DSN para establecer una conexión entre vCenter Server y la base de datos.

Si usa SQL Server para vCenter Server, no utilice la base de datos maestra ni ninguna otra base de datos del sistema.

Consulte la documentación de ODBC de Microsoft SQL para obtener instrucciones específicas para configurar la conexión de ODBC de SQL Server.

Precaución Si está usando una instancia con nombre de Microsoft SQL Server 2008 Standard Edition con vCenter Server, no coloque el nombre MSSQLSERVER a la instancia. Si lo hace, la conexión JDBC no funciona y ciertas funciones, como Gráficos de rendimiento, no están disponibles.

Requisitos previos

Implementar SQL Native Client versión 10 u 11.

Procedimiento

- 1 En el equipo en el que instalará vCenter Server, seleccione **Inicio > Herramientas de administración > Orígenes de datos (ODBC)**.
- 2 En la pestaña **DSN del sistema**, modifique una conexión de ODBC de SQL Server existente o cree una nueva.
 - Para modificar una conexión de ODBC de SQL Server existente, seleccione la conexión desde la lista Origen de datos del sistema y haga clic en **Configurar**.

Importante El DSN existente debe usar SQL Native Client versión 10 u 11.

- Para crear una nueva conexión de ODBC de SQL Server, haga clic en **Agregar**, seleccione **SQL Native Client** y presione en **Finalizar**.
- 3 En el cuadro de texto **Nombre**, introduzca un nombre para el origen de datos ODBC (DSN). Por ejemplo, **VMware vCenter Server**.
 - 4 (opcional) En el cuadro de texto **Descripción**, introduzca una descripción del DSN de ODBC.
 - 5 En el cuadro de texto **Servidor**, introduzca la dirección IP o FQDN de SQL Server y, si desea utilizar un puerto no predeterminado para acceder a SQL Server, introduzca un puerto personalizado separado con una coma.

Por ejemplo, si la dirección IP de SQL Server es 10.160.10.160 y desea acceder al servidor mediante el puerto personalizado 8347, introduzca **10.160.10.160,8347**.

Nota No se puede usar un alias de servidor de base de datos para crear un DSN.

- 6 Seleccione un método de autenticación.

- **Integrar autenticación de Windows.**

Además, también puede escribir el nombre principal de servicio (SPN, Service Principal Name).

Importante No puede utilizar esta opción si el servicio vCenter Server se ejecuta en una cuenta del sistema integrada de Microsoft Windows.

■ Autenticación de SQL Server.

Introduzca su nombre de inicio de sesión y contraseña de SQL Server.

- 7 Seleccione la base de datos creada para el sistema vCenter Server en el menú **Cambiar la base de datos predeterminada a**.
- 8 Haga clic en **Finalizar**.
- 9 Pruebe el origen de los datos. Para ello, seleccione **Probar origen de datos** y haga clic en **Aceptar** en el menú **Configuración de Microsoft SQL Server de ODBC**.
- 10 Compruebe que SQL Agent esté en ejecución en el servidor de base de datos.

Configurar TCP/IP de Microsoft SQL Server para JDBC

Si la base de datos de Microsoft SQL Server posee TCP/IP deshabilitado y no se configuran los puertos dinámicos, la conexión JDBC permanece cerrada. La conexión cerrada provoca un funcionamiento incorrecto de las estadísticas de vCenter Server. Puede configurar TCP/IP del servidor para JDBC.

Esta tarea se aplica a los servidores de base de datos remotos de Microsoft SQL Server. Puede omitir esta tarea si la base de datos se encuentra en el mismo equipo que vCenter Server.

Procedimiento

- 1 Seleccione **Inicio > Todos los programas > Microsoft SQL Server > Herramienta de configuración > Administrador de configuración de SQL Server**.
- 2 Seleccione **Configuración de red de SQL Server > Protocolos para *nombre de la instancia***.
- 3 Habilite TCP/IP.
- 4 Abra Propiedades de TCP/IP.
- 5 En la pestaña **Protocolo**, cree las siguientes entradas.

Habilitado	Sí
Escuchar todo	Sí
Mantener conexión	30000

- 6 En la pestaña **Direcciones IP**, realice las siguientes selecciones.

activa	Sí
Puertos dinámicos de TCP	0

- 7 Reinicie el servicio SQL Server desde **Administrador de configuración de SQL Server > Servicios de SQL Server**.
- 8 Inicie el servicio SQL Server Browser desde **Administrador de configuración de SQL > Server Servicios de SQL Server**.

Configurar bases de datos de Oracle

Si desea utilizar una base de datos de Oracle para el repositorio de vCenter Server, configure la base de datos para que funcione con vCenter Server.

Puede instalar y configurar la base de datos de Oracle en el mismo equipo en el que instalará vCenter Server. Puede instalar y configurar la base de datos de Oracle en otro equipo.

Procedimiento

1 Preparar la base de datos de Oracle de vCenter Server

Para usar una base de datos de Oracle con vCenter Server, debe crear la base de datos con determinados espacios de tablas y privilegios, y el usuario de la base de datos con unos permisos concretos.

2 (opcional) Usar un script para crear un esquema de base de datos de Oracle

El instalador de vCenter Server crea el esquema durante la instalación. Para administradores de bases de datos experimentados que necesitan más control sobre la creación de esquemas debido a limitaciones de los entornos, puede opcionalmente utilizar un script para crear su esquema de base de datos.

3 Crear un nombre del servicio de red

Para configurar un DSN de ODBC de Oracle, debe tener un nombre del servicio de red para la base de datos. En el equipo en el que se ejecute la base de datos de Oracle, debe crear un nombre del servicio de red para el espacio de tablas de vCenter Server.

4 Configurar una conexión de ODBC de Oracle

Tras crear y configurar una base de datos de Oracle y un usuario para vCenter Server, debe crear un DSN de 64 bits en el equipo en el que instalará vCenter Server. Durante la instalación de vCenter Server, usará el DSN para establecer una conexión entre vCenter Server y la base de datos.

Preparar la base de datos de Oracle de vCenter Server

Para usar una base de datos de Oracle con vCenter Server, debe crear la base de datos con determinados espacios de tablas y privilegios, y el usuario de la base de datos con unos permisos concretos.

Primero debe crear un espacio de tablas y un usuario para vCenter Server. A continuación, conceda los permisos al usuario de la base de datos. También debe habilitar la supervisión de la base de datos del usuario antes de instalar vCenter Server. Consulte [Requisitos de permisos de base de datos para vCenter Server](#).

Para realizar el siguiente procedimiento, puede usar la interfaz de usuario gráfica o ejecutar scripts. El paquete del instalador de vCenter Server contiene scripts de ejemplo en el archivo `vCenter-Server\dbschema\DB_and_schema_creation_scripts_PostgreSQL.txt`.

Requisitos previos

Inicie sesión en una sesión de SQL*Plus con la cuenta del sistema.

Procedimiento

1 Cree un espacio de tablas para vCenter Server.

Por ejemplo, para crear el espacio de tablas VPX, puede ejecutar el siguiente script:

```
CREATE SMALLFILE TABLESPACE "VPX" DATAFILE 'C:\database_path\vpx01.dbf'
SIZE 1G AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

2 Cree un usuario de la base de datos con los permisos adecuados para vCenter Server.

Por ejemplo, para crear el usuario VPXADMIN, puede ejecutar el siguiente script:

```
CREATE USER "VPXADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE "VPX"
ACCOUNT UNLOCK;
grant connect to VPXADMIN;
grant resource to VPXADMIN;
grant create view to VPXADMIN;
grant create sequence to VPXADMIN;
grant create table to VPXADMIN;
grant create materialized view to VPXADMIN;
grant execute on dbms_lock to VPXADMIN;
grant execute on dbms_job to VPXADMIN;
grant select on dba_lock to VPXADMIN;
grant select on dba_tablespaces to VPXADMIN;
grant select on dba_temp_files to VPXADMIN;
grant select on dba_data_files to VPXADMIN;
grant select on v_$session to VPXADMIN;
grant unlimited tablespace to VPXADMIN;
```

De forma predeterminada, el rol RECURSO tiene asignados los privilegios **CREAR PROCEDIMIENTO**, **CREAR TABLA** y **CREAR SECUENCIA**. Si el rol RECURSO no posee estos privilegios, concédaselos al usuario de la base de datos de vCenter Server.

Nota En lugar de conceder espacio de tablas ilimitado, puede establecer una cuota específica de espacio de tablas. La cuota recomendada es ilimitada, con un mínimo de 500 MB. Para establecer una cuota ilimitada, utilice el siguiente comando:

```
alter user "VPXADMIN" quota unlimited on "VPX";
```

Si establece una cuota limitada, supervise el espacio de tablas restante disponible para evitar el error que se muestra a continuación.

```
ORA-01536: se superó la cuota de espacio para el espacio de tablas 'espacio de tablas'
```

De este modo, tendrá el usuario de la base de datos de Oracle para vCenter Server.

- 3 Habilite la supervisión de la base de datos para el usuario de base de datos de vCenter Server.

Por ejemplo, para conceder permisos de supervisión de tamaño del disco de la base de datos al usuario VPXADMIN, puede ejecutar el siguiente script:

```
grant select on v_$system_event to VPXADMIN;
grant select on v_$sysmetric_history to VPXADMIN;
grant select on v_$sysstat to VPXADMIN;
grant select on dba_data_files to VPXADMIN;
grant select on v_$loghist to VPXADMIN;
```

Usar un script para crear un esquema de base de datos de Oracle

El instalador de vCenter Server crea el esquema durante la instalación. Para administradores de bases de datos experimentados que necesitan más control sobre la creación de esquemas debido a limitaciones de los entornos, puede opcionalmente utilizar un script para crear su esquema de base de datos.

Procedimiento

- 1 Abra una ventana de SQL*Plus con un usuario que posea derechos de propiedad de esquemas en la base de datos de vCenter Server.
- 2 Busque los scripts dbschema en el directorio */directorio de instalación/vCenter-Server/dbschema* del paquete de instalación de vCenter Server.
- 3 En SQL*Plus, ejecute los scripts en orden en la base de datos.

- a VCDB_oracle.SQL
- b VCDB_views_oracle.SQL
- c insert_stats_proc_oracle.sql
- d load_stats_proc_oracle.sql
- e purge_stat2_proc_oracle.sql
- f purge_stat3_proc_oracle.sql
- g purge_usage_stats_proc_oracle.sql
- h stats_rollup1_proc_oracle.sql
- i stats_rollup2_proc_oracle.sql
- j stats_rollup3_proc_oracle.sql
- k cleanup_events_oracle.sql
- l delete_stats_proc_oracle.sql
- m load_usage_stats_proc_oracle.sql
- n TopN_DB_oracle.sql

- o calc_topn1_proc_oracle.sql
- p calc_topn2_proc_oracle.sql
- q calc_topn3_proc_oracle.sql
- r calc_topn4_proc_oracle.sql
- s clear_topn1_proc_oracle.sql
- t clear_topn2_proc_oracle.sql
- u clear_topn3_proc_oracle.sql
- v clear_topn4_proc_oracle.sql
- w rule_topn1_proc_oracle.sql
- x rule_topn2_proc_oracle.sql
- y rule_topn3_proc_oracle.sql
- z rule_topn4_proc_oracle.sql
- aa process_license_snapshot_oracle.sql
- ab l_purge_stat2_proc_oracle.sql
- ac l_purge_stat3_proc_oracle.sql
- ad l_stats_rollup1_proc_oracle.sql
- ae l_stats_rollup2_proc_oracle.sql
- af l_stats_rollup3_proc_oracle.sql

- 4 (opcional) También puede ejecutar los siguientes scripts para habilitar la supervisión de mantenimiento de la base de datos.

- a job_dbm_performance_data_oracle.sql
- b process_performance_data_oracle.sql

- 5 Para todas las ediciones compatibles de Oracle Server, ejecute los scripts para configurar los trabajos programados en la base de datos.

- a job_schedule1_oracle.sql
- b job_schedule2_oracle.sql
- c job_schedule3_oracle.sql
- d job_cleanup_events_oracle.sql
- e job_topn_past_day_oracle.sql
- f job_topn_past_week_oracle.sql
- g job_topn_past_month_oracle.sql

```
h job_topn_past_year_oracle.sql
```

Resultados

Ha creado las tablas de vCenter Server de forma manual.

Nota Durante la instalación de vCenter Server, cuando aparezca el mensaje de advertencia de reinicialización, seleccione **No sobrescribir, dejar la base de datos existente como está** y continúe con la instalación.

Crear un nombre del servicio de red

Para configurar un DSN de ODBC de Oracle, debe tener un nombre del servicio de red para la base de datos. En el equipo en el que se ejecute la base de datos de Oracle, debe crear un nombre del servicio de red para el espacio de tablas de vCenter Server.

Procedimiento

- 1 Use un editor de texto o el asistente de configuración de Net8 para abrir el archivo `tnsnames.ora` que se encuentra en el directorio `C:\Oracle\Oraxx\NETWORK\ADMIN`, donde `xx` corresponde a 10g o 11g.
- 2 Agregue la siguiente entrada, donde `HOST` corresponde al host administrado al que debe conectarse el cliente.

```
VPX_TNS =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS= (PROTOCOL=TCP) (HOST=vpxd-Oracle) (PORT=1521))
  )
  (CONNECT_DATA =
    (SERVICE_NAME = ORCL)
  )
)
```

Configurar una conexión de ODBC de Oracle

Tras crear y configurar una base de datos de Oracle y un usuario para vCenter Server, debe crear un DSN de 64 bits en el equipo en el que instalará vCenter Server. Durante la instalación de vCenter Server, usará el DSN para establecer una conexión entre vCenter Server y la base de datos.

Requisitos previos

Instale Oracle Client 11.2.0.3 p16656151 (revisión 19) o una versión posterior, 11.2.0.4, 12.1.0.1.12 o posterior, o 12.1.0.2.

Procedimiento

- 1 En el equipo en el que instalará vCenter Server, seleccione **Inicio > Herramientas de administración > Orígenes de datos (ODBC)**.

- 2 En la pestaña **DSN del sistema**, modifique una conexión de ODBC de Oracle existente o cree una nueva.
 - Para modificar una conexión de ODBC de Oracle existente, seleccione la conexión desde la lista Origen de datos del sistema y haga clic en **Configurar**.
 - Para crear una conexión de ODBC de Oracle, haga clic en **Agregar**, seleccione el cliente Oracle y haga clic en **Finalizar**.
- 3 En el cuadro de texto **Nombre del origen de datos**, introduzca un nombre para el origen de datos (DSN) ODBC.
 Por ejemplo, **VMware vCenter Server**.
- 4 (opcional) En el cuadro de texto **Descripción**, introduzca una descripción del DSN de ODBC.
- 5 En el cuadro de texto **Nombre de servicio de TNS**, escriba el nombre del servicio de red para la base de datos a la que desea conectarse.
 Por ejemplo, **VPX_TNS**.
 Este es el nombre de servicio de red que configuró anteriormente en el archivo `tnsnames.ora` que se encuentra en la carpeta `NETWORK\ADMIN` de la ubicación de instalación de la base de datos de Oracle.
- 6 En el cuadro de texto **Identificador de usuario**, escriba el nombre de usuario de la base de datos de vCenter Server.
 Por ejemplo, **VPXADMIN**.
- 7 Haga clic en **Probar conexión**.
- 8 En el cuadro de texto **Contraseña**, escriba la contraseña del usuario de la base de datos y haga clic en **Aceptar**.
 Si ha configurado el DNS correctamente, aparecerá el mensaje `Conexión correcta`.
- 9 Haga clic en **Aceptar**.

Requisitos de permisos de base de datos para vCenter Server

vCenter Server requiere una base de datos. Si decide utilizar una base de datos de Oracle o Microsoft SQL Server externa, cuando cree la base de datos, deberá conceder determinados permisos al usuario de la base de datos.

Tabla 7-2. Permisos de base de datos Microsoft SQL para vCenter Server

Permiso	Descripción
GRANT ALTER ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorio cuando trabaja con el esquema personalizado de SQL Server.
GRANT REFERENCES ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorio cuando trabaja con el esquema personalizado de SQL Server.
GRANT INSERT ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorio cuando trabaja con el esquema personalizado de SQL Server.

Tabla 7-2. Permisos de base de datos Microsoft SQL para vCenter Server (continuación)

Permiso	Descripción
GRANT CREATE TABLE TO VC_ADMIN_ROLE	Necesario para crear una tabla.
GRANT CREATE VIEW TO VC_ADMIN_ROLE	Necesario para crear una vista.
GRANT CREATE PROCEDURE TO VC_ADMIN_ROLE	Necesario para crear un procedimiento almacenado.
GRANT SELECT ON SCHEMA :: [VMW] TO VC_USER_ROLE	Permisos que permiten ejecutar las operaciones SELECT, INSERT, DELETE y UPDATE en tablas que son parte del esquema VMW.
GRANT INSERT ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT DELETE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT UPDATE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT EXECUTE ON SCHEMA :: [VMW] TO VC_USER_ROLE	Necesario para ejecutar un procedimiento almacenado en el esquema de base de datos.
GRANT SELECT ON msdb.dbo.syscategories TO VC_ADMIN_ROLE	Necesario para implementar trabajos de SQL Server. Estos permisos son obligatorios solo durante la instalación y actualización y no son necesarios después de la implementación.
GRANT SELECT ON msdb.dbo.sysjobsteps TO VC_ADMIN_ROLE	
GRANT SELECT ON msdb.dbo.sysjobs TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE	
GRANT VIEW SERVER STATE TO [vpxuser]	Proporciona acceso a las vistas DMV de SQL Server y a la ejecución de sp_lock.
GRANT VIEW ANY DEFINITION TO [vpxuser]	Necesario para proporcionar al usuario los privilegios para observar los metadatos para objetos de SQL Server.

Tabla 7-3. Permisos de base de datos de Oracle para vCenter Server

Permiso	Descripción
GRANT CONNECT TO VPXADMIN	Necesario para la conexión con la base de datos de Oracle.
GRANT RESOURCE TO VPXADMIN	Necesario para la creación de un activador, secuencia, tipo, procedimiento, etc. De forma predeterminada, el rol RECURSO posee asignados los privilegios CREAR PROCEDIMIENTO, CREAR TABLA y CREAR SECUENCIA. Si el rol RECURSO no posee estos privilegios, concédaselos al usuario de la base de datos de vCenter Server.
GRANT CREATE VIEW TO VPXADMIN	Necesario para crear una vista.
GRANT CREATE SEQUENCE TO VPXADMIN	Necesario para crear una secuencia.
GRANT CREATE TABLE TO VPXADMIN	Necesario para crear una tabla.
GRANT CREATE MATERIALIZED VIEW TO VPXADMIN	Necesario para crear una vista materializada.
GRANT EXECUTE ON dbms_lock TO VPXADMIN	Necesario para garantizar que la base de datos de vCenter Server sea utilizada por una sola instancia de vCenter Server.
GRANT EXECUTE ON dbms_job TO VPXADMIN	Necesario durante la instalación o actualización para la programación y administración de trabajos de SQL. Este permiso no se requiere después de la implementación.
GRANT SELECT ON dba_lock TO VPXADMIN	Necesario para determinar los bloqueos existentes en la base de datos de vCenter Server.
GRANT SELECT ON dba_tablespaces TO VPXADMIN	Necesario durante la actualización para determinar el espacio en disco requerido. Este permiso no se requiere después de la implementación.
GRANT SELECT ON dba_temp_files TO VPXADMIN	Necesario durante la actualización para determinar el espacio en disco requerido. Este permiso no se requiere después de la implementación.
GRANT SELECT ON dba_data_files TO VPXADMIN	Necesario para la supervisión del espacio libre mientras está funcionando vCenter Server.
GRANT SELECT ON v_\$session TO VPXADMIN	Vista utilizada para determinar los bloqueos existentes en la base de datos de vCenter Server.
GRANT UNLIMITED TABLESPACE TO VPXADMIN	Necesario para conceder permisos de espacio de tabla ilimitados al usuario de la base de datos de vCenter Server.
GRANT SELECT ON v_\$system_event TO VPXADMIN	Necesario para comprobar los cambios del archivo de registro.
GRANT SELECT ON v_\$sysmetric_history TO VPXADMIN	Necesario para comprobar la utilización de la CPU.

Tabla 7-3. Permisos de base de datos de Oracle para vCenter Server (continuación)

Permiso	Descripción
GRANT SELECT ON v_\$sysstat TO VPXADMIN	Necesario para determinar la frecuencia de aciertos de memoria caché del búfer.
GRANT SELECT ON dba_data_files TO VPXADMIN	Necesario para determinar la utilización del espacio de tabla.
GRANT SELECT ON v_\$loghist TO VPXADMIN	Necesario para comprobar la frecuencia del punto de comprobación.

Los privilegios de la base de datos maestra se utilizan para supervisar la base de datos de vCenter Server. Por lo tanto, si se alcanza un umbral determinado, podrá observar una alerta.

Comprobar que vCenter Server puede comunicarse con la base de datos local

Si la base de datos se encuentra en el mismo equipo en el que se va a instalar vCenter Server y se modificó el nombre del equipo, compruebe la configuración. Asegúrese de que el DSN de vCenter Server esté configurado para comunicarse con el nuevo nombre del equipo.

El cambio de nombre del equipo de vCenter Server repercute en la comunicación con la base de datos si el servidor de bases de datos se encuentra en el mismo equipo de vCenter Server. Si modificó el nombre del equipo, puede comprobar que la comunicación permanezca intacta.

Si la base de datos es remota, puede omitir este procedimiento. El cambio de nombre no afecta a la comunicación con las bases de datos remotas.

Después de cambiar el nombre del servidor, compruebe con el administrador o el proveedor de bases de datos que todos los componentes estén en funcionamiento.

Requisitos previos

- Asegúrese de que el servidor de bases de datos se esté ejecutando.
- Asegúrese de que el nombre del equipo vCenter Server esté actualizado en el servicio de nombres de dominio (DNS).

Procedimiento

- 1 Actualice la información del origen de datos, según sea necesario.
- 2 Haga ping al nombre del equipo para probar esta conexión.

Por ejemplo, si el nombre de equipo es `host-1.company.com`, ejecute el siguiente comando en el símbolo del sistema de Windows:

```
ping host-1.company.com
```

Si puede hacer ping al nombre de equipo, el nombre se actualiza en DNS.

Resultados

Se confirma la comunicación con vCenter Server. Puede continuar con la preparación de otros componentes del entorno.

Mantener una base de datos de vCenter Server

Una vez que la instancia de base de datos de vCenter Server y vCenter Server están instalados y funcionan correctamente, realice procesos de mantenimiento de base de datos estándar.

Los procesos de mantenimiento de la base de datos incluyen las siguientes tareas:

- Supervisión del crecimiento del archivo de registro y compactación del archivo de registro de la base de datos, según sea necesario.
- Programación de copias de seguridad regulares de la base de datos.
- Creación de copias de seguridad de la base de datos antes de actualizar vCenter Server.

Consulte la documentación de su proveedor de base de datos para conocer los procedimientos de mantenimiento específicos y obtener asistencia.

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.

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.

Configurar el usuario administrador de vCenter Server

La forma en que se configure el administrador de vCenter Server depende de la implementación de vCenter Single Sign-On que se haya hecho.

En las versiones de vSphere anteriores a vSphere 5.1, los administradores de vCenter Server son los usuarios que pertenecen al grupo de administradores del sistema operativo local.

En vSphere 5.1.x, 5.5 y 6.0, cuando instale vCenter Server, deberá proporcionar el grupo de administradores o el usuario administrador predeterminado (inicial) de vCenter Server. Para implementaciones en las que vCenter Server y vCenter Single Sign-On se encuentran en la misma máquina virtual o el mismo servidor físico, puede designar el grupo Administradores del sistema operativo local como usuarios administrativos para vCenter Server. Esta es la opción predeterminada. Este comportamiento permanece sin modificaciones desde vCenter Server 5.0.

Para instalaciones de mayor tamaño, en donde vCenter Single Sign-On forma parte de Platform Services Controller y se implementan instancias de vCenter Server en diferentes máquinas virtuales o servidores físicos, no se puede mantener el mismo comportamiento que en vCenter Server 5.0. En su lugar, asigne la función de administrador de vCenter Server a un usuario o un grupo desde un origen de identidad registrado en el servidor vCenter Single Sign-On: Active Directory, OpenLDAP o el origen de identidad del sistema.

Autenticar con el entorno de vCenter Server

En vCenter Server versiones 5.1 y posteriores, los usuarios realizan la autenticación a través de vCenter Single Sign-On.

En las versiones de vCenter Server anteriores a vCenter Server 5.1, cuando un usuario se conecta con vCenter Server, vCenter Server realiza la autenticación del usuario a través de la validación del usuario frente a un dominio de Active Directory o la lista de usuarios locales del sistema operativo.

El usuario `administrator@your_domain_name` tiene privilegios de administrador para vCenter Single Sign-On de manera predeterminada. Cuando inicia sesión en el servidor vCenter Single Sign-On desde vSphere Web Client, el usuario `administrator@your_domain_name` puede asignar privilegios de administrador para vCenter Single Sign-On a otros usuarios. Estos usuarios podrían ser distintos de los otros usuarios que administran vCenter Server.

Los usuarios pueden iniciar sesión en vCenter Server con vSphere Web Client. Los usuarios se autentican con vCenter Single Sign-On. Los usuarios pueden ver todas las instancias de vCenter Server en las que el usuario tenga permisos. Después de que los usuarios se conectan a vCenter Server, no se requieren más autenticaciones. Las acciones que los usuarios pueden realizar en los objetos dependen de los permisos para vCenter Server que tengan en esos objetos.

Para obtener más información acerca de vCenter Single Sign-On, consulte *Seguridad de vSphere*.

Cómo vCenter Single Sign-On afecta el comportamiento de inicio de sesión

El comportamiento de inicio de sesión de vCenter Single Sign-On depende del dominio al que pertenece el usuario y los orígenes de identidad que agregó a vCenter Single Sign-On.

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.

vCenter Single Sign-On no propaga permisos para autenticar dicho resultado de los grupos anidados de orígenes de identidad disímiles. Por ejemplo, si agrega el grupo Administradores de dominio al grupo Administradores locales, los permisos no se propagan debido a que el sistema operativo local y Active Directory son orígenes de identidad por separado.

Después de la instalación en un sistema Windows, el usuario `administrator@your_domain_name` posee privilegios de administrador en el servidor de vCenter Single Sign-On y el sistema vCenter Server.

Después de implementar vCenter Server Appliance, el usuario `administrator@your_domain_name` posee privilegios de administrador en el servidor de vCenter Single Sign-On y el sistema vCenter Server.

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 **localos** 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.

Para obtener más información acerca de vCenter Single Sign-On, consulte *Seguridad de vSphere*.

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.

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.

Usar una cuenta de usuario para ejecutar vCenter Server

Puede utilizar la cuenta del sistema integrada de Microsoft Windows o una cuenta de usuario para ejecutar vCenter Server. Con una cuenta de usuario, puede habilitar la autenticación de Windows para SQL Server, y esto proporciona más seguridad.

La cuenta de usuario debe ser un administrador en la máquina local. En el asistente de instalación, especifique el nombre de la cuenta como *DomainName\Username*. Deberá configurar la base de datos de SQL Server para permitir el acceso de la cuenta de dominio a SQL Server.

La cuenta del sistema integrada de Microsoft Windows posee más permisos y derechos en el servidor que los que el sistema vCenter Server necesita, lo que podría representar problemas de seguridad.

Importante Si el servicio vCenter Server está en ejecución en la cuenta del sistema integrada de Microsoft Windows, al utilizar Microsoft SQL Server, vCenter Server 6.0 solo admite DSN con autenticación de SQL Server.

Para DNS de SQL Server configurados con autenticación de Windows, utilice la misma cuenta de usuario para el servicio VMware VirtualCenter Management Webservices y el usuario de DSN.

Si no tiene pensado utilizar la autenticación de Microsoft Windows para SQL Server o si va a utilizar una base de datos de Oracle, es posible que aún desee configurar una cuenta de usuario local para el sistema vCenter Server. El único requisito es que la cuenta de usuario sea un administrador en la máquina local y la cuenta debe tener concedido el privilegio **Iniciar sesión como servicio**.

Instalar vCenter Server en máquinas IPv6

Desde vSphere 6.0, vCenter Server admite conexión entre componentes de vCenter Server y vCenter Server mediante direcciones IPv4 o IPv6.

No se admite un entorno mixto de IPv4 y IPv6. Cuando instale vCenter Server en un entorno IPv6, use el nombre de dominio completo (FQDN) o el nombre de host de la máquina en la que instale vCenter Server. Para un entorno IPv4 puro, la práctica recomendada es utilizar el nombre de dominio completo (FQDN) o el nombre de host de la máquina en la que instale vCenter Server, ya que la dirección IP puede cambiar si la asigna DHCP.

Ejecutar el instalador de vCenter Server desde una unidad de red

Puede ejecutar el instalador de vCenter Server desde una unidad de red, pero no puede instalar el software en una unidad de red.

En Windows, puede ejecutar los instaladores desde la unidad de red e instalar el software en la máquina local.

Información obligatoria para instalar vCenter Server

Al instalar vCenter Server con una instancia de Platform Services Controller integrada o externa, el asistente para instalación solicita la información de instalación.

Información requerida para la instalación de vCenter Server con una instancia de Platform Services Controller integrada

El asistente de instalación de vCenter Server le solicita información de la instalación. Se recomienda mantener un registro de los valores introducidos por si debe reinstalar el producto.

Puede utilizar esta hoja de cálculo para registrar la información que necesita para la instalación de vCenter Server con una instancia de Platform Services Controller integrada.

Tabla 7-4. Información requerida para la instalación de vCenter Server con una instancia de Platform Services Controller integrada

Información necesaria		Predeterminado	Su entrada
Nombre del sistema local.			
El nombre de sistema que se va a utilizar para administrar el sistema local. El nombre de sistema debe ser un FQDN. Si no hay un DSN disponible, proporcione una dirección IP estática.			
Nuevo dominio de vCenter	Nombre de dominio	vsphere.local	
Single Sign-On.	Nombre de usuario	administrator	No puede modificar el nombre de usuario predeterminado durante la instalación.

Tabla 7-4. Información requerida para la instalación de vCenter Server con una instancia de Platform Services Controller integrada (continuación)

Información necesaria		Predeterminado	Su entrada
	Contraseña de la cuenta del administrador de sistema vCenter Single Sign-On. La contraseña debe contener al menos 8 caracteres y no más de 20. Esta debe cumplir los siguientes requisitos:		
	■ Debe contener al menos una letra mayúscula.		
	■ Debe contener al menos una letra minúscula.		
	■ Debe contener al menos un número.		
	■ Debe contener al menos un carácter especial, como una y comercial (&), una almohadilla (#) y el signo de porcentaje (%).		
	Nombre del sitio.		
	Un nombre para el sitio de vCenter Single Sign-On.		
Unirse a un dominio de vCenter Single Sign-On.	FQDN o dirección IP de Platform Services Controller.		
	Puerto HTTPS para comunicarse con un dominio de vCenter Single Sign-On existente	443	
	Contraseña de la cuenta del administrador de sistema vCenter Single Sign-On.		
	Únase a un sitio existente o cree un sitio nuevo.	Nombre del sitio al que se va a unir o nombre del nuevo sitio.	
Información de la cuenta del servicio de vCenter Server. Puede ser la cuenta del sistema de Windows o una cuenta especificada por el usuario.	Nombre de usuario de la cuenta		
	Se requiere si utiliza una cuenta de servicio de usuario.		
	Contraseña de la cuenta		
	Se requiere si utiliza una cuenta de servicio de usuario.		
Nombre de origen de datos (DSN).			
Se requiere si tiene pensado utilizar una base de datos externa existente.			
No se requiere si tiene pensado utilizar la base de datos PostgreSQL integrada. No se admiten los espacios iniciales y finales. Elimine los espacios al principio y al final del DSN.			
Nombre de usuario de la base de datos.	Se requiere si tiene pensado utilizar una base de datos existente. No es necesario si tiene planificado usar una base de datos de PostgreSQL en paquete.		
	No se admiten caracteres que no sean de ASCII.		
Contraseña de la base de datos.			

Tabla 7-4. Información requerida para la instalación de vCenter Server con una instancia de Platform Services Controller integrada (continuación)

Información necesaria	Predeterminado	Su entrada
Puerto HTTP.	80	
Puerto HTTPS.	443	
Puerto del servicio de Syslog.	514	
Puerto TLS del servicio de Syslog.	1514	
Puerto del servicio de token de seguridad.	7444	
Puerto de administración de Auto Deploy.	6502	
Puerto de servicio de Auto Deploy.	6501	
puerto de ESXi Dump Collector.	6500	
Puerto de latido de ESXi.	902	
Puerto de vSphere Web Client.	9443	
<p>Carpeta de destino.</p> <ul style="list-style-type: none"> ■ La carpeta en la que desea instalar vCenter Server. ■ La carpeta en la que desea almacenar los datos de vCenter Server con una instancia de Platform Services Controller integrada. <p>Las rutas de instalación no pueden contener caracteres que no sean ASCII, comas (,), puntos (.), signos de exclamación (!), numerales (#), arrobas (@) ni signos de porcentaje (%).</p>	<ul style="list-style-type: none"> ■ La carpeta de instalación predeterminada es C:\Archivos de programa\VMware. ■ La carpeta predeterminada para almacenamiento de datos es C:\ProgramData\VMware. 	
<p>Unirse o no al Programa de mejora de la experiencia del cliente (CEIP) de VMware.</p> <p>Para obtener más información sobre el CEIP, consulte la sección Configuración del Programa de mejora de la experiencia del cliente en <i>Administración de vCenter Server y hosts</i>.</p>	Unirse al CEIP	

Información obligatoria para instalar Platform Services Controller

Cuando instale vCenter Server con una instancia de Platform Services Controller externa, el asistente de instalación de Platform Services Controller le solicitará la información de instalación.

Se recomienda mantener un registro de los valores introducidos por si debe reinstalar el producto.

Puede usar esta hoja de cálculo para registrar la información que necesita para la instalación de una instancia de Platform Services Controller externa.

Tabla 7-5. Información obligatoria para instalar Platform Services Controller

Información necesaria		Predeterminado	Su entrada
Nombre del sistema local. El nombre de sistema que se va a utilizar para administrar el sistema local. El nombre de sistema debe ser un FQDN. Si no hay un DSN disponible, proporcione una dirección IP estática.			
Nuevo dominio de vCenter Single Sign-On.	Nombre de dominio	vsphere.local	
	Nombre de usuario	administrator	No puede modificar el nombre de usuario predeterminado durante la instalación.
	Contraseña de la cuenta del administrador de sistema vCenter Single Sign-On. La contraseña debe contener al menos 8 caracteres y no más de 20. Esta debe cumplir los siguientes requisitos:		
	<ul style="list-style-type: none"> ■ Debe contener al menos una letra mayúscula. ■ Debe contener al menos una letra minúscula. ■ Debe contener al menos un número. ■ Debe contener al menos un carácter especial, como una y comercial (&), una almohadilla (#) y el signo de porcentaje (%). 		
Nombre del sitio. Un nombre para el sitio de vCenter Single Sign-On.			
Unirse a un dominio de vCenter Single Sign-On.	FQDN o dirección IP de Platform Services Controller		
	Puerto HTTPS para comunicarse con un dominio de vCenter Single Sign-On existente	443	
	Contraseña de la cuenta del administrador de sistema vCenter Single Sign-On.		
	Unirse a un sitio existente o crear un nuevo sitio	Nombre del sitio al que se va a unir o nombre del nuevo sitio.	
Puerto HTTP.		80	
Puerto HTTPS.		443	
Puerto del servicio de Syslog.		514	
Puerto TLS del servicio de Syslog.		1514	

Tabla 7-5. Información obligatoria para instalar Platform Services Controller (continuación)

Información necesaria	Predeterminado	Su entrada
Puerto del servicio de token de seguridad.	7444	
<p>Carpeta de destino.</p> <ul style="list-style-type: none"> ■ La carpeta en la que se va a instalar Platform Services Controller. ■ La carpeta en la que se van a almacenar los datos de Platform Services Controller. <p>Las rutas de instalación no pueden contener caracteres que no sean ASCII, comas (,), puntos (.), signos de exclamación (!), numerales (#), arrobas (@) ni signos de porcentaje (%).</p>	<ul style="list-style-type: none"> ■ La carpeta de instalación predeterminada es C:\Archivos de programa\VMware. ■ La carpeta predeterminada para almacenamiento de datos es C:\ProgramData\VMware. 	
<p>Unirse o no al Programa de mejora de la experiencia del cliente (CEIP) de VMware.</p> <p>Para obtener más información sobre el CEIP, consulte la sección Configuración del Programa de mejora de la experiencia del cliente en <i>Administración de vCenter Server y hosts</i>.</p>	Unirse al CEIP	

Información obligatoria para instalar vCenter Server

Cuando instale vCenter Server con una instancia de Platform Services Controller externa, el asistente de instalación de vCenter Server le solicitará la información de instalación. Se recomienda mantener un registro de los valores que haya introducido en caso de que sea necesario reinstalar el producto.

Puede utilizar esta hoja de cálculo para registrar la información que necesita para la instalación de vCenter Server con una instancia de Platform Services Controller externa.

Tabla 7-6. Información requerida para la instalación de vCenter Server con una instancia de Platform Services Controller externa

Información necesaria	Valor predeterminado	Su entrada
<p>Nombre del sistema local.</p> <p>El nombre de sistema que se va a utilizar para administrar el sistema local. El nombre de sistema debe ser un FQDN. Si no hay un DSN disponible, proporcione una dirección IP estática.</p>		
<p>Información de Single Sign-On.</p>	FQDN o dirección IP de Platform Services Controller.	

Tabla 7-6. Información requerida para la instalación de vCenter Server con una instancia de Platform Services Controller externa (continuación)

Información necesaria	Valor predeterminado	Su entrada
Puerto HTTPS de Single Sign-On.	443	
Nombre de usuario de Single Sign-On.		
Contraseña de usuario de Single Sign-On.		
Información de la cuenta del servicio de vCenter Server.	Nombre de usuario de la cuenta Se requiere si utiliza una cuenta de servicio de usuario.	
Puede ser la cuenta del sistema de Windows o una cuenta especificada por el usuario.	Contraseña de la cuenta Se requiere si utiliza una cuenta de servicio de usuario.	
Nombre de origen de datos (DSN). Se requiere si utiliza una base de datos externa existente. No es necesario si va a usar una base de datos de PostgreSQL en paquete. No se admiten los espacios iniciales y finales. Elimine los espacios al principio y al final del DSN.		
Nombre de usuario de la base de datos.	Se requiere si tiene pensado utilizar una base de datos existente. No es necesario si tiene planificado usar una base de datos de PostgreSQL en paquete. No se admiten caracteres que no sean de ASCII.	
Contraseña de la base de datos.		
Puerto HTTP.	80	
Puerto HTTPS.	443	
Puerto del servicio de Syslog.	514	
Puerto TLS del servicio de Syslog.	1514	
Puerto de administración de Auto Deploy.	6502	
Puerto de servicio de Auto Deploy.	6501	
puerto de ESXi Dump Collector.	6500	
Puerto de latido de ESXi.	902	

Tabla 7-6. Información requerida para la instalación de vCenter Server con una instancia de Platform Services Controller externa (continuación)

Información necesaria	Valor predeterminado	Su entrada
Puerto de vSphere Web Client.	9443	
<p>Carpetas de destino.</p> <ul style="list-style-type: none"> ■ La carpeta en la que desea instalar vCenter Server. ■ La carpeta en la que almacenar los datos de vCenter Server con una instancia de Platform Services Controller externa. <p>Las rutas de instalación no pueden contener caracteres que no sean ASCII, comas (,), puntos (.), signos de exclamación (!), numerales (#), arrobas (@) ni signos de porcentaje (%).</p>	<ul style="list-style-type: none"> ■ La carpeta de instalación predeterminada es <code>C:\Archivos de programa\VMware</code>. ■ La carpeta predeterminada para almacenamiento de datos es <code>C:\ProgramData\VMware</code>. 	

Información necesaria para la implementación de vCenter Server Appliance

Cuando se implementa vCenter Server Appliance con una instancia de Platform Services Controller integrada o externa, el asistente de instalación solicita la información de la implementación.

Información necesaria para la implementación de vCenter Server Appliance con una instancia de Platform Services Controller integrada

El asistente de implementación de vCenter Server Appliance solicita la información de la implementación. Se recomienda mantener un registro de los valores introducidos por si debe reinstalar el producto.

Puede usar esta hoja de trabajo si desea registrar la información necesaria para implementar vCenter Server Appliance con una instancia de Platform Services Controller integrada.

Tabla 7-7. Información necesaria para la implementación de vCenter Server Appliance con una instancia de Platform Services Controller integrada

Información necesaria		Predeterminado	Su entrada
FQDN o IP del host ESXi o de la instancia de vCenter Server en la cual se implementa vCenter Server Appliance.			
<ul style="list-style-type: none"> ■ Si se utiliza el FQDN o la IP de un host ESXi, el asistente solicita un nombre de usuario y una contraseña con privilegios administrativos para el host ESXi. ■ Si se utiliza el FQDN o la IP de una instancia de vCenter Server, el asistente solicita un nombre de usuario y una contraseña con privilegios administrativos para la instancia de vCenter Server, el centro de datos o la carpeta del centro de datos y el grupo de recursos de un host ESXi o un clúster de DRS en el cual se desea implementar el dispositivo. 			
Nombre de vCenter Server Appliance		Ejemplo: Muestra-Dispositivo-Nombre	
<p>Contraseña del usuario raíz del sistema operativo de vCenter Server Appliance.</p> <p>La contraseña debe contener al menos 8 caracteres y no más de 20.</p> <p>Esta debe cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> ■ Debe contener al menos una letra mayúscula. ■ Debe contener al menos una letra minúscula. ■ Debe contener al menos un número. ■ Debe contener al menos un carácter especial, por ejemplo, un signo de dólar (\$), numeral (#), arroba (@), punto (.) o signo de exclamación (!). 			
Nuevo dominio de Single Sign-On.	Nombre de dominio	vsphere.local	
	Nombre de usuario	administrator	No puede modificar el nombre de usuario predeterminado durante la instalación.

Tabla 7-7. Información necesaria para la implementación de vCenter Server Appliance con una instancia de Platform Services Controller integrada (continuación)

Información necesaria	Predeterminado	Su entrada
<p>Contraseña de la cuenta del administrador de sistema vCenter Single Sign-On.</p> <p>La contraseña debe contener al menos 8 caracteres y no más de 20.</p> <p>Esta debe cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> ■ Debe contener al menos una letra mayúscula. ■ Debe contener al menos una letra minúscula. ■ Debe contener al menos un número. ■ Debe contener al menos un carácter especial, como una y comercial (&), una almohadilla (#) y el signo de porcentaje (%). 		
<p>Nombre del sitio.</p> <p>Un nombre para el sitio de vCenter Single Sign-On.</p>		
Unirse a un dominio de Single Sign-On.	FQDN o dirección IP de Platform Services Controller.	
	Contraseña de la cuenta del administrador de sistema vCenter Single Sign-On.	
	Número de puerto	443
	Nombre del sitio	
<p>Tamaño de vCenter Server Appliance.</p> <p>Las opciones pueden variar en función del tamaño del entorno de vSphere:</p> <ul style="list-style-type: none"> ■ Muy pequeño (máximo de 10 hosts y 100 máquinas virtuales) ■ Pequeño (máximo de 100 hosts y 1.000 máquinas virtuales) ■ Mediano (máximo de 400 hosts y 4.000 máquinas virtuales) ■ Grande (máximo de 1.000 hosts y 10.000 máquinas virtuales) 		Muy pequeño (máximo de 10 hosts y 100 máquinas virtuales)
Nombre del almacén de datos en el cual se implementa vCenter Server Appliance.		

Tabla 7-7. Información necesaria para la implementación de vCenter Server Appliance con una instancia de Platform Services Controller integrada (continuación)

Información necesaria		Predeterminado	Su entrada
Habilitar o deshabilitar el modo de discos delgados.		Deshabilitado como opción predeterminada	
Servidor de bases de datos de Oracle.	Es necesario si tiene planificado usar una base de datos de Oracle existente. No es necesario si tiene planificado usar una base de datos de PostgreSQL en paquete. No se admiten caracteres que no sean de ASCII.		
Puerto de base de datos de Oracle.			
Nombre de la instancia de la base de datos de Oracle.			
Nombre de usuario de la base de datos.			
Contraseña de la base de datos.			
Nombre de la red.			
Asignación de direcciones IP. Puede ser IPv4 o IPv6.		IPv4	
Tipo de red. Puede ser DHCP o estática para IPv4; y DHCP o estática para IPv6.		DHCP	
Dirección IPv4 asignada por la configuración de DHCP.	FQDN Si no hay ningún DNS habilitado en el entorno, deje el cuadro de texto FQDN en blanco.		
	Habilite o deshabilite SSH.	Deshabilitado como opción predeterminada	
Configuración de asignación estática de IPv4.	Dirección de red.		
	Nombre del sistema (FQDN o dirección IP). El nombre de sistema que se va a utilizar para administrar el sistema local. El nombre del sistema debe ser FQDN. Si el valor de DNS no está disponible, proporcione una dirección IP estática.		
	Máscara de subred.		
	Puerta de enlace de red.		

Tabla 7-7. Información necesaria para la implementación de vCenter Server Appliance con una instancia de Platform Services Controller integrada (continuación)

Información necesaria	Predeterminado	Su entrada
	Servidores DNS de red, separados por comas.	
	Habilite o deshabilite SSH.	Deshabilitado como opción predeterminada
Dirección IPv6 asignada por la configuración de DHCP	FQDN Si no hay ningún DNS habilitado en el entorno, deje el cuadro de texto FQDN en blanco.	
	Habilitar o deshabilitar SSH	Deshabilitado como opción predeterminada
Configuración de asignación estática de IPv6.	FQDN	
	Dirección de red.	
	Prefijo de red.	
	Puerta de enlace de red.	
	Servidores DNS de red, separados por comas.	
	Habilite o deshabilite SSH.	Deshabilitado como opción predeterminada
Configuración de sincronización de la hora. Puede sincronizar la hora de la aplicación con la hora del host ESXi o usar servidores NTP.	Nombres de los servidores NTP, separados por comas. Es necesario para usar servidores NTP para la sincronización de la hora.	
Unirse o no al Programa de mejora de la experiencia del cliente (CEIP) de VMware. Para obtener más información sobre el CEIP, consulte la sección Configuración del Programa de mejora de la experiencia del cliente en <i>Administración de vCenter Server y hosts</i> .		Unirse al CEIP

Información necesaria para la implementación de Platform Services Controller Appliance

El asistente de implementación de Platform Services Controller solicita la información de la implementación. Se recomienda mantener un registro de los valores introducidos por si debe reinstalar el producto.

Puede usar esta hoja de trabajo para registrar la información necesaria para implementar un dispositivo Platform Services Controller externo.

Tabla 7-8. Información necesaria para la implementación de un dispositivo Platform Services Controller externo

Información necesaria	Valor predeterminado	Su entrada
<p>FQDN o IP del host ESXi o de la instancia de vCenter Server en la cual se implementa el dispositivo Platform Services Controller.</p> <ul style="list-style-type: none"> ■ Si se utiliza el FQDN o la IP de un host ESXi, el asistente solicita un nombre de usuario y una contraseña con privilegios administrativos para el host ESXi. ■ Si se utiliza el FQDN o la IP de una instancia de vCenter Server, el asistente solicita un nombre de usuario y una contraseña con privilegios administrativos para la instancia de vCenter Server, el centro de datos o la carpeta del centro de datos y el grupo de recursos de un host ESXi o un clúster de DRS en el cual se desea implementar el dispositivo. 		
Nombre de la aplicación Platform Services Controller	Ejemplo: Muestra-Dispositivo-Nombre	
<p>Contraseña del usuario raíz del sistema operativo de vCenter Server Appliance.</p> <p>La contraseña debe contener al menos 8 caracteres y no más de 20.</p> <p>Esta debe cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> ■ Debe contener al menos una letra mayúscula. ■ Debe contener al menos una letra minúscula. ■ Debe contener al menos un número. ■ Debe contener al menos un carácter especial, por ejemplo, un signo de dólar (\$), numeral (#), arroba (@), punto (.) o signo de exclamación (!). 		
Nuevo dominio de Single Sign-On.	Nombre de dominio	vsphere.local

Tabla 7-8. Información necesaria para la implementación de un dispositivo Platform Services Controller externo (continuación)

Información necesaria	Valor predeterminado	Su entrada
<p>Contraseña de la cuenta del administrador de sistema vCenter Single Sign-On.</p> <p>La contraseña debe contener al menos 8 caracteres y no más de 20.</p> <p>Esta debe cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> ■ Debe contener al menos una letra mayúscula. ■ Debe contener al menos una letra minúscula. ■ Debe contener al menos un número. ■ Debe contener al menos un carácter especial, como una Y comercial (&), una almohadilla (#) y el signo de porcentaje (%). 		
	<p>Nombre del sitio.</p> <p>Un nombre para el sitio de vCenter Single Sign-On.</p>	
Unirse a un dominio de Single Sign-On.	Platform Services Controller FQDN o dirección IP	
	Contraseña de la cuenta del administrador de sistema vCenter Single Sign-On.	
	Número de puerto	443
	Nombre del sitio	
Tamaño de la aplicación Platform Services Controller.	Platform Services Controller	No es posible cambiar la opción predeterminada. La aplicación virtual que se implemente tendrá 2 CPU y 2 GB de memoria.
Nombre del almacén de datos en el cual se implementa la aplicación Platform Services Controller.		
Habilitar o deshabilitar el modo de discos delgados.	Deshabilitado como opción predeterminada	
Nombre de la red.		
Asignación de direcciones IP. Puede ser IPv4 o IPv6.	IPv4	

Tabla 7-8. Información necesaria para la implementación de un dispositivo Platform Services Controller externo (continuación)

Información necesaria		Valor predeterminado	Su entrada
Tipo de red. Puede ser DHCP o estática para IPv4; y DHCP o estática para IPv6.		DHCP	
Dirección IPv4 asignada por la configuración de DHCP	FQDN Si no hay ningún DDNS habilitado en el entorno, deje el cuadro de texto FQDN en blanco.		
	Habilite o deshabilite SSH.	Deshabilitado como opción predeterminada	
Configuración de asignación estática de IPv4.	Dirección de red.		
	Nombre del sistema (FQDN o dirección IP). El nombre de sistema que se va a utilizar para administrar el sistema local. El nombre del sistema debe ser FQDN. Si el valor de DNS no está disponible, proporcione una dirección IP estática.		
	Máscara de subred.		
	Puerta de enlace de red.		
	Servidores DNS de red, separados por comas.		
	Habilite o deshabilite SSH.	Deshabilitado como opción predeterminada	
Dirección IPv6 asignada por la configuración de DHCP	FQDN Si no ha habilitado DNS, deje el cuadro de texto FQDN en blanco.		
	Habilitar o deshabilitar SSH	Deshabilitado como opción predeterminada	
Configuración de asignación estática de IPv6.	FQDN		
	Dirección de red.		
	Prefijo de red.		
	Puerta de enlace de red.		

Tabla 7-8. Información necesaria para la implementación de un dispositivo Platform Services Controller externo (continuación)

Información necesaria		Valor predeterminado	Su entrada
	Servidores DNS de red, separados por comas.		
	Habilite o deshabilite SSH.	Deshabilitado como opción predeterminada	
Configuración de sincronización de la hora. Puede sincronizar la hora de la aplicación con la hora del host ESXi o usar servidores NTP.	Nombres de los servidores NTP, separados por comas. Es necesario para usar servidores NTP para la sincronización de la hora.		
Unirse o no al Programa de mejora de la experiencia del cliente (CEIP) de VMware. Para obtener más información sobre el CEIP, consulte la sección Configuración del Programa de mejora de la experiencia del cliente en <i>Administración de vCenter Server y hosts</i> .		Unirse al CEIP	

Información necesaria para la implementación de vCenter Server Appliance

El asistente de implementación de vCenter Server Appliance solicita la información de la implementación. Se recomienda mantener un registro de los valores introducidos por si debe reinstalar el producto.

Puede usar esta hoja de trabajo para registrar la información necesaria a fin de implementar un vCenter Server Appliance con un Platform Services Controller externo.

Tabla 7-9. Información necesaria para la implementación de vCenter Server Appliance

Información necesaria	Valor predeterminado	Su entrada
<p>FQDN o IP del host ESXi o de la instancia de vCenter Server en la cual se implementa vCenter Server Appliance.</p> <ul style="list-style-type: none"> ■ Si se utiliza el FQDN o la IP de un host ESXi, el asistente solicita un nombre de usuario y una contraseña con privilegios administrativos para el host ESXi. ■ Si se utiliza el FQDN o la IP de una instancia de vCenter Server, el asistente solicita un nombre de usuario y una contraseña con privilegios administrativos para la instancia de vCenter Server, el centro de datos o la carpeta del centro de datos y el grupo de recursos de un host ESXi o un clúster de DRS en el cual se desea implementar el dispositivo. 		
Nombre de vCenter Server Appliance	Ejemplo: Muestra-Dispositivo-Nombre	
<p>Contraseña del usuario raíz del sistema operativo de vCenter Server Appliance.</p> <p>La contraseña debe contener al menos 8 caracteres y no más de 20.</p> <p>Esta debe cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> ■ Debe contener al menos una letra mayúscula. ■ Debe contener al menos una letra minúscula. ■ Debe contener al menos un número. ■ Debe contener al menos un carácter especial, por ejemplo, un signo de dólar (\$), numeral (#), arroba (@), punto (.) o signo de exclamación (!). 		
<p>FQDN o dirección IP de Platform Services Controller.</p> <p>Debe proporcionar un valor de FQDN o dirección IP de un Platform Services Controller que ya haya instalado o implementado.</p>		
Contraseña de administrador de vCenter Single Sign-On.		
Puerto HTTPS de vCenter Single Sign-On.	443	
<p>Tamaño de vCenter Server Appliance.</p> <p>Las opciones pueden variar en función del tamaño del entorno vSphere.</p> <ul style="list-style-type: none"> ■ Muy pequeño (máximo de 10 hosts y 100 máquinas virtuales) ■ Pequeño (máximo de 100 hosts y 1.000 máquinas virtuales) ■ Mediano (máximo de 400 hosts y 4.000 máquinas virtuales) ■ Grande (máximo de 1.000 hosts y 10.000 máquinas virtuales) 		
	Muy pequeño (máximo de 10 hosts y 100 máquinas virtuales)	

Tabla 7-9. Información necesaria para la implementación de vCenter Server Appliance (continuación)

Información necesaria		Valor predeterminado	Su entrada
Nombre del almacén de datos en el cual se implementa vCenter Server Appliance.			
Habilitar o deshabilitar el modo de discos delgados.		Deshabilitado como opción predeterminada	
Servidor de bases de datos de Oracle.	Solamente es necesario si tiene planificado usar una base de datos existente de Oracle. No es necesario si va a usar una base de datos de PostgreSQL en paquete. No se admiten caracteres que no sean de ASCII.		
Puerto de base de datos de Oracle.			
Nombre de la instancia de la base de datos de Oracle.			
Nombre de usuario de la base de datos.			
Contraseña de la base de datos.			
Nombre de la red.			
Asignación de direcciones IP. Puede ser IPv4 o IPv6.		IPv4	
Tipo de red. Puede ser DHCP o estática para IPv4; y DHCP o estática para IPv6.		DHCP	
Dirección IPv4 asignada por la configuración de DHCP	FQDN Si no hay ningún DNS habilitado en el entorno, deje el cuadro de texto FQDN en blanco.		
	Habilite o deshabilite SSH.	Deshabilitado como opción predeterminada	
Configuración de asignación estática de IPv4.	Dirección de red.		
	Nombre del sistema (FQDN o dirección IP). El nombre de sistema que se va a utilizar para administrar el sistema local. El nombre del sistema debe ser FQDN. Si el valor de DNS no está disponible, proporcione una dirección IP estática.		
	Máscara de subred.		

Tabla 7-9. Información necesaria para la implementación de vCenter Server Appliance (continuación)

Información necesaria		Valor predeterminado	Su entrada
	Puerta de enlace de red.		
	Servidores DNS de red, separados por comas.		
	Habilite o deshabilite SSH.	Deshabilitado como opción predeterminada	
Dirección IPv6 asignada por la configuración de DHCP	FQDN Si no hay ningún DNS habilitado en el entorno, deje el cuadro de texto FQDN en blanco.		
	Habilitar o deshabilitar SSH	Deshabilitado como opción predeterminada	
Configuración de asignación estática de IPv6.	FQDN		
	Dirección de red.		
	Prefijo de red.		
	Puerta de enlace de red.		
	Servidores DNS de red, separados por comas.		
	Habilite o deshabilite SSH.	Deshabilitado como opción predeterminada	
Configuración de sincronización de la hora. Puede sincronizar la hora de la aplicación con la hora del host ESXi o usar servidores NTP.	Nombres de los servidores NTP, separados por comas. Es necesario para usar servidores NTP para la sincronización de la hora.		

Instalar vCenter Server en un servidor físico o una máquina virtual de Windows

8

Puede instalar vCenter Server en una máquina virtual o un servidor físico de Microsoft Windows para administrar el entorno de vSphere.

Antes de instalar vCenter Server, descargue el archivo ISO y móntelo en el equipo host Windows desde el cual desea realizar la implementación y, a continuación, inicie el asistente de instalación.

Para obtener información sobre los requisitos de vCenter Server, consulte [Requisitos de vCenter Server para Windows](#).

Para obtener información sobre las entradas requeridas durante la instalación de vCenter Server, consulte [Información obligatoria para instalar vCenter Server](#).

Después de instalar vCenter Server, solo el usuario `administrator@your_domain_name` tiene privilegios para iniciar sesión en el sistema vCenter Server.

El usuario `administrator@your_domain_name` puede realizar las siguientes tareas:

- Agregar un origen de identidad en el que los usuarios y grupos adicionales se definen en vCenter Single Sign-On.
- Asignar roles a usuarios y grupos para concederles privilegios.

Para obtener información sobre cómo agregar orígenes de identidad y conceder permisos a usuarios y grupos, consulte *Seguridad de vSphere*.

Este capítulo incluye los siguientes temas:

- [Descargar vCenter Server para Windows Installer](#)
- [Instalación de vCenter Server con una instancia de Platform Services Controller integrada](#)
- [Instalación de vCenter Server con un Platform Services Controller externo](#)
- [Instalar vCenter Server en un entorno con varias NIC](#)

Descargar vCenter Server para Windows Installer

Descargue el instalador `.iso` para vCenter Server para Windows y los componentes asociados de vCenter Server y sus herramientas de soporte.

Requisitos previos

Cree una cuenta de Customer Connect en <https://my.vmware.com/web/vmware/>.

Procedimiento

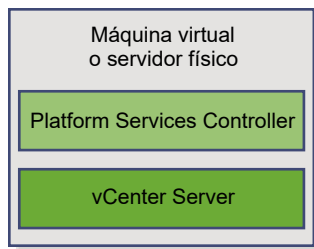
- 1 Descargue el instalador de vCenter Server del sitio web de VMware en <https://my.vmware.com/web/vmware/downloads>.
vCenter Server forma parte de VMware vCloud Suite y VMware vSphere, incluidos en Centro de datos e infraestructura de nube.
- 2 Confirme que el valor de md5sum sea correcto.
Consulte el tema del sitio web de VMware Uso de sumas de comprobación de MD5 en <http://www.vmware.com/download/md5.html>.
- 3 Monte la imagen ISO en la máquina virtual Windows o el servidor físico donde desea instalar vCenter Server para Windows.

Instalación de vCenter Server con una instancia de Platform Services Controller integrada

Puede implementar vCenter Server, los componentes de vCenter Server y Platform Services Controller en una máquina virtual o servidor físico.

Después de implementar vCenter Server con una instancia de Platform Services Controller integrada, puede volver a configurar la topología y cambiar a vCenter Server con una instancia de Platform Services Controller externa. Este es un proceso unidireccional. Una vez realizado, no se puede volver a vCenter Server con una instancia de Platform Services Controller integrada. Puede redireccionar la instancia de vCenter Server solo a una instancia de Platform Services Controller externa configurada para replicar los datos de infraestructura dentro del mismo dominio.

Figura 8-1. vCenter Server con un Platform Services Controller integrado



Importante No se admiten instalaciones simultáneas de instancias de vCenter Server con Platform Services Controller integrados. Debe instalar las instancias de vCenter Server con Platform Services Controller integrados en una secuencia.

Requisitos previos

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software.

- Descargue el instalador de vCenter Server.
- Si desea utilizar vSphere Web Client en el equipo host en el que va a instalar vCenter Server, compruebe que Adobe Flash Player 11.9 o posterior esté instalado en el sistema.

Procedimiento

- 1 En el directorio del instalador del software, haga doble clic en el archivo `autorun.exe` para iniciar el instalador.
- 2 Seleccione **vCenter Server para Windows** y haga clic en **Instalar**.
- 3 Siga las indicaciones del asistente para instalación para revisar la página principal y acepte el contrato de licencia.
- 4 Seleccione **vCenter Server y Platform Services Controller** integrado y haga clic en **Siguiente**.
- 5 Introduzca el nombre de la red del sistema, de preferencia un FQDN y haga clic en **Siguiente**.

También puede introducir una dirección IP. Si introduce una dirección IP, proporcione una dirección IP estática.

Importante Asegúrese de que la FQDN o la dirección IP que proporciona no cambie. El nombre del sistema no puede cambiar después de la implementación. Si el nombre del sistema cambia, debe desinstalar vCenter Server y volver a instalarlo.

6 Cree un nuevo dominio de vCenter Single Sign-On o únase a un dominio existente.

Importante Aunque puede elegir unirse a un dominio de vCenter Single Sign-On, también puede utilizar vCenter Server con una instancia de Platform Services Controller integrada como instalación independiente y no utilizarlo para replicar los datos de infraestructura.

Opción	Descripción
Crear un nuevo dominio de Single Sign-On	<p>Crea un nuevo servidor vCenter Single Sign-On.</p> <ol style="list-style-type: none"> Introduzca el nombre de dominio; por ejemplo, <code>vsphere.local</code>. Defina la contraseña para la cuenta de administrador de vCenter Single Sign-On. <p>Esta es la contraseña del usuario <code>administrator@su_nombre_de_dominio</code>, donde <code>su_nombre_de_dominio</code> es un nuevo dominio creado por vCenter Single Sign-On. Tras la instalación, puede iniciar sesión en vCenter Single Sign-On y en vCenter Server como <code>administrator@su_nombre_de_dominio</code>.</p> <ol style="list-style-type: none"> Introduzca el nombre del sitio para vCenter Single Sign-On. <p>El nombre del sitio es importante si utiliza vCenter Single Sign-On en varias ubicaciones. Seleccione su propio nombre para el sitio de vCenter Single Sign-On. No puede cambiar el nombre después de la instalación.</p> <p>Solo se admiten caracteres alfanuméricos y guiones (-).</p>
Unirse a un dominio de Single Sign-On en una instancia de Platform Services Controller existente	<p>Se une a un nuevo servidor vCenter Single Sign-On a un dominio de vCenter Single Sign-On en una instancia de Platform Services Controller existente. Debe proporcionar la información sobre el servidor vCenter Single Sign-On al que se va a unir el nuevo servidor vCenter Single Sign-On.</p> <ol style="list-style-type: none"> Escriba el nombre de dominio completo (fully qualified domain name, FQDN) o la dirección IP de la instancia de Platform Services Controller que contiene el servidor vCenter Single Sign-On al que se va a unir. Escriba el puerto HTTPS que se va a usar para comunicarse con la instancia de Platform Services Controller. Escriba la contraseña de la cuenta de administrador de vCenter Single Sign-On. Haga clic en Siguiente. Apruebe el certificado proporcionado por la máquina remota. Determine si desea crear un sitio de vCenter Single Sign-On o unirse a uno existente.

7 Haga clic en **Siguiente**.

- 8 Seleccione la cuenta de servicio de vCenter Server y haga clic en **Siguiente**.

Opción	Descripción
Utilizar cuenta del sistema local Windows	El servicio vCenter Server se ejecuta en la cuenta del sistema local Windows. Esta opción le impide conectarse a una base de datos externa mediante la autenticación integrada de Windows.
Especificar una cuenta de servicio de usuario	El servicio vCenter Server se ejecuta en una cuenta de usuario administrativo con el nombre de usuario y la contraseña que proporcione.

Importante Las credenciales de usuario que brinda deben pertenecer a un usuario del grupo de administradores locales y tener el privilegio **Inicio de sesión como servicio**.

- 9 Seleccione el tipo de base de datos que desee utilizar y haga clic en **Siguiente**.

Opción	Descripción
Usar una base de datos integrada (PostgreSQL)	vCenter Server utiliza la base de datos integrada de PostgreSQL. Esta base de datos es adecuada para implementaciones de pequeña escala.
Usar una base de datos externa	vCenter Server utiliza una base de datos externa existente. a Seleccione la base de datos en la lista de DSN disponibles. b Escriba el nombre de usuario y la contraseña del DSN. Si su base de datos utiliza autenticación de Windows NT, los cuadros de texto para nombre de usuario y contraseña están deshabilitados.

- 10 Para cada componente, acepte los números de puerto predeterminados o, si otro servicio está utilizando los valores predeterminados, introduzca los puertos alternativos y haga clic en **Siguiente**.

Asegúrese de que los puertos 80 y 443 estén libres y sean dedicados, para que vCenter Single Sign-On pueda utilizarlos. De lo contrario, utilice puertos personalizados durante la instalación.

- 11 (opcional) Cambie las carpetas de destino predeterminadas y haga clic en **Siguiente**.

Importante No utilice carpetas que terminen con un signo de exclamación (!).

- 12 Revise la página del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware y decida si desea unirse a él.

Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administración de vCenter Server y hosts*.

- 13 Revise el resumen de la configuración de instalación y haga clic en **Instalar**.

- 14 (opcional) Haga clic en **Iniciar vSphere Web Client** para abrir vSphere Web Client e inicie sesión en vCenter Server.

- 15 Una vez concluida la instalación, haga clic en **Finalizar**.

Resultados

vCenter Server, los componentes devCenter Server y Platform Services Controller están instalados.

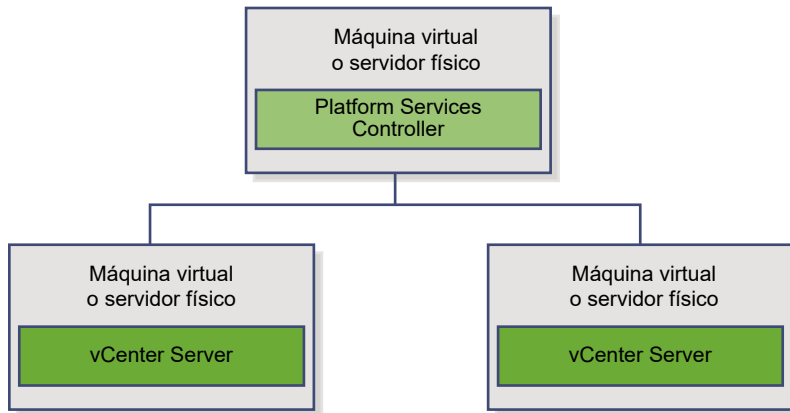
Instalación de vCenter Server con un Platform Services Controller externo

Puede instalar vCenter Server y el Platform Services Controller en máquinas virtuales o servidores físicos diferentes.

Puede separar el Platform Services Controller y vCenter Server y tenerlos instalados en diferentes máquinas virtuales o servidores físicos. En primer lugar, instale el Platform Services Controller y, a continuación, instale vCenter Server y los componentes de vCenter Server en otra máquina física o virtual, y conecte vCenter Server al Platform Services Controller. Puede conectar varias instancias de vCenter Server a un Platform Services Controller.

Importante No se admiten las instalaciones simultáneas de instancias de vCenter Server y Platform Services Controller. Deberá instalar los Platform Services Controller e instancias de vCenter Server en secuencia.

Figura 8-2. vCenter Server con un Platform Services Controller externo



Después de implementar vCenter Server con una instancia de Platform Services Controller integrada, puede volver a configurar la topología y cambiar a vCenter Server con una instancia de Platform Services Controller externa. Este es un proceso unidireccional. Una vez realizado, no se puede volver a vCenter Server con una instancia de Platform Services Controller integrada. Puede redireccionar la instancia de vCenter Server solo a una instancia de Platform Services Controller externa configurada para replicar los datos de infraestructura dentro del mismo dominio.

Importante Antes de instalar vCenter Server con un Platform Services Controller externo, sincronice los relojes en la red de vSphere. El sesgo horario en las máquinas virtuales o servidores físicos en los que instala el Platform Services Controller y vCenter Server podría causar un error de implementación. Para obtener instrucciones sobre la sincronización de los relojes en su red de vSphere, consulte [Sincronizar los relojes en la red de vSphere](#).

Instalar Platform Services Controller en una máquina con Windows

Para instalar vCenter Server con una instancia de Platform Services Controller externa, instale en primer lugar una instancia de Platform Services Controller para Windows. Platform Services Controller contiene los servicios comunes, como vCenter Single Sign-On y License service, que se pueden compartir en varias instancias de vCenter Server.

Puede instalar varias instancias de Platform Services Controller y asociarlas al mismo dominio de vCenter Single Sign-On. No se admiten instalaciones simultáneas de instancias de Platform Services Controller. Deberá instalar las instancias de Platform Services Controller en secuencia.

Importante Si desea reemplazar el certificado firmado por VMCA por un certificado firmado por CA, instale Platform Services Controller en primer lugar y, a continuación, incluya VMCA en la cadena de certificados y genere certificados nuevos desde VMCA que estén firmados por toda la cadena. A continuación, puede instalar vCenter Server. Para obtener información sobre la administración de certificados de vCenter Server, consulte la documentación de *Seguridad de vSphere*.

Requisitos previos

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software.
- Descargue el instalador de vCenter Server.
- Si desea unir la nueva instalación de Platform Services Controller a un dominio de vCenter Single Sign-On existente, verifique que todas las instancias de Platform Services Controller dentro del dominio correspondan a la misma actualización o parche versión 6.0 que la instancia Platform Services Controller que está instalando. Para obtener información acerca de cómo actualizar y aplicar revisiones en una instalación o dispositivo de Windows Platform Services Controller, consulte la documentación de *Actualización de vSphere*.

Procedimiento

- 1 En el directorio del instalador del software, haga doble clic en el archivo `autorun.exe` para iniciar el instalador.
- 2 Seleccione **vCenter Server para Windows** y haga clic en **Instalar**.
- 3 Siga las indicaciones del asistente para instalación para revisar la página principal y acepte el contrato de licencia.
- 4 Seleccione **Platform Services Controller** y haga clic en **Siguiente**.

- 5 Introduzca el nombre del sistema, preferiblemente un FQDN, y haga clic en **Siguiente**.

También puede introducir una dirección IP. Si introduce una dirección IP, proporcione una dirección IP estática.

Importante Cuando proporcione un FQDN o una dirección IP como el nombre del sistema de Platform Services Controller, asegúrese de que el FQDN o la dirección IP no sufran cambios. Si el FQDN o la dirección IP del equipo host cambia, deberá volver a instalar Platform Services Controller y las instancias de vCenter Server registradas con este. El FQDN o la dirección IP de Platform Services Controller se utiliza para generar un certificado SSL para el equipo host de Platform Services Controller.

- 6 Cree un nuevo dominio de vCenter Single Sign-On o únase a un dominio existente.

Opción	Descripción
Crear un nuevo dominio de Single Sign-On	<p>Crea un nuevo servidor vCenter Single Sign-On.</p> <ol style="list-style-type: none"> Introduzca el nombre de dominio; por ejemplo, vsphere.local. Defina la contraseña para la cuenta de administrador de vCenter Single Sign-On. <p>Esta es la contraseña del usuario <code>administrator@su_nombre_de_dominio</code>, donde <code>su_nombre_de_dominio</code> es un nuevo dominio creado por vCenter Single Sign-On. Tras la instalación, puede iniciar sesión en vCenter Single Sign-On y en vCenter Server como <code>administrator@su_nombre_de_dominio</code>.</p> <ol style="list-style-type: none"> Introduzca el nombre del sitio para vCenter Single Sign-On. <p>El nombre del sitio es importante si utiliza vCenter Single Sign-On en varias ubicaciones. Seleccione su propio nombre para el sitio de vCenter Single Sign-On. No puede cambiar el nombre después de la instalación.</p> <p>Solo se admiten caracteres alfanuméricos y guiones (-).</p>
Unirse a un dominio de Single Sign-On en una instancia de Platform Services Controller existente	<p>Se une a un nuevo servidor vCenter Single Sign-On a un dominio de vCenter Single Sign-On en una instancia de Platform Services Controller existente. Debe proporcionar la información sobre el servidor vCenter Single Sign-On al que se va a unir el nuevo servidor vCenter Single Sign-On.</p> <ol style="list-style-type: none"> Escriba el nombre de dominio completo (fully qualified domain name, FQDN) o la dirección IP de la instancia de Platform Services Controller que contiene el servidor vCenter Single Sign-On que se va a unir. Escriba el puerto HTTPS que se va a usar para comunicarse con la instancia de Platform Services Controller. Escriba la contraseña de la cuenta de administrador de vCenter Single Sign-On. Haga clic en Siguiente. Apruebe el certificado proporcionado por la máquina remota. Determine si desea crear un sitio de vCenter Single Sign-On o unirse a uno existente.

Si decide unirse a un dominio de vCenter Single Sign-On existente, se habilita la característica Enhanced Linked Mode. La instancia de Platform Services Controller replicará los datos de infraestructura con el servidor vCenter Single Sign-On que se unió.

7 Haga clic en **Siguiente**.

8 Para cada componente, acepte los números de puerto predeterminados o, si otro servicio está utilizando los valores predeterminados, introduzca los puertos alternativos y haga clic en **Siguiente**.

Asegúrese de que los puertos 80 y 443 estén libres y sean dedicados, para que vCenter Single Sign-On pueda utilizarlos. De lo contrario, utilice puertos personalizados durante la instalación.

9 (opcional) Cambie las carpetas de destino predeterminadas y haga clic en **Siguiente**.

Importante No utilice carpetas que terminen con un signo de exclamación (!).

10 Revise la página del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware y decida si desea unirse a él.

Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administración de vCenter Server y hosts*.

11 Revise el resumen de la configuración de instalación y haga clic en **Instalar**.

12 Una vez concluida la instalación, haga clic en **Finalizar**.

Resultados

Platform Services Controller está instalado.

Pasos siguientes

Instale vCenter Server en otra máquina virtual o servidor físico con Windows y registre vCenter Server y los componentes de vCenter Server en Platform Services Controller.

Instalar vCenter Server y los componentes de vCenter Server

Después de instalar Platform Services Controller en un equipo host con Windows o de implementar un dispositivo Platform Services Controller, podrá instalar vCenter Server y los componentes de vCenter Server y conectar la instancia de vCenter Server al Platform Services Controller implementado.

No se admiten las instalaciones simultáneas de instancias de vCenter Server. Si desea instalar varias instancias de vCenter Server y registrarlas con el mismo Platform Services Controller o el dispositivo Platform Services Controller, instale las instancias de vCenter Server una por una en secuencia.

Requisitos previos

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software.

- Descargue el instalador de vCenter Server.
- Si desea utilizar vSphere Web Client en el equipo host en el que va a instalar vCenter Server, compruebe que Adobe Flash Player 11.9 o posterior esté instalado en el sistema.

Procedimiento

- 1 En el directorio del instalador del software, haga doble clic en el archivo `autorun.exe` para iniciar el instalador.
- 2 Seleccione **vCenter Server para Windows** y haga clic en **Instalar**.
- 3 Siga las indicaciones del asistente para instalación para revisar la página principal y acepte el contrato de licencia.
- 4 Seleccione **vCenter Server** y haga clic en **Siguiente**.
- 5 Introduzca el nombre de red del sistema, preferiblemente una dirección IP estática, y haga clic en **Siguiente**.

Importante El nombre que introduzca se codifica en el certificado SSL del sistema. Los componentes se comunican entre sí con este nombre. El nombre del sistema debe ser una dirección IP estática o un nombre de dominio completo (FQDN). Asegúrese de que no se cambie el nombre del sistema. No podrá cambiar el nombre del sistema después de que se complete la instalación.

- 6 Proporcione el nombre del sistema de Platform Services Controller que ya ha instalado o implementado, el puerto HTTPS que se va a utilizar para la comunicación con el servidor de vCenter Single Sign-On y la contraseña de vCenter Single Sign-On, y haga clic en **Siguiente**.

Importante Asegúrese de utilizar la dirección IP o el FQDN que proporcionó durante la instalación de Platform Services Controller. Si ha proporcionado el FQDN como un nombre del sistema de Platform Services Controller, no podrá utilizar una dirección IP y a la inversa. Cuando un servicio de vCenter Server se conecta a un servicio que se ejecuta en Platform Services Controller, se verifica el certificado. Si cambia la dirección IP o el FQDN, se produce un error en la verificación y vCenter Server no puede conectarse al Platform Services Controller.

- 7 Apruebe el certificado proporcionado por la máquina remota.

- 8 Seleccione la cuenta de servicio de vCenter Server y haga clic en **Siguiente**.

Opción	Descripción
Utilizar cuenta del sistema local Windows	El servicio vCenter Server se ejecuta en la cuenta del sistema local Windows. Esta opción le impide conectarse a una base de datos externa mediante la autenticación integrada de Windows.
Especificar una cuenta de servicio de usuario	El servicio vCenter Server se ejecuta en una cuenta de usuario administrativo con el nombre de usuario y la contraseña que proporcione.

Importante Las credenciales de usuario que brinda deben pertenecer a un usuario del grupo de administradores locales y tener el privilegio **Inicio de sesión como servicio**.

- 9 Seleccione el tipo de base de datos que desee utilizar y haga clic en **Siguiente**.

Opción	Descripción
Usar una base de datos integrada (PostgreSQL)	vCenter Server utiliza la base de datos integrada de PostgreSQL. Esta base de datos es adecuada para implementaciones de pequeña escala.
Usar una base de datos externa	vCenter Server utiliza una base de datos externa existente. a Seleccione la base de datos en la lista de DSN disponibles. b Escriba el nombre de usuario y la contraseña del DSN. Si su base de datos utiliza autenticación de Windows NT, los cuadros de texto para nombre de usuario y contraseña están deshabilitados.

- 10 Para cada componente, acepte los números de puerto predeterminados o, si otro servicio está utilizando los valores predeterminados, introduzca los puertos alternativos y haga clic en **Siguiente**.
- 11 (opcional) Cambie las carpetas de destino predeterminadas y haga clic en **Siguiente**.

Importante No utilice carpetas que terminen con un signo de exclamación (!).

- 12 Revise el resumen de la configuración de instalación y haga clic en **Instalar**.
- 13 (opcional) Haga clic en **Iniciar vSphere Web Client** para abrir vSphere Web Client e inicie sesión en vCenter Server.
- 14 Una vez concluida la instalación, haga clic en **Finalizar**.

Resultados

vCenter Server se instala en modo de evaluación. Puede activar vCenter Server mediante vSphere Web Client. Para obtener información sobre la activación de vCenter Server, consulte *Administración de vCenter Server y hosts*.

Instalar vCenter Server en un entorno con varias NIC

Si desea instalar vCenter Server con una instancia de Platform Services Controller externa en un entorno con varias NIC, debe mantener un registro de las direcciones IP o los FQDN que utiliza como nombres de red del sistema.

Por ejemplo, si desea instalar Platform Services Controller en una máquina virtual y vCenter Server en otra, y cada máquina virtual tiene dos NIC, puede usar el siguiente flujo de trabajo:

- 1 Instale Platform Services Controller en una de las máquinas virtuales y utilice una de sus direcciones IP o un FQDN como nombre de red del sistema.
- 2 En la otra máquina virtual, inicie la instalación de vCenter Server y use una de sus direcciones IP o un FQDN como nombre de red del sistema.
- 3 Cuando se le pida que proporcione el nombre de red del sistema de Platform Services Controller, escriba la dirección IP o el FQDN que introdujo durante la instalación de Platform Services Controller.

Si escribe la otra dirección IP o el otro FQDN de Platform Services Controller, recibirá un mensaje de error.

- 4 Una vez que finalice la instalación, podrá iniciar sesión en vSphere Web Client con cualquier dirección IP o FQDN de NIC de vCenter Server.

Implementar vCenter Server Appliance

9

Como alternativa a la instalación de vCenter Server en una máquina virtual o servidor físico Windows, puede implementar vCenter Server Appliance.

Antes de implementar vCenter Server Appliance, descargue el archivo ISO y móntelo en el equipo host Windows desde el cual desea realizar la implementación. Instale el complemento de integración de clientes y, a continuación, inicie el asistente de instalación.

Para obtener información sobre los requisitos de vCenter Server Appliance, consulte [Requisitos de vCenter Server Appliance](#).

Para obtener información sobre las entradas requeridas durante la implementación de vCenter Server Appliance, consulte [Información necesaria para la implementación de vCenter Server Appliance](#).

vCenter Server Appliance tiene los siguientes nombres de usuario predeterminados:

- raíz con la contraseña del sistema operativo que se introduce al implementar el dispositivo virtual.
- `administrator@your_domain_name` con la contraseña de vCenter Single Sign-On que se introduce al implementar el dispositivo virtual.

Después de implementar vCenter Server Appliance, solo el usuario `administrator@your_domain_name` tiene los privilegios para iniciar sesión en el sistema vCenter Server.

El usuario `administrator@your_domain_name` puede proceder de la siguiente manera:

- Agregar un origen de identidad en el cual los usuarios y grupos tienen definido vCenter Single Sign-On.
- Otorgar permisos a los usuarios y grupos.

Para obtener información sobre cómo agregar orígenes de identidad y conceder permisos a usuarios y grupos, consulte *Seguridad de vSphere*.

La versión 6.0 de vCenter Server Appliance se implementa con la versión 8 del hardware virtual, que admite 32 CPU virtuales por máquina virtual en ESXi. En función de los hosts que vaya a administrar con vCenter Server Appliance, sería conveniente actualizar los hosts de ESXi y actualizar la versión del hardware de vCenter Server Appliance para admitir más CPU virtuales:

- ESXi 5.5.x admite hardware virtual hasta la versión 10 con hasta 64 CPU virtuales por máquina virtual.
- ESXi 6.0 admite hardware virtual hasta la versión 11 con hasta 128 CPU virtuales por máquina virtual.

Importante No puede implementarse vCenter Server Appliance mediante vSphere Client ni vSphere Web Client. Durante la implementación de vCenter Server Appliance, debe proporcionar varias entradas, como las contraseñas de vCenter Single Sign-On y del sistema operativo. Si intenta implementar la aplicación mediante vSphere Client o vSphere Web Client, el sistema no le solicita que proporcione estas entradas de datos y se produce un error en la implementación.

Para obtener información sobre la actualización de vCenter Server Appliance, consulte *Actualización de vSphere*.

Para los límites de inventario y otros límites de configuración de vCenter Server Appliance, consulte la documentación *Máximos de configuración*.

Para ver información acerca de la configuración de vCenter Server Appliance, consulte *Configuración de vCenter Server Appliance*.

Importante vCenter Server 6.0 admite conexión entre componentes de vCenter Server y vCenter Server mediante direcciones IPv4 o IPv6. No se admite un entorno mixto de IPv4 y IPv6. Si desea configurar vCenter Server Appliance para usar una asignación de dirección IPv6, asegúrese de utilizar el nombre de dominio completo (FQDN, fully qualified domain name) o nombre de host del dispositivo. En un entorno IPv4, la práctica recomendada es usar el FQDN o nombre de host del dispositivo, ya que la dirección IP puede cambiar si se asigna mediante DHCP.

Este capítulo incluye los siguientes temas:

- [Descargar el instalador de vCenter Server Appliance](#)
- [Instalar el complemento de integración de clientes](#)
- [Implementación de vCenter Server Appliance con una instancia de Platform Services Controller integrada](#)
- [Implementar vCenter Server Appliance con una instancia de Platform Services Controller externa](#)

Descargar el instalador de vCenter Server Appliance

Descargue el instalador `.iso` para vCenter Server Appliance y el complemento de integración de clientes.

Requisitos previos

Cree una cuenta de Customer Connect en <https://my.vmware.com/web/vmware/>.

Procedimiento

- 1 Descargue el instalador de vCenter Server Appliance del sitio web de VMware en <https://my.vmware.com/web/vmware/downloads>.
- 2 Confirme que el valor de md5sum sea correcto.
Consulte el tema del sitio web de VMware Uso de sumas de comprobación de MD5 en <http://www.vmware.com/download/md5.html>.
- 3 Monte la imagen ISO en el servidor físico o la máquina virtual con Windows donde desea instalar el complemento de integración de clientes para la implementación o actualización de vCenter Server Appliance.

Si la máquina virtual ejecuta Windows, puede usar vSphere Web Client para configurar la imagen ISO como un archivo ISO de almacén de datos para la unidad de CD/DVD de la máquina virtual. Consulte *Administración de máquinas virtuales de vSphere*.

Instalar el complemento de integración de clientes

El complemento de integración de clientes permite acceder a la consola de una máquina virtual en vSphere Web Client y ofrece acceso a otras características de infraestructura de vSphere. El complemento de integración de clientes también le permite iniciar sesión en vSphere Web Client con credenciales de sesión de Windows.

El complemento de integración de clientes se utiliza para implementar plantillas OVF u OVA y transferir archivos con el explorador del almacén de datos. También puede utilizarlo para conectar dispositivos virtuales que residen en un equipo cliente a una máquina virtual.

Instale el complemento de integración de clientes solo una vez para habilitar todas las funciones que proporciona. Debe cerrar el explorador web antes de instalar el complemento.

Para obtener información sobre los exploradores y los sistemas operativos compatibles, consulte la documentación de *Instalación y configuración de vSphere*.

Vea el vídeo "Instalación del complemento de integración de clientes" para obtener información al respecto:



Instalar el complemento de integración de clientes
(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_6p2x7nkr/uiConfId/49694343/)

Procedimiento

- 1 En vSphere Web Client, busque el vínculo para descargar el complemento de integración de clientes.

Opción	Descripción
Página de inicio de sesión de vSphere Web Client	<ol style="list-style-type: none"> a Abra un explorador web y escriba la URL de vSphere Web Client. b En la parte inferior de la página de inicio de sesión de vSphere Web Client, haga clic en Descargar complemento de integración de clientes. <p>Nota Si el complemento de integración de clientes ya está instalado en el sistema, no verá el vínculo para descargar el complemento. Si desinstala el complemento de integración de clientes, el vínculo para descargarlo se mostrará en la página de inicio de sesión de vSphere Web Client.</p>
asistente para implementación de OVF	<ol style="list-style-type: none"> a Seleccione un host en el inventario y elija Acciones > Implementar plantilla de OVF. b Haga clic en Descargar complemento de integración de clientes.

- 2 Si el navegador 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.

Implementación de vCenter Server Appliance con una instancia de Platform Services Controller integrada

Cuando se elige implementar vCenter Server Appliance con una instancia de Platform Services Controller integrada, se implementan Platform Services Controller y vCenter Server como una sola aplicación.

Importante Las implementaciones simultáneas de vCenter Server Appliance con instancias de Platform Services Controller integradas no son compatibles. Las instancias de vCenter Server Appliance deben implementarse con instancias de Platform Services Controller integradas en una secuencia.

Requisitos previos

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software.
- Descargue el instalador de vCenter Server Appliance.
- Instale el complemento de integración de clientes.
- Compruebe que el host ESXi de destino en el que implementó vCenter Server Appliance no esté en modo de bloqueo o de mantenimiento.
- Compruebe si preparó la información de implementación correcta para la configuración de red. Conozca toda la información necesaria durante la implementación en el tema [Información necesaria para la implementación de vCenter Server Appliance con una instancia de Platform Services Controller integrada](#).

- Si va a utilizar servidores NTP para sincronizar la hora, asegúrese de que la hora de los servidores NTP esté sincronizada con la del host ESXi.

Procedimiento

- 1 En el directorio del instalador del software, haga doble clic en **vcsa-setup.html**.
- 2 Espere tres segundos a que el explorador detecte el complemento de integración de clientes y permita que este se ejecute en el explorador cuando se le pida.
- 3 En la página de inicio, haga clic en **Instalar** para iniciar el asistente para implementación de vCenter Server Appliance.
- 4 Lea y acepte el contrato de licencia, y haga clic en **Siguiente**.
- 5 Conéctese al servidor de destino en el cual desea implementar vCenter Server Appliance y haga clic en **Siguiente**.
 - Puede conectarse a un host ESXi para implementar el dispositivo allí.
 - a Escriba el FQDN o la dirección IP del host ESXi.
 - b Escriba el nombre de usuario y la contraseña de un usuario que tenga privilegios administrativos en el host ESXi (por ejemplo, el usuario raíz).
 - Puede conectarse a una instancia de vCenter Server para implementar el dispositivo en un host o un clúster de DRS ESXi desde el inventario de vCenter Server.
 - a Escriba el nombre de dominio completo o la dirección IP de la instancia de vCenter Server.
 - b Escriba el nombre de usuario y la contraseña de un usuario que tenga privilegios administrativos en la instancia de vCenter Server, por ejemplo, el usuario `administrator@su_nombre_de_dominio`.
- 6 (opcional) Si recibe una advertencia de certificado, acéptela haciendo clic en **Sí**.
- 7 Si desea implementar vCenter Server Appliance en una instancia de vCenter Server, seleccione el centro de datos o la carpeta de centro de datos donde se encuentra el host ESXi o el clúster de DRS en el cual desea implementar el dispositivo y haga clic en **Siguiente**.

Nota Es necesario seleccionar un centro de datos o una carpeta de centro de datos que contenga al menos un host ESXi que no se encuentre en modo de bloqueo o de mantenimiento.

- 8 Si desea implementar vCenter Server Appliance en una instancia de vCenter Server, seleccione el grupo de recursos de un host ESXi o un clúster de DRS en el cual desea implementar el dispositivo y haga clic en **Siguiente**.

Nota Si selecciona un grupo de recursos de un clúster que no se encuentra en modo DRS, el asistente le pedirá que seleccione un host ESXi del clúster.

- 9 En la página Configurar máquina virtual, escriba el nombre de vCenter Server Appliance, establezca la contraseña para el usuario raíz y haga clic en **Siguiente**.

La contraseña debe contener al menos ocho caracteres, entre los cuales se debe incluir un número, letras mayúsculas y minúsculas, y un carácter especial, como un signo de exclamación (!), un numeral (#), una arroba (@) o un paréntesis (()).

- 10 En la página Seleccionar tipo de implementación, seleccione **Instalar vCenter Server con una instancia de Platform Services Controller integrada** y haga clic en **Siguiente**.

Esta opción implementa una aplicación en la que están instalados Platform Services Controller y también vCenter Server.

- 11 Cree un nuevo dominio de vCenter Single Sign-On o únase a un dominio existente y haga clic en **Siguiente**.

Importante Aunque puede elegir unirse a un dominio de vCenter Single Sign-On, también puede utilizar vCenter Server Appliance con una instancia de Platform Services Controller integrada como implementación independiente y no utilizarlo para replicar los datos de infraestructura.

Opción	Descripción
Crear un nuevo dominio de Single Sign-On	<p>Crea un nuevo servidor vCenter Single Sign-On.</p> <ol style="list-style-type: none"> Defina la contraseña para la cuenta de administrador de vCenter Single Sign-On. <p>Esta es la contraseña del usuario <code>administrator@su_nombre_de_dominio</code>, donde <code>su_nombre_de_dominio</code> es un nuevo dominio creado por vCenter Single Sign-On. Tras la instalación, puede iniciar sesión en vCenter Single Sign-On y en vCenter Server como <code>administrator@su_nombre_de_dominio</code>.</p> <ol style="list-style-type: none"> Introduzca el nombre de dominio; por ejemplo, <code>vsphere.local</code>. Introduzca el nombre del sitio para vCenter Single Sign-On. <p>El nombre del sitio es importante si utiliza vCenter Single Sign-On en varias ubicaciones. Seleccione su propio nombre para el sitio de vCenter Single Sign-On. No puede cambiar el nombre después de la instalación.</p> <p>Solo se admiten caracteres alfanuméricos y guiones (-).</p>
Unirse a un dominio de Single Sign-On en una instancia de Platform Services Controller existente	<p>Une un nuevo servidor vCenter Single Sign-On a un dominio de vCenter Single Sign-On en una instancia de Platform Services Controller existente. Debe proporcionar la información sobre el servidor vCenter Single Sign-On al que se va a unir el nuevo servidor vCenter Single Sign-On.</p> <ol style="list-style-type: none"> Escriba el nombre de dominio completo (fully qualified domain name, FQDN) o la dirección IP de la instancia de Platform Services Controller que contiene el servidor vCenter Single Sign-On al que se va a unir. Escriba la contraseña de la cuenta de administrador de vCenter Single Sign-On. Escriba el puerto HTTPS que se va a usar para comunicarse con Platform Services Controller y haga clic en Siguiente. Determine si desea crear un sitio de vCenter Single Sign-On o unirse a uno existente.

- 12 En la página Seleccionar tamaño de la aplicación, seleccione el tamaño de vCenter Server Appliance para el inventario de vSphere y haga clic en **Siguiente**.

Opción	Descripción
Muy pequeño (hasta 10 hosts y 100 máquinas virtuales)	Implementa un dispositivo con 2 CPU y 8 GB de memoria.
Pequeño (hasta 100 hosts y 1.000 máquinas virtuales)	Implementa un dispositivo con 4 CPU y 16 GB de memoria.

Opción	Descripción
Mediano (hasta 400 hosts y 4.000 máquinas virtuales)	Implementa un dispositivo con 8 CPU y 24 GB de memoria.
Grande (hasta 1.000 hosts y 10.000 máquinas virtuales)	Implementa un dispositivo con 16 CPU y 32 GB de memoria.

- 13 En la lista de almacenes de datos disponibles, seleccione la ubicación en la que se almacenarán todos los archivos de configuración y discos virtuales de la máquina virtual. Opcionalmente, seleccione **Habilitar el modo de disco fino** para habilitar el aprovisionamiento fino.

- 14 Seleccione el tipo de base de datos que desee utilizar y haga clic en **Siguiente**.

Opción	Descripción
Usar una base de datos integrada (PostgreSQL)	Configura vCenter Server en el dispositivo para que utilice la base de datos integrada de PostgreSQL.
Usar una base de datos de Oracle	<p>Configura vCenter Server en el dispositivo para que utilice una base de datos externa de Oracle existente.</p> <ul style="list-style-type: none"> a Escriba la dirección IP o el FQDN del equipo en el que está instalada la base de datos de Oracle. b Escriba el puerto que se utilizará para comunicarse con la base de datos de Oracle. c Introduzca el nombre de la instancia de base de datos. d Escriba el nombre de usuario y la contraseña de la base de datos. <p>Importante Asegúrese de brindar las credenciales correctas. De lo contrario, la implementación podría presentar errores.</p>

- 15 En la página Configuración de red, establezca la configuración de red.

La dirección IP o el FQDN del dispositivo se utilizan como nombre del sistema. Se recomienda utilizar un FQDN. Sin embargo, si desea utilizar una dirección IP, utilice asignación de direcciones IP estáticas del dispositivo, ya que las direcciones IP que asigna DHCP podrían cambiar.

Opción	Acción
Elegir una red	<p>Seleccione la red a la que desea conectarse.</p> <p>Las redes que se muestran en el menú desplegable dependen de la configuración de red del servidor de destino. En el caso de la implementación directa de un dispositivo en un host ESXi, los grupos de puertos virtuales distribuidos que no son efímeros no se admiten y no se muestran en el menú desplegable.</p>
Familia de direcciones IP	<p>Seleccione la versión de IP del dispositivo.</p> <p>Puede seleccionar la versión IPv4 o IPv6.</p>

Opción	Acción
Tipo de red	<p>Seleccione cómo asignar la dirección IP del dispositivo.</p> <ul style="list-style-type: none"> ■ Estático <p>Se le pide que escriba la dirección IP y la configuración de red.</p> ■ DHCP <p>Los servidores DHCP se utilizan para asignar la dirección IP. Seleccione esta opción solo si hay un servidor DHCP disponible en el entorno.</p>
FQDN (opcional)	<p>Escriba un nombre de dominio completo (fully qualified domain name, FQDN) preferido del dispositivo.</p> <p>Nota Si decide utilizar IPv6 con el tipo de red DHCP, no verá la opción FQDN.</p>

Si utiliza una dirección IP como nombre del sistema, no puede modificarla ni actualizar la configuración de DNS después de la implementación.

- Configure la hora del dispositivo y, como alternativa, seleccione **Habilitar SSH** para asegurar la conexión. A continuación, haga clic en **Siguiente**.

Opción	Descripción
Sincronizar la hora del dispositivo con el host ESXi	Habilita la sincronización horaria periódica y permite que VMware Tools establezca la hora del sistema operativo invitado para que sea la misma que la hora del host ESXi.
Usar servidores NTP (separados por comas)	Utiliza un servidor de protocolo de tiempo de red para sincronizar la hora. Si selecciona esta opción, debe escribir los nombres de los servidores NTP separados por comas.

- Revise la página del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware y decida si desea unirse a él.

Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administración de vCenter Server y hosts*.
- En la página Listo para finalizar, revise la configuración de implementación de vCenter Server Appliance y haga clic en **Finalizar** para completar el proceso de implementación.
- (opcional) Una vez finalizada la implementación, haga clic en el vínculo **https://vcenter_server_appliance_ip_address/vsphere-client** para iniciar vSphere Web Client e iniciar sesión en la instancia de vCenter Server en vCenter Server Appliance.
- Haga clic en **Cerrar** para cerrar el asistente.

Implementar vCenter Server Appliance con una instancia de Platform Services Controller externa

Puede implementar un vCenter Server Appliance con una instancia externa de Platform Services Controller. De esta forma, puede implementar dos dispositivos diferentes.

Para implementar Platform Services Controller y la instancia de vCenter Server como dos dispositivos diferentes, en primer lugar, implemente Platform Services Controller y, a continuación, implemente vCenter Server y los componentes de vCenter Server como otro dispositivo virtual, y registre vCenter Server Appliance en Platform Services Controller.

Importante No se admiten las implementaciones simultáneas de instancias de vCenter Server Appliance y dispositivos Platform Services Controller. Deberá implementar los dispositivos Platform Services Controller y las instancias de vCenter Server Appliance en secuencia.

Importante Antes de implementar vCenter Server Appliance con una instancia de Platform Services Controller externa, sincronice los relojes en la red de vSphere. El sesgo horario en las máquinas virtuales podría causar un error en la implementación. Para obtener instrucciones sobre la sincronización de los relojes en su red de vSphere, consulte [Sincronizar los relojes en la red de vSphere](#).

Implementación de Platform Services Controller Appliance

Si planea implementar vCenter Server Appliance con un Platform Services Controller externo, implemente primero una aplicación de Platform Services Controller. La aplicación de Platform Services Controller contiene todos los servicios necesarios, como vCenter Single Sign-On y servicio de licencia, que se puede compartir entre varias instancias de vCenter Server.

Importante Puede implementar muchas aplicaciones Platform Services Controller y unir las al mismo dominio de vCenter Single Sign-On. No se admiten implementaciones simultáneas Platform Services Controller. Debe implementar Platform Services Controller en una secuencia.

Requisitos previos

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software.
- Descargue el instalador de vCenter Server Appliance.
- Instale el complemento de integración de clientes.
- Compruebe que el host ESXi en el que implementó el dispositivo Platform Services Controller no esté en modo de mantenimiento ni de bloqueo.
- Si desea unir el nuevo dispositivo Platform Services Controller a un dominio de vCenter Single Sign-On existente, verifique que todas las instancias de Platform Services Controller dentro del dominio correspondan a la misma actualización o parche versión 6.0 que el dispositivo Platform Services Controller que está implementando. Para obtener información acerca de cómo actualizar y aplicar revisiones en una instalación o dispositivo de Windows Platform Services Controller, consulte la documentación de *Actualización de vSphere*.
- Compruebe si preparó la información de implementación correcta para la configuración de red. Conozca toda la información necesaria durante la implementación en el tema [Información necesaria para la implementación de Platform Services Controller Appliance](#).

- Si va a utilizar servidores NTP para sincronizar la hora, asegúrese de que la hora de los servidores NTP esté sincronizada con la del host ESXi.

Procedimiento

- 1 En el directorio del instalador del software, haga doble clic en **vcsa-setup.html**.
- 2 Espere tres segundos a que el explorador detecte el complemento de integración de clientes y permita que este se ejecute en el explorador cuando se le pida.
- 3 En la página de inicio, haga clic en **Instalar** para iniciar el asistente para implementación de vCenter Server Appliance.
- 4 Lea y acepte el contrato de licencia, y haga clic en **Siguiente**.
- 5 Conéctese al servidor de destino en el cual desea implementar el dispositivo Platform Services Controller y haga clic en **Siguiente**.
 - Puede conectarse a un host ESXi para implementar el dispositivo allí.
 - a Escriba el FQDN o la dirección IP del host ESXi.
 - b Escriba el nombre de usuario y la contraseña de un usuario que tenga privilegios administrativos en el host ESXi, por ejemplo, el usuario raíz.
 - Puede conectarse a una instancia de vCenter Server para implementar el dispositivo en un host o un clúster de DRS ESXi desde el inventario de vCenter Server.
 - a Escriba el nombre de dominio completo o la dirección IP de la instancia de vCenter Server.
 - b Escriba el nombre de usuario y la contraseña de un usuario que tenga privilegios administrativos en la instancia de vCenter Server, por ejemplo, el usuario `administrator@your_domain_name`.
- 6 (opcional) Si recibe una advertencia de certificado, acéptela haciendo clic en **Sí**.
- 7 Si desea implementar Platform Services Controller en una instancia de vCenter Server, seleccione el centro de datos o la carpeta de centro de datos donde se encuentra el host ESXi o el clúster de DRS en el cual desea implementar el dispositivo y haga clic en **Siguiente**.

Nota Es necesario seleccionar un centro de datos o una carpeta de centro de datos que contenga al menos un host ESXi que no se encuentre en modo de bloqueo o de mantenimiento.

- 8 Si desea implementar Platform Services Controller en una instancia de vCenter Server, seleccione el grupo de recursos de un host ESXi o un clúster de DRS en el cual desea implementar el dispositivo y haga clic en **Siguiente**.

Nota Si selecciona un grupo de recursos de un clúster que no se encuentra en modo DRS, el asistente le pedirá que seleccione un host ESXi del clúster.

- 9 En la página Configurar máquina virtual, escriba el nombre de dispositivo Platform Services Controller, establezca la contraseña para el usuario raíz y haga clic en **Siguiente**.

La contraseña debe contener al menos ocho caracteres, entre los cuales se debe incluir un número, letras mayúsculas y minúsculas, y un carácter especial, como un signo de exclamación (!), un numeral (#), una arroba (@) o un paréntesis ().

- 10 En la página Seleccionar un tipo de implementación, seleccione **Instalar Platform Services Controller** y haga clic en **Siguiente**.
- 11 Cree un nuevo dominio de vCenter Single Sign-On o únase a un dominio existente y haga clic en **Siguiente**.

Opción	Descripción
Crear un nuevo dominio de Single Sign-On	<p>Crea un nuevo servidor vCenter Single Sign-On.</p> <ol style="list-style-type: none"> a Defina la contraseña para la cuenta de administrador de vCenter Single Sign-On. <p>Esta es la contraseña del usuario <code>administrator@su_nombre_de_dominio</code>, donde <code>su_nombre_de_dominio</code> es un nuevo dominio creado por vCenter Single Sign-On. Tras la instalación, puede iniciar sesión en vCenter Single Sign-On y en vCenter Server como <code>administrator@su_nombre_de_dominio</code>.</p> <ol style="list-style-type: none"> b Introduzca el nombre de dominio; por ejemplo, vsphere.local. c Introduzca el nombre del sitio para vCenter Single Sign-On. <p>El nombre del sitio es importante si utiliza vCenter Single Sign-On en varias ubicaciones. Seleccione su propio nombre para el sitio de vCenter Single Sign-On. No puede cambiar el nombre después de la instalación.</p> <p>Solo se admiten caracteres alfanuméricos y guiones (-).</p>
Unirse a un dominio de Single Sign-On en una instancia de Platform Services Controller existente	<p>Se une a un nuevo servidor vCenter Single Sign-On a un dominio de vCenter Single Sign-On en una instancia de Platform Services Controller existente. Debe proporcionar la información sobre el servidor vCenter Single Sign-On al que se va a unir el nuevo servidor vCenter Single Sign-On.</p> <ol style="list-style-type: none"> a Escriba el nombre de dominio completo (fully qualified domain name, FQDN) o la dirección IP de la instancia de Platform Services Controller que contiene el servidor vCenter Single Sign-On al que se va a unir. b Escriba la contraseña de la cuenta de administrador de vCenter Single Sign-On. c Escriba el puerto HTTPS que se va a usar para comunicarse con Platform Services Controller y haga clic en Siguiente. d Determine si desea crear un sitio de vCenter Single Sign-On o unirse a uno existente.

Si decide unirse a un dominio de vCenter Single Sign-On existente, se habilita la característica Enhanced Linked Mode. La instancia de Platform Services Controller replicará los datos de infraestructura con el servidor vCenter Single Sign-On que se unió.

- 12 En la página Seleccionar tamaño de la aplicación del asistente, haga clic en **Siguiente**.

Puede implementar una aplicación de Platform Services Controller con hasta 2 CPU y 2 GB de memoria.

- 13 En la lista de almacenes de datos disponibles, seleccione la ubicación en la que se almacenarán todos los archivos de configuración y discos virtuales de la máquina virtual. Opcionalmente, seleccione **Habilitar el modo de disco fino** para habilitar el aprovisionamiento fino.

- 14 En la página Configuración de red, establezca la configuración de red.

La dirección IP o el FQDN del dispositivo se utilizan como nombre del sistema. Se recomienda utilizar un FQDN. Sin embargo, si desea utilizar una dirección IP, utilice asignación de direcciones IP estáticas del dispositivo, ya que las direcciones IP que asigna DHCP podrían cambiar.

Opción	Acción
Elegir una red	<p>Seleccione la red a la que desea conectarse.</p> <p>Las redes que se muestran en el menú desplegable dependen de la configuración de red del servidor de destino. En el caso de la implementación directa de un dispositivo en un host ESXi, los grupos de puertos virtuales distribuidos que no son efímeros no se admiten y no se muestran en el menú desplegable.</p>
Familia de direcciones IP	<p>Seleccione la versión de IP del dispositivo.</p> <p>Puede seleccionar la versión IPv4 o IPv6.</p>
Tipo de red	<p>Seleccione cómo asignar la dirección IP del dispositivo.</p> <ul style="list-style-type: none"> ■ Estático <p>Se le pide que escriba la dirección IP y la configuración de red.</p> ■ DHCP <p>Los servidores DHCP se utilizan para asignar la dirección IP. Seleccione esta opción solo si hay un servidor DHCP disponible en el entorno.</p>
FQDN (opcional)	<p>Escriba un nombre de dominio completo (fully qualified domain name, FQDN) preferido del dispositivo.</p> <p>Nota Si decide utilizar IPv6 con el tipo de red DHCP, no verá la opción FQDN.</p>

Si utiliza una dirección IP como nombre del sistema, no puede modificarla ni actualizar la configuración de DNS después de la implementación.

- 15 Configure la hora del dispositivo y, como alternativa, seleccione **Habilitar SSH** para asegurar la conexión. A continuación, haga clic en **Siguiente**.

Opción	Descripción
Sincronizar la hora del dispositivo con el host ESXi	Habilita la sincronización horaria periódica y permite que VMware Tools establezca la hora del sistema operativo invitado para que sea la misma que la hora del host ESXi.
Usar servidores NTP (separados por comas)	Utiliza un servidor de protocolo de tiempo de red para sincronizar la hora. Si selecciona esta opción, debe escribir los nombres de los servidores NTP separados por comas.

- 16 Revise la página del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware y decida si desea unirse a él.

Para obtener más información sobre el CEIP, consulte la sección Configurar el Programa de mejora de la experiencia del cliente en *Administración de vCenter Server y hosts*.

- 17 En la página Listo para finalizar, revise la configuración de implementación de vCenter Server Appliance y haga clic en **Finalizar** para completar el proceso de implementación.

Pasos siguientes

Ahora puede implementar vCenter Server Appliance y conectarlo al dispositivo Platform Services Controller.

Implementación de vCenter Server Appliance

Implemente vCenter Server Appliance después de haber implementado la aplicación Platform Services Controller o haber instalado Platform Services Controller en una máquina virtual o servidor físico Windows.

Importante No se admiten implementaciones simultáneas vCenter Server Appliance. Si desea implementar muchas aplicaciones vCenter Server Appliance y registrarlas con la misma aplicación Platform Services Controller o Platform Services Controller, implemente vCenter Server Appliance una por una en secuencia.

Requisitos previos

- Compruebe que su sistema cumpla con los requisitos mínimos de hardware y software.
- Descargue el instalador de vCenter Server Appliance.
- Instale el complemento de integración de clientes.
- Compruebe que el host ESXi de destino en el que implementó vCenter Server Appliance no esté en modo de bloqueo o de mantenimiento.
- Compruebe si preparó la información de implementación correcta para la configuración de red. Conozca toda la información necesaria durante la implementación en el tema [Información necesaria para la implementación de vCenter Server Appliance](#).

- Si va a utilizar servidores NTP para sincronizar la hora, asegúrese de que la hora de los servidores NTP esté sincronizada con la del host ESXi.

Procedimiento

- 1 En el directorio del instalador del software, haga doble clic en **vcsa-setup.html**.
- 2 Espere tres segundos a que el explorador detecte el complemento de integración de clientes y permita que este se ejecute en el explorador cuando se le pida.
- 3 En la página de inicio, haga clic en **Instalar** para iniciar el asistente para implementación de vCenter Server Appliance.
- 4 Lea y acepte el contrato de licencia, y haga clic en **Siguiente**.
- 5 Conéctese al servidor de destino en el cual desea implementar vCenter Server Appliance y haga clic en **Siguiente**.
 - Puede conectarse a un host ESXi para implementar el dispositivo allí.
 - a Escriba el FQDN o la dirección IP del host ESXi.
 - b Escriba el nombre de usuario y la contraseña de un usuario que tenga privilegios administrativos en el host ESXi (por ejemplo, el usuario raíz).
 - Puede conectarse a una instancia de vCenter Server para implementar el dispositivo en un host o un clúster de DRS ESXi desde el inventario de vCenter Server.
 - a Escriba el nombre de dominio completo o la dirección IP de la instancia de vCenter Server.
 - b Escriba el nombre de usuario y la contraseña de un usuario que tenga privilegios administrativos en la instancia de vCenter Server, por ejemplo, el usuario `administrator@su_nombre_de_dominio`.
- 6 (opcional) Si recibe una advertencia de certificado, acéptela haciendo clic en **Sí**.
- 7 Si desea implementar vCenter Server Appliance en una instancia de vCenter Server, seleccione el centro de datos o la carpeta de centro de datos donde se encuentra el host ESXi o el clúster de DRS en el cual desea implementar el dispositivo y haga clic en **Siguiente**.

Nota Es necesario seleccionar un centro de datos o una carpeta de centro de datos que contenga al menos un host ESXi que no se encuentre en modo de bloqueo o de mantenimiento.

- 8 Si desea implementar vCenter Server Appliance en una instancia de vCenter Server, seleccione el grupo de recursos de un host ESXi o un clúster de DRS en el cual desea implementar el dispositivo y haga clic en **Siguiente**.

Nota Si selecciona un grupo de recursos de un clúster que no se encuentra en modo DRS, el asistente le pedirá que seleccione un host ESXi del clúster.

- 9 En la página Configurar máquina virtual, escriba el nombre de vCenter Server Appliance, establezca la contraseña para el usuario raíz y haga clic en **Siguiente**.

La contraseña debe contener al menos ocho caracteres, entre los cuales se debe incluir un número, letras mayúsculas y minúsculas, y un carácter especial, como un signo de exclamación (!), un numeral (#), una arroba (@) o un paréntesis (()).

- 10 En la página Seleccionar tipo de implementación, seleccione **Instalar vCenter Server** y haga clic en **Siguiente**.

- 11 Suministre el FQDN o la dirección IP de un Platform Services Controller ya instalado o implementado, introduzca la contraseña de vCenter Single Sign-On y haga clic en **Siguiente**.

Si instaló Platform Services Controller en Windows, proporcione el nombre del sistema del equipo host en la cual instaló Platform Services Controller.

- 12 En la página Seleccionar tamaño de la aplicación, seleccione el tamaño de vCenter Server Appliance según el tamaño del inventario de vSphere y, a continuación, haga clic en **Siguiente**.

Opción	Descripción
Muy pequeño (hasta 10 hosts y 100 máquinas virtuales)	Implementa un dispositivo con 2 CPU y 8 GB de memoria.
Pequeño (hasta 100 hosts y 1.000 máquinas virtuales)	Implementa un dispositivo con 4 CPU y 16 GB de memoria.
Mediano (hasta 400 hosts y 4.000 máquinas virtuales)	Implementa un dispositivo con 8 CPU y 24 GB de memoria.
Grande (hasta 1.000 hosts y 10.000 máquinas virtuales)	Implementa un dispositivo con 16 CPU y 32 GB de memoria.

- 13 En la lista de almacenes de datos disponibles, seleccione la ubicación en la que se almacenarán todos los archivos de configuración y discos virtuales de la máquina virtual. Opcionalmente, seleccione **Habilitar el modo de disco fino** para habilitar el aprovisionamiento fino.

14 Seleccione el tipo de base de datos que desee utilizar y haga clic en **Siguiente**.

Opción	Descripción
Usar una base de datos integrada (PostgreSQL)	Configura vCenter Server en el dispositivo para que utilice la base de datos integrada de PostgreSQL.
Usar una base de datos de Oracle	<p>Configura vCenter Server en el dispositivo para que utilice una base de datos externa de Oracle existente.</p> <ol style="list-style-type: none"> Escriba la dirección IP o el FQDN del equipo en el que está instalada la base de datos de Oracle. Escriba el puerto que se utilizará para comunicarse con la base de datos de Oracle. Introduzca el nombre de la instancia de base de datos. Escriba el nombre de usuario y la contraseña de la base de datos. <p>Importante Asegúrese de brindar las credenciales correctas. De lo contrario, la implementación podría presentar errores.</p>

15 En la página Configuración de red, establezca la configuración de red.

La dirección IP o el FQDN del dispositivo se utilizan como nombre del sistema. Se recomienda utilizar un FQDN. Sin embargo, si desea utilizar una dirección IP, utilice asignación de direcciones IP estáticas del dispositivo, ya que las direcciones IP que asigna DHCP podrían cambiar.

Opción	Acción
Elegir una red	<p>Seleccione la red a la que desea conectarse.</p> <p>Las redes que se muestran en el menú desplegable dependen de la configuración de red del servidor de destino. En el caso de la implementación directa de un dispositivo en un host ESXi, los grupos de puertos virtuales distribuidos que no son efímeros no se admiten y no se muestran en el menú desplegable.</p>
Familia de direcciones IP	<p>Seleccione la versión de IP del dispositivo.</p> <p>Puede seleccionar la versión IPv4 o IPv6.</p>
Tipo de red	<p>Seleccione cómo asignar la dirección IP del dispositivo.</p> <ul style="list-style-type: none"> ■ Estático <p>Se le pide que escriba la dirección IP y la configuración de red.</p> ■ DHCP <p>Los servidores DHCP se utilizan para asignar la dirección IP. Seleccione esta opción solo si hay un servidor DHCP disponible en el entorno.</p>
FQDN (opcional)	<p>Escriba un nombre de dominio completo (fully qualified domain name, FQDN) preferido del dispositivo.</p> <p>Nota Si decide utilizar IPv6 con el tipo de red DHCP, no verá la opción FQDN.</p>

Si utiliza una dirección IP como nombre del sistema, no puede modificarla ni actualizar la configuración de DNS después de la implementación.

- 16 Configure la hora del dispositivo y, como alternativa, seleccione **Habilitar SSH** para asegurar la conexión. A continuación, haga clic en **Siguiente**.

Opción	Descripción
Sincronizar la hora del dispositivo con el host ESXi	Habilita la sincronización horaria periódica y permite que VMware Tools establezca la hora del sistema operativo invitado para que sea la misma que la hora del host ESXi.
Usar servidores NTP (separados por comas)	Utiliza un servidor de protocolo de tiempo de red para sincronizar la hora. Si selecciona esta opción, debe escribir los nombres de los servidores NTP separados por comas.

- 17 En la página Listo para finalizar, revise la configuración de implementación de vCenter Server Appliance y haga clic en **Finalizar** para completar el proceso de implementación.
- 18 (opcional) Una vez finalizada la implementación, haga clic en el vínculo **https://vcenter_server_appliance_ip_address/vsphere-client** para iniciar vSphere Web Client e iniciar sesión en la instancia de vCenter Server en vCenter Server Appliance.
- 19 Haga clic en **Cerrar** para cerrar el asistente.

Solucionar problemas de instalación o implementación de vCenter Server

10

Los temas de solución de problemas de instalación o implementación de vCenter Server proporcionan soluciones a problemas que podrían surgir durante la instalación de vCenter Server o la implementación de vCenter Server Appliance.

Este capítulo incluye los siguientes temas:

- [Recopilar registros para solucionar problemas de una instalación o actualización de vCenter Server](#)
- [Instalar Platform Services Controller después de un error de instalación anterior](#)
- [Microsoft SQL Database configurado en modo de compatibilidad no admitido provoca errores en la instalación o actualización de vCenter Server](#)

Recopilar registros para solucionar problemas de una instalación o actualización de vCenter Server

Puede recopilar archivos de registro de instalación o actualización de vCenter Server. Si se produce un error en una instalación o actualización, la comprobación de los archivos de registro puede ayudar a identificar el origen del error.

Puede utilizar el asistente de instalación o el método manual para guardar y recuperar archivos de registro de vCenter Server en el caso de un error en la instalación de Windows.

También puede recopilar archivos de registro de implementación de vCenter Server Appliance.

- [Recopilar registros de instalación mediante el asistente de instalación](#)
Puede usar la página Configuración interrumpida del asistente de instalación para desplazarse hasta el archivo `.zip` generado de los archivos de registro de instalación de vCenter Server para Windows.
- [Recuperar registros de instalación de forma manual](#)
Puede recuperar manualmente los archivos de registro de instalación para examinarlos.
- [Recopilar archivos de registro de implementación para vCenter Server Appliance](#)
Si se produce algún error en la implementación de vCenter Server Appliance, puede recuperar los archivos del registro y analizarlos en busca del motivo del error.

■ Exportar un paquete de soporte de vCenter Server para solución de problemas

Si desea exportar el paquete de soporte de la instancia de vCenter Server en vCenter Server Appliance para solución de problemas, puede hacerlo mediante la URL que se muestra en la pantalla de inicio de DCUI.

Recopilar registros de instalación mediante el asistente de instalación

Puede usar la página Configuración interrumpida del asistente de instalación para desplazarse hasta el archivo .zip generado de los archivos de registro de instalación de vCenter Server para Windows.

Si se produce un error en la instalación, aparece la página Configuración interrumpida con las casillas de recopilación de registros seleccionadas de forma predeterminada.

Procedimiento

- 1 Deje las casillas activadas y haga clic en **Finalizar**.

Los archivos de instalación se recopilan en un archivo .zip en el escritorio, por ejemplo, `VMware-VCS-logs-time-of-installation-attempt.zip`, donde *time-of-installation-attempt* muestra el año, mes, fecha, hora, minutos y segundos del intento de instalación.

- 2 Recupere los archivos de registro del archivo .zip del escritorio.

Pasos siguientes

Analice los archivos de registro para determinar la causa del error.

Recuperar registros de instalación de forma manual

Puede recuperar manualmente los archivos de registro de instalación para examinarlos.

Procedimiento

- 1 Desplácese hasta las ubicaciones de los archivos de registro de instalación.

- El directorio `%PROGRAMDATA%\VMware\vCenterServer\logs`, generalmente `C:\ProgramData\VMware\vCenterServer\logs`
- El directorio `%TEMP%`, generalmente `C:\Users\username\AppData\Local\Temp`
Los archivos en el directorio `%TEMP%` incluyen `vminst.log`, `pkgmgr.log`, `pkgmgr-comp-msi.log` y `vim-vcs-msi.log`.

- 2 Abra los archivos de registro de la instalación en un editor de texto para su análisis.

Recopilar archivos de registro de implementación para vCenter Server Appliance

Si se produce algún error en la implementación de vCenter Server Appliance, puede recuperar los archivos del registro y analizarlos en busca del motivo del error.

La ruta de acceso completa de los archivos de registro aparece en el asistente de implementación de vCenter Server Appliance.

En caso de error en el primer arranque, puede descargar el paquete de soporte en un equipo host Windows y revisar los archivos de registro para determinar qué script de primera opción de arranque produjo el error. Consulte [Exportar un paquete de soporte de vCenter Server para solución de problemas](#).

Procedimiento

- 1 En la máquina Windows que usa para implementar vCenter Server Appliance, desplácese hasta la carpeta de los archivos de registro.

Si inició sesión como administrador, la carpeta predeterminada es

`C:\Users\Administrator\AppData\Local\VMware\CIP\vcsaInstaller.`

- 2 Abra los archivos de registro de la instalación en un editor de texto para su análisis.

Exportar un paquete de soporte de vCenter Server para solución de problemas

Si desea exportar el paquete de soporte de la instancia de vCenter Server en vCenter Server Appliance para solución de problemas, puede hacerlo mediante la URL que se muestra en la pantalla de inicio de DCUI.

También puede recopilar el paquete de soporte del shell de Bash de vCenter Server Appliance, mediante la ejecución del script `vc-support.sh`.

El paquete de soporte se exporta en formato `.tgz`.

Procedimiento

- 1 Inicie sesión en el equipo host de Windows en el que desea descargar el paquete.
- 2 Abra un explorador web y escriba la URL del paquete de soporte que se muestra en la DCUI.
`https://appliance-fully-qualified-domain-name:443/appliance/support-bundle`
- 3 Escriba el nombre de usuario y la contraseña del usuario raíz.

- 4 Haga clic en **Entrar**.

El paquete de soporte se descarga como archivo `.tgz` en su equipo Windows.

- 5 (opcional) Para determinar cuál fue el script de primer arranque que generó un error, examine el archivo `firstbootStatus.json`.

Si ejecutó el script `vc-support.sh` en el shell de Bash de vCenter Server Appliance, para examinar el archivo `firstbootStatus.json`, ejecute

```
cat /var/log/firstboot/firstbootStatus.json
```

Instalar Platform Services Controller después de un error de instalación anterior

Cuando desee replicar los datos de Platform Services Controller, es posible que no pueda asociar un dominio de vCenter Single Sign-On a una instancia de Platform Services Controller existente.

Problema

Al intentar instalar una instancia de Platform Services Controller, ya sea integrada o externa, y asociar Platform Services Controller a un dominio o sitio de vCenter Single Sign-On, la instalación puede producir un error y este error puede dejar datos incompletos en la federación de Platform Services Controller.

Causa

Los datos de Platform Services Controller no se depuran cuando se produce un error en una instalación de Platform Services Controller. Considere la siguiente situación:

- 1 Instale Platform Services Controller A.
- 2 Al intentar instalar Platform Services Controller B y asociarlo al mismo dominio que Platform Services Controller A, se produce un error en la instalación.
- 3 El segundo intento de instalar Platform Services Controller B y asociarlo al mismo dominio que Platform Services Controller A falla, debido a que Platform Services Controller A contiene datos incompletos.

Solución

- 1 Inicie sesión como administrador en la máquina en la que desea instalar Platform Services Controller A.
- 2 En la línea de comandos, diríjase al comando `vdcleavefed`.

El comando `vdcleavefed` está ubicado en `C:\Archivos de programa\VMware\vCenter Server\vmmdir\` en Windows y `/usr/lib/vmware-vmmdir/bin/` en Linux.

- 3 Ejecute el comando `vdcleavefed` para eliminar los datos.

```
vdcleavefed -h Platform-Services-Controller-B-System-Name -u Administrator
```

- 4 Instale Platform Services Controller B.

Microsoft SQL Database configurado en modo de compatibilidad no admitido provoca errores en la instalación o actualización de vCenter Server

Se produce un error en la instalación de vCenter Server con una base de datos de Microsoft SQL cuando la base de datos está configurada en modo de compatibilidad con una versión no compatible.

Problema

Aparece el siguiente mensaje de error: El usuario de base de datos ingresado no tiene los permisos necesarios para instalar y configurar vCenter Server con la base de datos seleccionada. Corrija los siguientes errores: %s

Causa

La versión de la base de datos debe ser compatible para vCenter Server. En el caso de SQL, aunque la base de datos sea de una versión compatible, si se configura para que se ejecute en modo de compatibilidad con una versión no compatible, se produce este error. Por ejemplo, si SQL 2008 está configurada para que ejecute el modo de compatibilidad de SQL 2000, se presenta este error.

Solución

- ◆ Asegúrese de que la base de datos de vCenter Server sea de una versión compatible y no esté configurada en el modo de compatibilidad con una versión no compatible. Consulte las matrices de interoperabilidad de productos VMware en http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

Después de instalar vCenter Server o implementar vCenter Server Appliance

11

Después de instalar vCenter Server o implementar vCenter Server Appliance, tenga en cuenta estas opciones posteriores a la instalación antes de agregarle inventario a vCenter Server para que lo administre.

Este capítulo incluye los siguientes temas:

- [Iniciar sesión en vCenter Server con vSphere Web Client](#)
- [Recopilar archivos de registro de vCenter Server](#)
- [Instalar o actualizar vSphere Authentication Proxy](#)
- [Desinstalar vCenter Server](#)
- [Redirigir vCenter Server a otra instancia de Platform Services Controller externa](#)
- [Reconfigurar una instancia de vCenter Server independiente con una instancia de Platform Services Controller integrada en un vCenter Server con una instancia de Platform Services Controller externa](#)
- [Reconfigurar varias instancias combinadas de vCenter Server con una instancia de Platform Services Controller integrada en vCenter Server con una instancia de Platform Services Controller externa](#)

Iniciar sesión en vCenter Server con vSphere Web Client

Inicie sesión en vCenter Server con vSphere Web Client para administrar su inventario de vSphere.

Requisitos previos

Si quiere usar vCenter Server 5.0 con vSphere Web Client, compruebe que el sistema vCenter Server 5.0 esté registrado en vSphere Web Client.

Si quiere usar vCenter Server 5.1 o vCenter Server 5.5 con vSphere Web Client, compruebe que vCenter Server esté instalado y que tanto vCenter Server como vSphere Web Client apunten a la misma instancia de vCenter Single Sign-On.

En vSphere 6.0, vSphere Web Client se instala como parte de vCenter Server en Windows o la implementación de vCenter Server Appliance. De esta manera, vSphere Web Client siempre apunta a la misma instancia de vCenter Single Sign-On.

Procedimiento

- 1 Abra un explorador web e introduzca la dirección URL de vSphere Web Client: `https://vcenter_server_ip_address_or_fqdn/vsphere-client` o `https://vcenter_server_ip_address_or_fqdn:9443`.
- 2 Introduzca las credenciales de un usuario que tenga permisos en vCenter Server y haga clic en **Iniciar sesión**.
- 3 Si aparece un mensaje de advertencia acerca de un certificado SSL que no es de confianza, seleccione la acción correcta según su directiva de seguridad.

Opción	Acción
Omita la advertencia de seguridad para esta sesión de inicio de sesión solamente.	Haga clic en Omitir .
Omita la advertencia de seguridad para esta sesión de inicio de sesión e instale el certificado predeterminado para que la advertencia no vuelva a aparecer.	<p>Seleccione Instalar este certificado y no mostrar ninguna advertencia de seguridad para este servidor y haga clic en Omitir.</p> <p>Seleccione esta opción solamente si al usar el certificado predeterminado no se presenta un problema de seguridad en el entorno.</p>
Cancele e instale un certificado firmado antes de continuar.	Haga clic en Cancelar y asegúrese de que esté instalado un certificado firmado en el sistema de vCenter Server antes de intentar volver a conectarse.

Resultados

vSphere Web Client conecta todos los sistemas devCenter Server para los que el usuario especificado tiene permisos, y así permite ver y administrar el inventario.

Recopilar archivos de registro de vCenter Server

Después de instalar vCenter Server, puede recopilar los archivos de registro de vCenter Server para el diagnóstico y la solución de problemas.

Nota Este procedimiento brinda información sobre cómo recopilar los archivos de registro para la instalación de Windows de vCenter Server. Para obtener información sobre cómo exportar un paquete de soporte y examinar los archivos de registro en vCenter Server Appliance, consulte *Configuración de vCenter Server Appliance*.

Procedimiento

- 1 Inicie sesión como administrador en la máquina con Windows en la que está instalado vCenter Server.
- 2 Genere el paquete de registros.
 - Desplácese hasta **Inicio > Programas > VMware > Generar paquete de registros de vCenter Server**.

Puede generar paquetes de registros de vCenter Server incluso si no puede conectar con vCenter Server a través de vSphere Web Client.

- En el símbolo del sistema, desplácese hasta `installation_directory\VMware\vCenter Server\bin` y ejecute el comando `vc-support.bat`.

Resultados

Los archivos de registro para el sistema vCenter Server se generan y se almacenan en un archivo `.tgz` en su escritorio.

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.

Pasos siguientes

Configure ESXi para que use vSphere Authentication Proxy para unirse a un dominio. Consulte la documentación de *Seguridad de vSphere*.

Desinstalar vCenter Server

Debe tener privilegios de administrador para desinstalar VMware vCenter Server.

Importante Si va a utilizar la base de datos PostgreSQL integrada, la desinstalación de vCenter Server hará que se desinstale la base de datos integrada y se perderán todos los datos.

Requisitos previos

Si va a desinstalar el sistema vCenter Server, elimine los hosts del inventario de hosts y clústeres.

Procedimiento

- 1 Como usuario administrador en el sistema Windows, haga clic en **Inicio > Panel de control > Programas y características**.
- 2 Seleccione **VMware vCenter Server** en la lista y haga clic en **Quitar**.
- 3 Haga clic en **Quitar** para confirmar que desea eliminar el programa.
- 4 Haga clic en **Finalizar**.
- 5 Reinicie el sistema.

Redirigir vCenter Server a otra instancia de Platform Services Controller externa

La unión de las instancias de Platform Services Controller externas en el mismo dominio de vCenter Single Sign-On garantiza la alta disponibilidad del sistema.

Si una instancia externa de Platform Services Controller deja de responder o si se desea distribuir la carga de una instancia externa de Platform Services Controller, es posible volver a apuntar las instancias de vCenter Server a otra instancia de Platform Services Controller dentro del mismo dominio y sitio.

- Puede redirigir la instancia de vCenter Server a una instancia de Platform Services Controller funcional existente que tenga la capacidad de carga libre en el mismo dominio y el mismo sitio.
- Puede instalar o implementar una nueva instancia de Platform Services Controller en el mismo dominio y el mismo sitio a los que redirigirá la instancia vCenter Server.

Requisitos previos

- Si la instancia de Platform Services Controller antigua no responde, quite el nodo y limpie los datos obsoletos de vmdir mediante la ejecución del comando `cmsso-util unregister`. Para obtener información sobre la retirada de una instancia de Platform Services Controller, consulte <https://kb.vmware.com/kb/2106736>.
- Compruebe que la instancia antigua y la nueva de Platform Services Controller estén en el mismo dominio y sitio de vCenter Single Sign-On mediante la ejecución del comando `vdcrepadmin -f showservers`. Para obtener información sobre el uso del comando, consulte <https://kb.vmware.com/kb/2127057>.

Procedimiento

- 1 Inicie sesión en la instancia de vCenter Server.
 - Para una instancia de vCenter Server Appliance, inicie sesión en el shell de vCenter Server Appliance como raíz.
 - Para una instancia de vCenter Server en Windows, inicie sesión como administrador en la máquina virtual o el servidor físico de vCenter Server.
- 2 Si la instancia de vCenter Server se ejecuta en Windows, abra el símbolo del sistema de este sistema operativo y desplácese hasta `C:\Archivos de programa\VMware\vCenter Server\bin`.
- 3 Ejecute el comando `cmsso-util repoint`.

```
cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
```

donde los corchetes ([]) encierran las opciones del comando.

Aquí, *psc_fqdn_or_static_ip* es el nombre de sistema utilizado para identificar la instancia de Platform Services Controller. El nombre de este sistema debe ser un FQDN o una dirección IP estática.

Nota El valor de FQDN distingue entre mayúsculas y minúsculas.

Utilice la opción `--dc-port port_number` si la instancia de Platform Services Controller se ejecuta en un puerto HTTPS personalizado. El valor predeterminado del puerto HTTPS es 443.

- 4 Inicie sesión en la instancia de vCenter Server mediante vSphere Web Client para comprobar que vCenter Server esté en ejecución y pueda administrarse.

Resultados

La instancia de vCenter Server está registrada con la nueva instancia de Platform Services Controller.

Reconfigurar una instancia de vCenter Server independiente con una instancia de Platform Services Controller integrada en un vCenter Server con una instancia de Platform Services Controller externa

Si implementó o instaló una instancia de vCenter Server independiente con una instancia de Platform Services Controller integrada y desea ampliar el dominio de vCenter Single Sign-On con más instancias de vCenter Server, puede reconfigurar y redireccionar la instancia de vCenter Server existente a una instancia de Platform Services Controller externa.

Figura 11-1. Reconfiguración de una instancia de vCenter Server independiente con una instancia de Platform Services Controller integrada y redireccionamiento a una instancia de Platform Services Controller externa

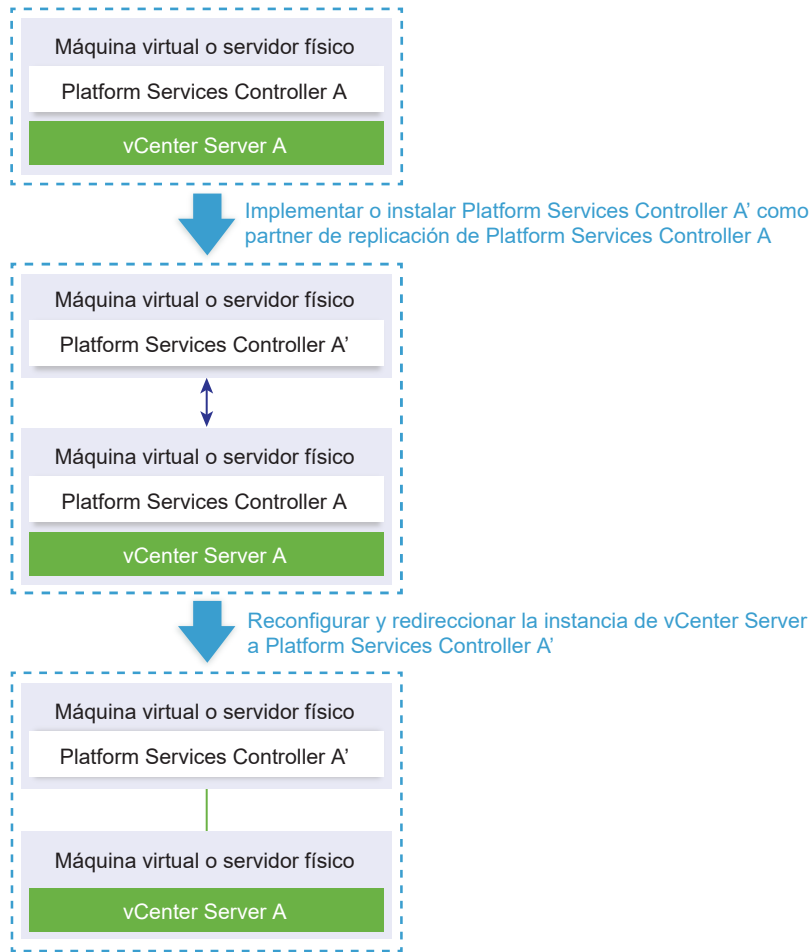


Tabla 11-1. Leyenda

Flecha o línea	Descripción
	Acuerdo de replicación entre dos instancias de Platform Services Controller
	Registro de vCenter Server en una instancia de Platform Services Controller externa
	Paso de transición

Nota La reconfiguración de una instancia de vCenter Server con una instancia de Platform Services Controller integrada y el redireccionamiento a una instancia de Platform Services Controller externa es un proceso de un solo sentido después del cual no se puede volver a cambiar a vCenter Server con una instancia de Platform Services Controller integrada.

Requisitos previos

- Implemente o instale la instancia de Platform Services Controller externa como partner de replicación de la instancia de Platform Services Controller integrada existente en el mismo sitio de vCenter Single Sign-On.

Nota Puede determinar el sitio de vCenter Single Sign-On actual mediante el comando `vmfad-cli`.

- En el caso de una instancia de vCenter Server Appliance con una instancia de Platform Services Controller integrada, inicie sesión en el shell del dispositivo como raíz y ejecute el comando.

```
/usr/lib/vmware-vmafd/bin/vmafd-cli get-site-name --server-name localhost
```

- Para una instalación de Windows de una instancia de vCenter Server con una instancia de Platform Services Controller integrada, inicie sesión en el equipo Windows como administrador, abra el símbolo del sistema de Windows y ejecute el comando.

```
C:\Program Files\VMware\vCenter Server\vmafdd\vmafd-cli get-site-name --server-name localhost
```

- Cree snapshots de vCenter Server con una instancia de Platform Services Controller integrada y una instancia de Platform Services Controller externa, de manera que pueda revertir a los snapshots si la reconfiguración produce errores.

Procedimiento

- 1 Inicie sesión en la instancia de vCenter Server con una instancia de Platform Services Controller integrada.

Opción	Pasos
Para un vCenter Server Appliance con una instancia de Platform Services Controller integrada	<p>Inicie sesión en el shell del dispositivo como raíz.</p> <ul style="list-style-type: none"> ■ Si tiene acceso directo a la consola del dispositivo, presione Alt+F1. ■ Si desea conectarse de forma remota, utilice SSH u otra conexión de consola remota para iniciar una sesión en el dispositivo.
Para una instalación de Windows de vCenter Server con una instancia de Platform Services Controller integrada	Inicie sesión en el equipo Windows como administrador.

- 2 Compruebe que todos los servicios de Platform Services Controller estén en ejecución.

Opción	Pasos
Para un vCenter Server Appliance con una instancia de Platform Services Controller integrada	Ejecute el comando <code>service-control --status --all</code> .
Para una instalación de Windows de vCenter Server con una instancia de Platform Services Controller integrada	Seleccione Inicio > Panel de control > Herramientas administrativas > Servicios .

Los servicios de Platform Services Controller que deben ejecutarse son VMware License Service, VMware Identity Management Service, VMware Security Token Service, VMware Certificate Service y VMware Directory Service.

- 3 Si vCenter Server con una instancia de Platform Services Controller integrada se ejecuta en Windows, abra el símbolo del sistema de Windows y desplácese hasta `C:\Archivos de programa\VMware\vCenter Server\bin`.
- 4 Ejecute el comando `cmsso-util reconfigure`.

```
cmsso-util reconfigure --repoint-psc psc_fqdn_or_static_ip --username username --
domain-name domain_name --passwd password [--dc-port port_number]
```

donde los corchetes [] encierran elementos opcionales.

Aquí, *psc_fqdn_or_static_ip* representa el nombre del sistema utilizado para identificar la instancia de Platform Services Controller externa. El nombre de este sistema debe ser un FQDN o una dirección IP estática.

Nota El valor de FQDN distingue entre mayúsculas y minúsculas.

Las opciones *username* y *password* son el nombre de usuario y la contraseña del administrador de vCenter Single Sign-On *domain_name*.

Utilice la opción `--dc-port` si la instancia de Platform Services Controller externa se ejecuta en un puerto HTTPS personalizado. El valor predeterminado del puerto HTTPS es 443.

Por ejemplo, si la instancia de Platform Services Controller externa se ejecuta en un puerto HTTPS 449 personalizado, debe ejecutar:

```
cmsso-util reconfigure --repoint-psc psc.acme.local --username administrator --
domain-name vsphere.local --passwd Password1! --dc-port 449
```

- 5 Inicie sesión en la instancia de vCenter Server mediante vSphere Web Client para comprobar que vCenter Server esté en ejecución y pueda administrarse.

Resultados

vCenter Server con una instancia de Platform Services Controller integrada se disminuye de nivel, y vCenter Server se direcciona a una instancia de Platform Services Controller externa.

Pasos siguientes

Puede implementar o instalar instancias de vCenter Server y Platform Services Controller adicionales en el dominio de vCenter Single Sign-On.

Reconfigurar varias instancias combinadas de vCenter Server con una instancia de Platform Services Controller integrada en vCenter Server con una instancia de Platform Services Controller externa

Si implementó o instaló dos o más instancias combinadas de vCenter Server con una instancia de Platform Services Controller integrada, puede reconfigurarlas como varias instancias de vCenter Server que usan instancias combinadas de Platform Services Controller externas.

Figura 11-2. Ejemplo de reconfiguración de tres instancias combinadas de vCenter Server con una instancia de Platform Services Controller integrada en dos sitios de vCenter Single Sign-On

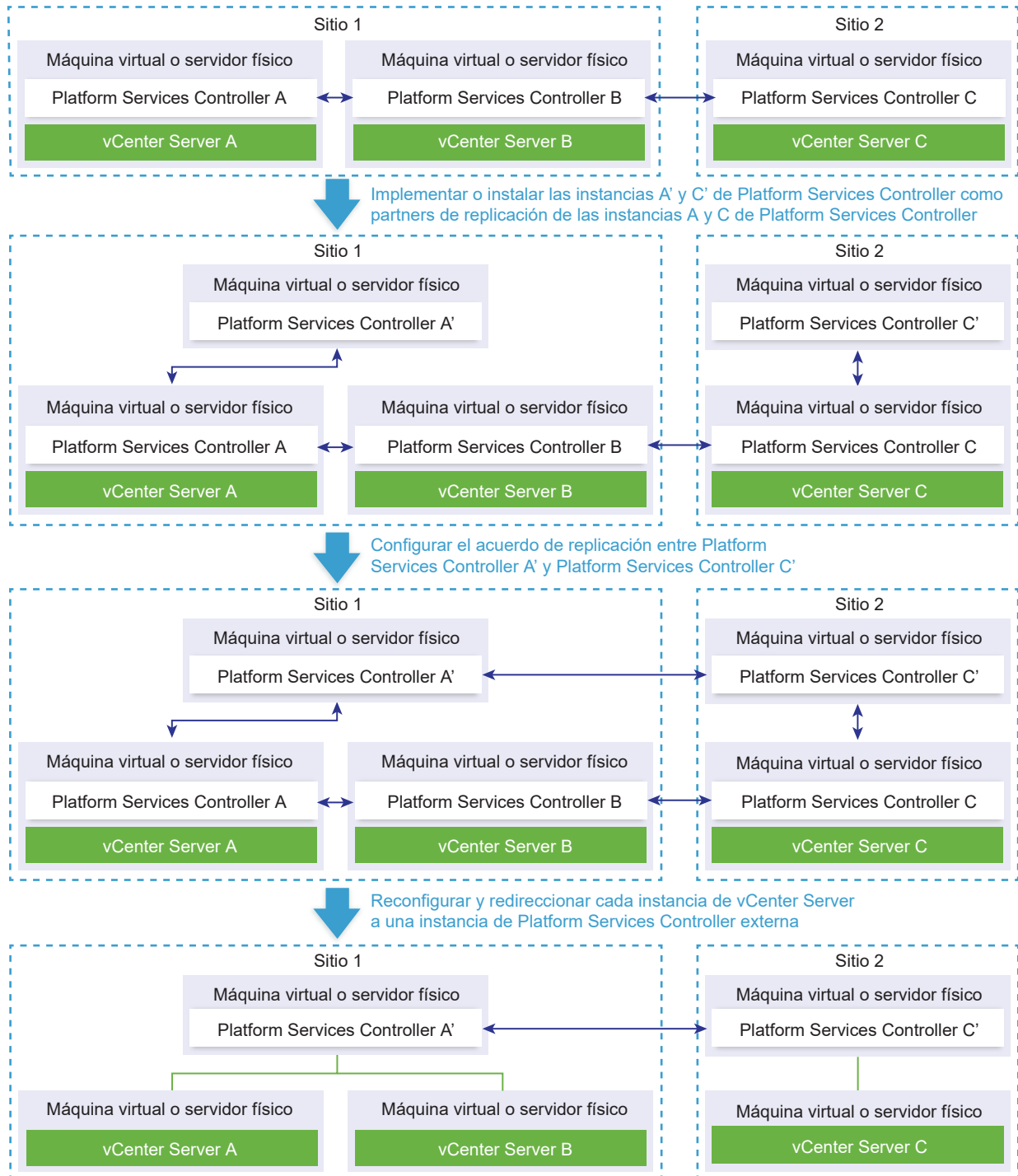





Tabla 11-2. Leyenda

Flecha o línea	Descripción
	Acuerdo de replicación entre dos instancias de Platform Services Controller
	Registro de vCenter Server en una instancia de Platform Services Controller externa
	Paso de transición

Nota La reconfiguración de una instancia de vCenter Server con una instancia de Platform Services Controller integrada y el redireccionamiento a una instancia de Platform Services Controller externa es un proceso de un solo sentido después del cual no se puede volver a cambiar a vCenter Server con una instancia de Platform Services Controller integrada.

Requisitos previos

- Para cada sitio de vCenter Single Sign-On, implemente o instale una instancia de Platform Services Controller externa como partner de replicación de una instancia de Platform Services Controller integrada existente del sitio.

Nota Puede determinar los sitios de vCenter Single Sign-On actuales mediante el comando `vmfad-cli`.

- En el caso de una instancia de vCenter Server Appliance con una instancia de Platform Services Controller integrada, inicie sesión en el shell del dispositivo como raíz y ejecute el comando.

```
/usr/lib/vmware-vmafd/bin/vmafd-cli get-site-name --server-name localhost
```

- Para una instalación de Windows de una instancia de vCenter Server con una instancia de Platform Services Controller integrada, inicie sesión en el equipo Windows como administrador, abra el símbolo del sistema de Windows y ejecute el comando.

```
C:\Program Files\VMware\vCenter Server\vmafdd\vmafd-cli get-site-name --server-name localhost
```

- Puede crear snapshots de las instancias de vCenter Server con una instancia de Platform Services Controller integrada y las instancias de Platform Services Controller externas, de manera que pueda revertir a los snapshots si se producen errores en la reconfiguración.

Procedimiento

1 Comprobar que los servicios de las instancias de Platform Services Controller integradas estén en ejecución

Para asegurar un redireccionamiento correcto de una instancia de vCenter Server desde una instancia de Platform Services Controller integrada hasta una instancia externa, todos los servicios de la instancia de Platform Services Controller integrada existente deben estar en ejecución.

2 Configurar el acuerdo de replicación entre todas las instancias de Platform Services Controller externas

Tras implementar o instalar una instancia externa de Platform Services Controller de replicación en cada sitio de vCenter Single Sign-On, debe combinar todas las instancias de Platform Services Controller externas en un acuerdo de replicación.

3 Reconfigurar cada instancia de vCenter Server y redireccionarla de una instancia integrada de Platform Services Controller a una externa

Con la reconfiguración, se disminuye el nivel de cada instancia integrada de Platform Services Controller y se redirecciona la instancia de vCenter Server para utilizar una instancia externa de Platform Services Controller.

Comprobar que los servicios de las instancias de Platform Services Controller integradas estén en ejecución

Para asegurar un redireccionamiento correcto de una instancia de vCenter Server desde una instancia de Platform Services Controller integrada hasta una instancia externa, todos los servicios de la instancia de Platform Services Controller integrada existente deben estar en ejecución.

Procedimiento

1 Inicie sesión en una instancia de vCenter Server con una instancia de Platform Services Controller integrada.

Opción	Pasos
Para un vCenter Server Appliance con una instancia de Platform Services Controller integrada	<p>Inicie sesión en el shell del dispositivo como raíz.</p> <ul style="list-style-type: none"> ■ Si tiene acceso directo a la consola del dispositivo, presione Alt+F1. ■ Si desea conectarse de forma remota, utilice SSH u otra conexión de consola remota para iniciar una sesión en el dispositivo.
Para una instalación de Windows de vCenter Server con una instancia de Platform Services Controller integrada	Inicie sesión en el equipo Windows como administrador.

- 2 Compruebe que todos los servicios de Platform Services Controller estén en ejecución.

Opción	Pasos
Para un vCenter Server Appliance con una instancia de Platform Services Controller integrada	Ejecute el comando <code>service-control --status --all</code> .
Para una instalación de Windows de vCenter Server con una instancia de Platform Services Controller integrada	Seleccione Inicio > Panel de control > Herramientas administrativas > Servicios .

Los servicios de Platform Services Controller que deben ejecutarse son VMware License Service, VMware Identity Management Service, VMware Security Token Service, VMware Certificate Service y VMware Directory Service.

- 3 Repita este procedimiento para cada instancia de vCenter Server con una instancia de Platform Services Controller integrada.

Configurar el acuerdo de replicación entre todas las instancias de Platform Services Controller externas

Tras implementar o instalar una instancia externa de Platform Services Controller de replicación en cada sitio de vCenter Single Sign-On, debe combinar todas las instancias de Platform Services Controller externas en un acuerdo de replicación.

Figura 11-3. Ejemplo de configuración del acuerdo de replicación entre dos instancias externas de Platform Services Controller en diferentes sitios de vCenter Single Sign-On

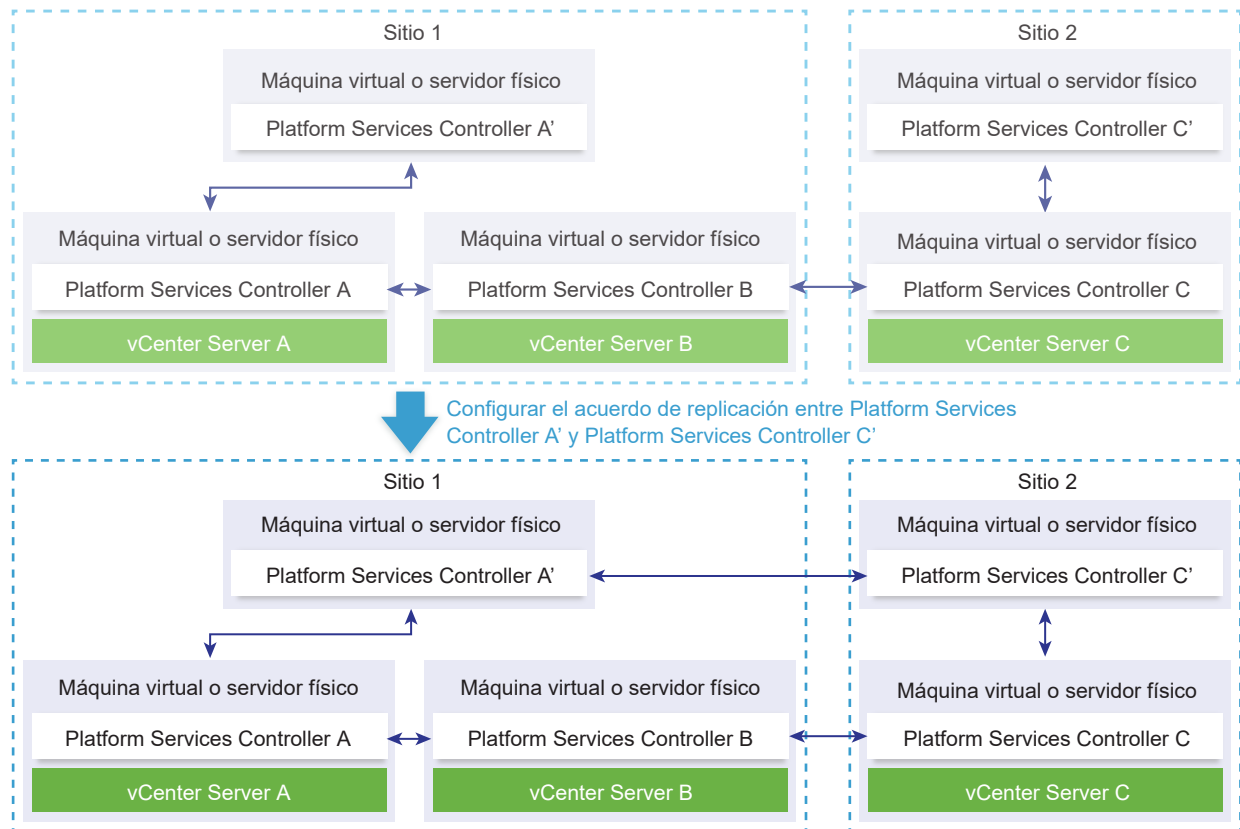





Tabla 11-3. Leyenda

Flecha o línea	Descripción
	Acuerdo de replicación entre dos instancias de Platform Services Controller
	Registro de vCenter Server en una instancia de Platform Services Controller externa
	Paso de transición

Para configurar el acuerdo de replicación entre dos instancias de Platform Services Controller, puede usar una conexión con cualquiera de las instancias de vCenter Server o Platform Services Controller desde el dominio de vCenter Single Sign-On.

Procedimiento

- 1 Establezca una conexión con una instancia de vCenter Server o Platform Services Controller desde el dominio de vCenter Single Sign-On.

Opción	Pasos
Si desea establecer una conexión con un vCenter Server Appliance o un dispositivo de Platform Services Controller:	<p>Inicie sesión en el shell de Bash del dispositivo como raíz.</p> <ol style="list-style-type: none"> 1 Iniciar sesión en el shell del dispositivo <ul style="list-style-type: none"> ■ Si tiene acceso directo a la consola del dispositivo, presione Alt+F1. ■ Si desea conectarse de forma remota, utilice SSH u otra conexión de consola remota para iniciar una sesión en el dispositivo. 2 Habilitar el shell de Bash <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <pre>shell.set --enabled true</pre> </div> 3 Ejecute el comando <code>shell</code>.
Si desea conectar con una instalación de Windows de vCenter Server o Platform Services Controller:	<p>Inicie sesión en el equipo Windows como administrador y abra el símbolo del sistema de Windows.</p>

- 2 Ejecute el comando `vdcrepadmin` con el parámetro `showpartners` en una instancia de Platform Services Controller externa.

Determine las relaciones existentes de la instancia de Platform Services Controller con otras instancias de Platform Services Controller en el dominio de vCenter Single Sign-On.

- Si usa una conexión con vCenter Server Appliance o un dispositivo de Platform Services Controller, ejecute el siguiente comando.

```
/usr/lib/vmware-vmtoolsd/bin/vdcrepadmin -f showpartners -h psc_fqdn_or_static_ip -u administrator
```

- Si usa una conexión con una instalación de Windows de vCenter Server o Platform Services Controller, ejecute el siguiente comando.

```
C:\Program Files\VMware\vCenter Server\vmware-vmdir\bin\vdcrepadmin -f
showpartners -h psc_fqdn_or_static_ip -u administrator
```

Cuando se le requiera, introduzca la contraseña de administrador de vCenter Single Sign-On.

- 3 Repita el paso 2 en cada instancia de Platform Services Controller externa.

Determinó las relaciones existentes entre todas las instancias de Platform Services Controller en el dominio de vCenter Single Sign-On.

- 4 Si hay una instancia de Platform Services Controller externa que no se incluye en un acuerdo de replicación con otra instancia de Platform Services Controller externa, ejecute el comando `vdcrepadmin` con el parámetro `createagreement` en dicha instancia de Platform Services Controller para combinarla con otra instancia de Platform Services Controller externa.

- Si usa una conexión con vCenter Server Appliance o un dispositivo de Platform Services Controller, ejecute el siguiente comando.

```
/usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement -2 -h
psc_fqdn_or_static_ip -H partner_psc_fqdn_or_static_ip -u administrator
```

- Si usa una conexión con una instalación de Windows de vCenter Server o Platform Services Controller, ejecute el siguiente comando.

```
C:\Program Files\VMware\vCenter Server\vmware-vmdir\bin\vdcrepadmin -f
createagreement -2 -h psc_fqdn_or_static_ip -H partner_psc_fqdn_or_static_ip -u
administrator
```

Cuando se le requiera, introduzca la contraseña de administrador de vCenter Single Sign-On.

Creó una relación entre las dos instancia de Platform Services Controller.

- 5 Repita el paso 4 en cada instancia de Platform Services Controller externa que no se haya incluido en un acuerdo de replicación con otra instancia de Platform Services Controller externa.
- 6 Repita los pasos 2 y 3 para comprobar que configuró una topología de relaciones en anillo de las instancias de Platform Services Controller externas.

Reconfigurar cada instancia de vCenter Server y redireccionarla de una instancia integrada de Platform Services Controller a una externa

Con la reconfiguración, se disminuye el nivel de cada instancia integrada de Platform Services Controller y se redirecciona la instancia de vCenter Server para utilizar una instancia externa de Platform Services Controller.

Figura 11-4. Ejemplo de reconfiguración de tres instancias combinadas de vCenter Server con una instancia integrada de Platform Services Controller y redireccionamiento de esas instancias a instancias externas de Platform Services Controller

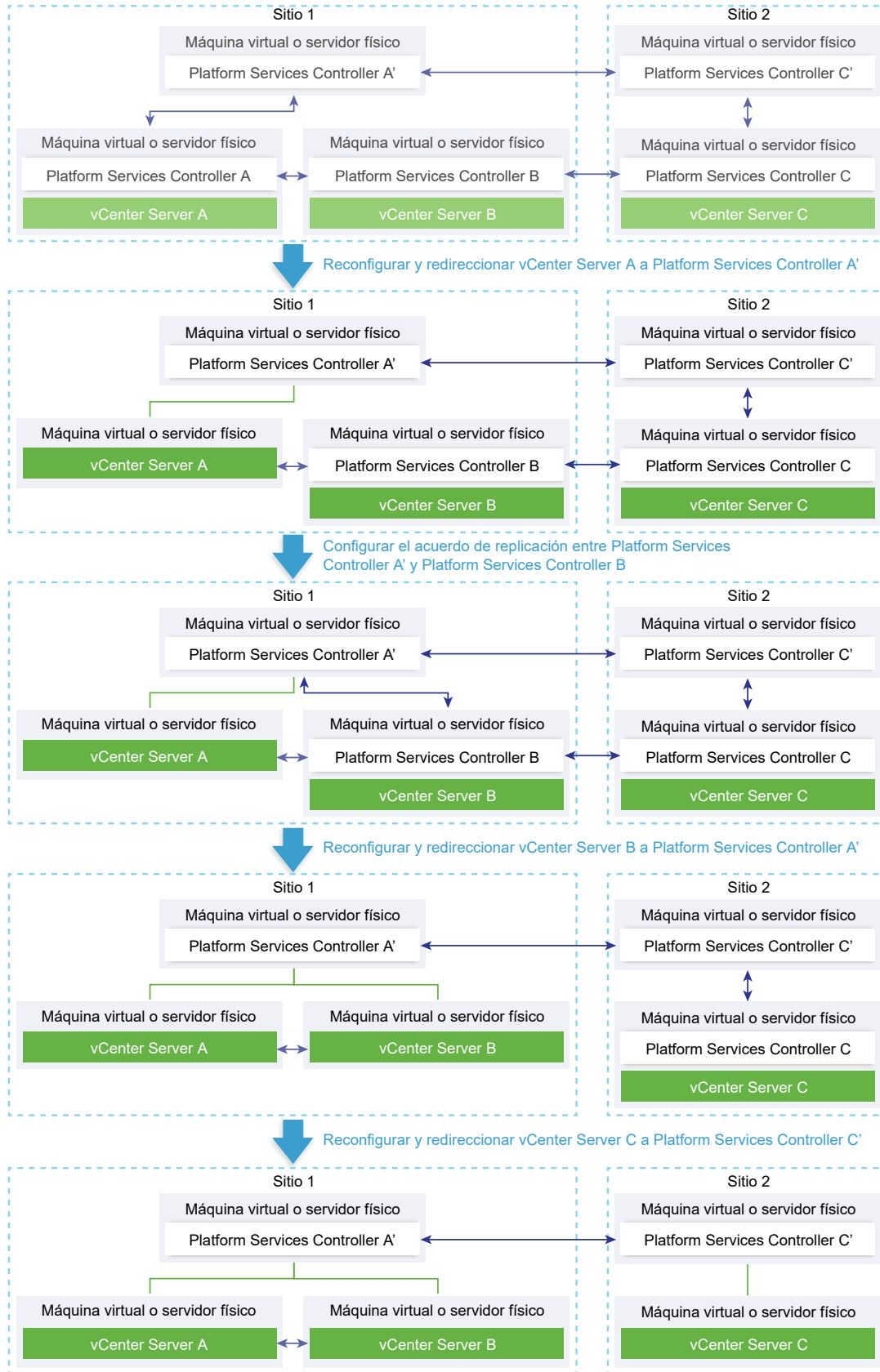





Tabla 11-4. Leyenda

Flecha o línea	Descripción
	Acuerdo de replicación entre dos instancias de Platform Services Controller
	Registro de vCenter Server en una instancia de Platform Services Controller externa
	Paso de transición

Procedimiento

- 1 Inicie sesión en la instancia de vCenter Server con una instancia de Platform Services Controller integrada.

Opción	Pasos
Para un vCenter Server Appliance con una instancia de Platform Services Controller integrada	<p>Inicie sesión en el shell del dispositivo como raíz.</p> <ul style="list-style-type: none"> ■ Si tiene acceso directo a la consola del dispositivo, presione Alt+F1. ■ Si desea conectarse de forma remota, utilice SSH u otra conexión de consola remota para iniciar una sesión en el dispositivo.
Para una instalación de Windows de vCenter Server con una instancia de Platform Services Controller integrada	Inicie sesión en el equipo Windows como administrador.

- 2 Si vCenter Server con una instancia integrada de Platform Services Controller y la instancia externa de Platform Services Controller no son partners de replicación directos, cree un acuerdo de replicación de ese tipo.

- Para un dispositivo vCenter Server Appliance con una instancia integrada de Platform Services Controller, en el shell de Bash del dispositivo, ejecute el siguiente comando.

```
/usr/lib/vmware-vmware/bin/vdcrepadmin -f createagreement -h localhost -H
psc_fqdn_or_static_ip -u administrator
```

- Para una instalación en Windows de vCenter Server con una instancia integrada de Platform Services Controller, en el símbolo del sistema de Windows, ejecute el siguiente comando.

```
C:\Program Files\VMware\vCenter Server\vmware-vmware\bin\vdcrepadmin -f
createagreement -h localhost -H psc_fqdn_or_static_ip -u administrator
```

Cuando se le requiera, introduzca la contraseña de administrador de vCenter Single Sign-On.

- 3 Si vCenter Server con una instancia integrada de Platform Services Controller se ejecuta en Windows, en el símbolo del sistema de Windows, desplácese hasta C:\Archivos de programa\VMware\vCenter Server\bin.

4 Ejecute el comando `cmsso-util reconfigure`.

```
cmsso-util reconfigure --repoint-psc psc_fqdn_or_static_ip --username username --  
domain-name domain_name --passwd password [--dc-port port_number]
```

donde los corchetes [] encierran elementos opcionales.

Aquí, *psc_fqdn_or_static_ip* representa el nombre del sistema utilizado para identificar la instancia de Platform Services Controller externa. El nombre de este sistema debe ser un FQDN o una dirección IP estática.

Nota El valor de FQDN distingue entre mayúsculas y minúsculas.

Las opciones *username* y *password* son el nombre de usuario y la contraseña del administrador de vCenter Single Sign-On *domain_name*.

Utilice la opción `--dc-port` si la instancia de Platform Services Controller externa se ejecuta en un puerto HTTPS personalizado. El valor predeterminado del puerto HTTPS es 443.

Por ejemplo, si la instancia de Platform Services Controller externa se ejecuta en un puerto HTTPS 449 personalizado, debe ejecutar:

```
cmsso-util reconfigure --repoint-psc psc.acme.local --username administrator --  
domain-name vsphere.local --passwd Password1! --dc-port 449
```

- 5 Inicie sesión en la instancia de vCenter Server mediante vSphere Web Client para comprobar que vCenter Server esté en ejecución y pueda administrarse.
- 6 Repita este procedimiento para cada instancia de vCenter Server con una instancia de Platform Services Controller integrada.

Resultados

Se disminuye el nivel de las instancias de vCenter Server con una instancia de Platform Services Controller integrada, y las instancias de vCenter Server se redireccionan a las instancias de Platform Services Controller externas.

Hacer copias de seguridad del entorno de vCenter Server y restaurar

12

Puede utilizar vSphere Data Protection o un producto de otro proveedor integrado con VMware vSphere Storage APIs - Data Protection para hacer copias de seguridad y restaurar una máquina virtual (VM) que contenga vCenter Server, un vCenter Server Appliance o un Platform Services Controller.

vSphere Data Protection es una solución de copia de seguridad y recuperación suministrada por EMC. vSphere Data Protection se integra completamente con vCenter Server y permite administrar los trabajos de copia de seguridad y, al mismo tiempo, almacenar las copias de seguridad en ubicaciones de almacenamiento de destino deduplicadas. Después de implementar y configurar vSphere Data Protection, puede acceder a vSphere Data Protection mediante la interfaz de vSphere Web Client para seleccionar, programar, configurar y administrar copias de seguridad y recuperaciones de máquinas virtuales. Durante la copia de seguridad, vSphere Data Protection crea una instantánea en modo inactivo para la máquina virtual. La deduplicación se ejecuta de manera automática con cada copia de seguridad.

En vSphere 6.0, para hacer una copia de seguridad y una restauración de una máquina virtual que contiene vCenter Server vCenter Server Appliance o Platform Services Controller, debe hacer una copia de seguridad de la imagen completa. Además, la máquina virtual debe cumplir con los siguientes requisitos:

- VMware Tools debe estar instalado y en ejecución en la máquina virtual.
- La máquina virtual debe utilizar un nombre de dominio completo (FQDN) con una resolución de DNS correcta o debe configurarse con una dirección IP estática.

Las siguientes operaciones de copia de seguridad y recuperación no son compatibles:

- Copias de seguridad incrementales
- Copias de seguridad diferenciales
- Copias de seguridad de discos individuales
- Máquinas virtuales con instantáneas
- Máquinas virtuales configuradas con Fault Tolerance

También se puede utilizar vSphere Data Protection para restaurar una máquina virtual que contiene una instancia de vCenter Server o Platform Services Controller directamente en el host ESXi que ejecuta vSphere Data Protection Appliance cuando el servicio de vCenter Server deja de estar disponible o cuando no se puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

Alternativamente a vSphere Data Protection puede utilizar productos de otros proveedores integrados con VMware vSphere Storage APIs - Data Protection para hacer copias de seguridad y restaurar una máquina virtual que contenga vCenter Server, un vCenter Server Appliance o un Platform Services Controller.

VMware vSphere Storage APIs - Data Protection es un marco de protección de datos que habilita las copias de seguridad de los productos para realizar copias de seguridad centralizadas, efectivas, fuera del host y sin utilizar la red LAN de las máquinas virtuales vSphere. Para obtener información acerca de VMware vSphere Storage APIs - Data Protection, visite el sitio web de VMware. Para obtener información acerca de la integración de productos de copia de seguridad con VMware vSphere Storage APIs - Data Protection, póngase en contacto con su proveedor de copias de seguridad.

La sección [Flujo de trabajo general de vSphere Data Protection](#) incluye tareas básicas de vSphere Data Protection. Las secciones [Hacer copias de seguridad de vCenter Server con una instancia de Platform Services Controller integrada y restaurar](#), [Hacer copias de seguridad del entorno de vCenter Server con una instancia externa única de Platform Services Controller y restaurarlas](#) y [Hacer copias de seguridad del entorno de vCenter Server con varias instancias de Platform Services Controller y restaurarlo](#) proporcionan flujos de trabajo detallados sobre cómo hacer copias de seguridad y restauraciones del entorno según el tipo de implementación y la cantidad de instancias de Platform Services Controller.

Este capítulo incluye los siguientes temas:

- [Flujo de trabajo general de vSphere Data Protection](#)
- [Hacer copias de seguridad de vCenter Server con una instancia de Platform Services Controller integrada y restaurar](#)
- [Hacer copias de seguridad del entorno de vCenter Server con una instancia externa única de Platform Services Controller y restaurarlas](#)
- [Hacer copias de seguridad del entorno de vCenter Server con varias instancias de Platform Services Controller y restaurarlo](#)

Flujo de trabajo general de vSphere Data Protection

Para hacer una copia de seguridad y una restauración de una máquina virtual que contiene instancias de vCenter Server, vCenter Server Appliance o Platform Services Controller, debe implementar y configurar vSphere Data Protection y, a continuación, realizar las tareas básicas de copia de seguridad y restauración.

Implementación de la plantilla de OVF de vSphere Data Protection

Implemente vSphere Data Protection para realizar una copia de seguridad y restaurar una máquina virtual que contiene vCenter Server o vCenter Server Appliance.

Nota Este procedimiento se completa utilizando vSphere Data Protection 6.0. Si utiliza una versión diferente de vSphere Data Protection, los pasos a seguir pueden variar.

Requisitos previos

- Compruebe que la versión de ESXi sea 5.0 o posterior.
- Si hay un firewall habilitado en el entorno, compruebe que el puerto 902 esté abierto para la comunicación entre vSphere Data Protection Appliance y el host ESXi. Consulte la documentación de *vSphere Data Protection*.
- Compruebe que el complemento de integración de clientes de VMware esté instalado en el explorador. Para obtener más información, consulte [Instalar el complemento de integración de clientes](#).
- Utilice vSphere Web Client para iniciar sesión como administrador en la instancia de vCenter Server que administra su entorno.

Procedimiento

- 1 Seleccione **vCenter > Centros de datos**.
- 2 En la pestaña **Objetos**, haga clic en **Acciones** y seleccione **Implementar plantilla de OVF**.
- 3 Desplácese hasta la ubicación del archivo `.ova` de vSphere Data Protection Appliance y haga clic en **Abrir**.
- 4 Compruebe los detalles de la plantilla de OVF y haga clic en **Siguiente**.
- 5 Revise los detalles de la plantilla, haga clic en **Siguiente** y siga los avisos del asistente para aceptar el contrato de licencia.
- 6 En la página Seleccionar nombre y carpeta, introduzca un FQDN para vSphere Data Protection Appliance, seleccione la carpeta o el centro de datos en los que desea implementar vSphere Data Protection Appliance y haga clic en **Siguiente**.

La configuración de vSphere Data Protection usa el nombre que se introduce para buscar vSphere Data Protection Appliance en el inventario de vCenter Server. No cambie el nombre de vSphere Data Protection Appliance después de la instalación.
- 7 Seleccione el host en el que desea implementar vSphere Data Protection Appliance y haga clic en **Siguiente**.
- 8 Seleccione el formato de disco virtual y la ubicación de almacenamiento de vSphere Data Protection Appliance y haga clic en **Siguiente**.
- 9 Seleccione la red de destino de vSphere Data Protection Appliance y haga clic en **Siguiente**.

- 10 En la página Personalizar plantilla, especifique la configuración de la red, como la puerta de enlace predeterminada, el DNS, la dirección IP de la red y la máscara de red, y haga clic en **Siguiente**.

Confirme que las direcciones IP sean correctas y que coincidan con el valor introducido para el servidor DNS. Si introduce direcciones IP incorrectas, deberá volver a implementar vSphere Data Protection Appliance.

Nota vSphere Data Protection Appliance no es compatible con DHCP. Se requiere una dirección IP estática.

- 11 En la página Listo para finalizar, confirme que todas las opciones de implementación sean correctas, seleccione **Encender después de la implementación** y haga clic en **Finalizar**.

Resultados

Se inicia el proceso de implementación de vSphere Data Protection Appliance y vSphere Data Protection Appliance arranca en modo de instalación.

Pasos siguientes

Establezca las opciones de configuración inicial de vSphere Data Protection. Consulte [Configuración de vSphere Data Protection](#).

Configuración de vSphere Data Protection

Durante la configuración inicial de vSphere Data Protection, puede ajustar la configuración de red y la información de zona horaria para vSphere Data Protection Appliance. Puede utilizar el asistente **Configuración de vSphere Data Protection** para registrar vSphere Data Protection Appliance con vCenter Server.

Nota Este procedimiento se completa utilizando vSphere Data Protection 6.0. Si utiliza una versión diferente de vSphere Data Protection, los pasos a seguir pueden variar.

Requisitos previos

- Implemente vSphere Data Protection Appliance.
- Lea la *Guía de administración de vSphere Data Protection* para acceder a la lista completa de pasos para configurar vSphere Data Protection.
- Compruebe que exista espacio suficiente en el disco en el almacén de datos. Cuando se ejecuta una prueba de análisis de rendimiento opcional durante la configuración inicial de la aplicación, se requieren 41 GB para cada disco en cada almacén de datos. Si el espacio disponible es insuficiente, la prueba informa un valor de 0 para todas las pruebas de lectura, escritura y búsqueda, y muestra un estado final de espacio insuficiente.
- Utilice vSphere Web Client para iniciar sesión como administrador en la instancia de vCenter Server que administra su entorno.

Procedimiento

- 1 En vSphere Web Client, seleccione **Listas de inventario de vCenter > Máquinas virtuales**.

- 2 Haga clic con el botón derecho en vSphere Data Protection Appliance y seleccione **Abrir consola**.

Después de que se carguen los archivos de instalación, se mostrará la pantalla de bienvenida para el menú de vSphere Data Protection.

- 3 En un explorador web, diríjase a la dirección URL de vSphere Data Protection Configuration Utility.

`https://ip_address_VDP_Appliance:8543/vdp-configure/`

- 4 Inicie sesión como raíz.

La contraseña predeterminada es changeme.

Se abrirá el asistente **Configuración de vSphere Data Protection**.

- 5 En la página Configuración de red del asistente, introduzca o confirme la información de red y servidor para vSphere Data Protection Appliance y haga clic en **Siguiente**.

Asegúrese de que los valores se completen de forma correcta. De lo contrario, se producirá un error en la configuración inicial.

- 6 Seleccione la zona horaria apropiada para vSphere Data Protection Appliance y haga clic en **Siguiente**.

- 7 En la página Credenciales de VDP, seleccione una nueva contraseña raíz para la aplicación virtual y haga clic en **Siguiente**.

- 8 En la página Registro de vCenter, registre la aplicación con vCenter Server:

- a En el cuadro de texto **Nombre de usuario de vCenter**, introduzca un nombre de usuario administrador de vCenter Server. Por ejemplo, **administrator@vsphere.local**.

Si el usuario pertenece a una cuenta de dominio, introduzca el nombre de usuario con el formato *DOMAIN\UserName*.

Importante Si introduce el nombre de usuario de administrador de vCenter Single Sign-On con el formato de nombre principal de usuario (UPN), las tareas relacionadas con las operaciones de vSphere Data Protection no aparecerán en el panel Tareas recientes de vSphere Web Client. Si desea utilizar el nombre de usuario de administrador de vCenter Single Sign-On, introduzca el nombre de usuario de vCenter Single Sign-On con el formato UPN.

- b En el cuadro de texto **Contraseña de vCenter**, introduzca la contraseña de vCenter Server.
- c Introduzca una dirección IP o FQDN de vCenter.

- d (Requerido) Cambie el puerto HTTP predeterminado de vCenter Server.

Introduzca un valor personalizado para el puerto HTTP si debe conectarse a vCenter Server a través del puerto HTTP, en lugar del puerto HTTPS, que se utiliza para todas las otras comunicaciones.

- e Introduzca un puerto HTTPS de vCenter (el puerto predeterminado es 443).

- f Seleccione la casilla **Utilizar vCenter para la autenticación SSO**.

- g (opcional) Haga clic en **Probar conexión**.

Aparecerá un mensaje de conexión exitosa. Si este mensaje no aparece, resuelva los problemas de su configuración y repita este paso hasta que aparezca un mensaje exitoso.

- 9 Haga clic en **Siguiente** y responda los mensajes del asistente para completar la configuración.

Pasos siguientes

Cree un trabajo de copia de seguridad con una directiva de retención y una programación de copia de seguridad específicos. Para obtener más información, consulte [Crear un trabajo de copia de seguridad en vSphere Data Protection](#).

Crear un trabajo de copia de seguridad en vSphere Data Protection

Es posible crear trabajos de copia de seguridad para asociar la copia de seguridad de un conjunto de una o más máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller con una programación de copias de seguridad y directivas de retención específicas.

Nota Este procedimiento se completa utilizando vSphere Data Protection 6.0. Si utiliza una versión diferente de vSphere Data Protection, los pasos a seguir pueden variar.

Requisitos previos

- Implemente y configure vSphere Data Protection Appliance.
- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.
- 2 En el menú **Acciones del trabajo de copia de seguridad**, seleccione **Nuevo** para ejecutar el asistente **Crear nuevo trabajo de copia de seguridad**.
- 3 En la página Tipo de trabajo, seleccione **Imágenes de invitado** y haga clic en **Siguiente**.
- 4 En la página Tipo de datos, seleccione **Imagen completa** y haga clic en **Siguiente**.

Puede ver todos los objetos y máquinas virtuales del inventario de vCenter Server.

- 5 En la página Destinos de copia de seguridad, seleccione la máquina virtual que contiene la instancia de vCenter Server o Platform Services Controller de la que desea crear una copia de seguridad y haga clic en **Siguiente**.
- 6 En la página Programación, seleccione la programación para el trabajo de copia de seguridad y haga clic en **Siguiente**.
- 7 En la página Directiva de retención, seleccione un período de retención y haga clic en **Siguiente**.

Nota Cuando introduzca un período de mantenimiento nuevo que siga a la caducidad de una copia de seguridad, vSphere Data Protection Appliance elimina su referencia a los datos de la copia de seguridad y no podrá restaurar la copia de seguridad caducada. vSphere Data Protection Appliance determina si cualquier otro punto de restauración utiliza los datos de la copia de seguridad y, si el sistema determina que no se han utilizado, los datos se eliminan y la capacidad del disco estará disponible.

- 8 En la página Nombre, introduzca un nombre para el trabajo de copia de seguridad y haga clic en **Siguiente**.
- 9 En la página Listo para completar, examine la información de resumen del trabajo de copia de seguridad y haga clic en **Finalizar**.

El trabajo de copia de seguridad recientemente creado aparecerá incluido en una lista en la pestaña **Copia de seguridad**. El trabajo de copia de seguridad se iniciará automáticamente según la programación configurada.

Pasos siguientes

- Ejecute ahora un trabajo de copia de seguridad existente. Para obtener más información, consulte [Iniciar un trabajo de copia de seguridad de forma manual](#).
- Restaure una instancia de copia de seguridad de vCenter Server, vCenter Server Appliance o Platform Services Controller. Para obtener más información, consulte [Restaurar el entorno de vCenter Server](#).

Iniciar un trabajo de copia de seguridad de forma manual

Una operación de copia de seguridad se inicia automáticamente de acuerdo con la programación de fecha, hora y frecuencia configuradas en el trabajo de copia de seguridad. Si desea ejecutar un trabajo de copia de seguridad existente de inmediato, puede iniciar este proceso de forma manual.

Nota Este procedimiento se completa utilizando vSphere Data Protection 6.0. Si utiliza una versión diferente de vSphere Data Protection, los pasos a seguir pueden variar.

Requisitos previos

- Implemente y configure vSphere Data Protection Appliance.

- Cree un trabajo de copia de seguridad. Consulte [Crear un trabajo de copia de seguridad en vSphere Data Protection](#).
- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.
- 2 En la pestaña **Copia de seguridad**, seleccione el trabajo de copia de seguridad que desea ejecutar.
- 3 Haga clic en **Realizar copia de seguridad ahora** y seleccione **Realizar copia de seguridad de todas las fuentes**.

Un cuadro de diálogo confirma que la operación de copia de seguridad se inició correctamente.

Pasos siguientes

Restaure la copia de seguridad de un vCenter Server, vCenter Server Appliance o Platform Services Controller. Para obtener más información, consulte [Restaurar el entorno de vCenter Server](#).

Restaurar el entorno de vCenter Server

Después de hacer una copia de seguridad de una máquina virtual que contiene vCenter Server, vCenter Server Appliance o Platform Services Controller, es posible restaurar las imágenes de copia de seguridad a la ubicación original o a una nueva.

Para restaurar las máquinas virtuales a la ubicación original, sobrescriba la máquina virtual con copia de seguridad o cree una que contenga la instancia restaurada de vCenter Server, vCenter Server Appliance o Platform Services Controller en el mismo host ESXi. También puede restaurar las VM en un nuevo host de ESXi.

Importante No se admite restaurar máquinas virtuales que tengan instantáneas.

Puede restaurar la VM en el host de ESXi que ejecuta vSphere Data Protection Appliance. La operación de restauración de emergencia directa a host permite restaurar la máquina virtual cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de vSphere Data Protection mediante vSphere Web Client.

■ [Restaurar una máquina virtual a la ubicación original](#)

Es posible restaurar copias de seguridad de imágenes completas de máquinas virtuales que contienen vCenter Server, vCenter Server Appliance o Platform Services Controller de forma manual mediante el asistente **Restaurar copia de seguridad**.

- [Restaurar una máquina virtual en una nueva ubicación](#)

Puede restaurar copias de seguridad de imágenes completas mediante el asistente **Restaurar copia de seguridad**.

- [Restaurar una máquina virtual con la operación de restauración de emergencia directa a host](#)

La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene vCenter Server, vCenter Server Appliance o Platform Services Controller cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

Restaurar una máquina virtual a la ubicación original

Es posible restaurar copias de seguridad de imágenes completas de máquinas virtuales que contienen vCenter Server, vCenter Server Appliance o Platform Services Controller de forma manual mediante el asistente **Restaurar copia de seguridad**.

Nota Este procedimiento se completa utilizando vSphere Data Protection 6.0. Si utiliza una versión diferente de vSphere Data Protection, los pasos a seguir pueden variar.

Requisitos previos

- Implemente y configure vSphere Data Protection Appliance.
- Haga una copia de seguridad de una máquina virtual con instancias de vCenter Server, vCenter Server Appliance o Platform Services Controller en ejecución. Consulte [Crear un trabajo de copia de seguridad en vSphere Data Protection](#).
- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.
- Compruebe que la máquina virtual que desea restaurar esté apagada.

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.
- 2 Haga clic en la pestaña **Restaurar**.
- 3 (opcional) Filtre las copias de seguridad para acotar la búsqueda.
- 4 Seleccione una máquina virtual de las que se enumeran en la columna Nombre y, a continuación, elija uno o más elementos de copia de seguridad que desee restaurar.

Al seleccionar una máquina virtual, puede ver la lista de las copias de seguridad realizadas para esa máquina.
- 5 Haga clic en **Restaurar** para iniciar el asistente **Restaurar copia de seguridad**.
- 6 En la página Seleccionar copia de seguridad, compruebe que la lista de copias de seguridad sea correcta, quite las copias de seguridad que desee excluir de la operación de restauración y haga clic en **Siguiente**.

- 7 En la página Establecer opciones de restauración, deje seleccionada la casilla **Restaurar a la ubicación original**.

Importante Si el disco virtual de la VM original se ha extraído o eliminado, no podrá restaurar la máquina virtual a su ubicación original. El disco de la máquina virtual (VMDK) deberá restaurarse a una ubicación nueva.

- 8 (opcional) En **Opciones avanzadas**, seleccione un almacén de datos nueva para encender la VM después de que se restaure y reconecte a la NIC.
- 9 Haga clic en **Siguiente**.
- 10 En la página Listo para completar, examine el resumen de sus solicitudes de restauración y haga clic en **Finalizar** para iniciar la operación de restauración.

Nota Si en [Paso 8](#) se seleccionó la reconexión con la NIC durante el proceso de restauración, compruebe que la configuración de red de la máquina virtual recientemente creada sea correcta. La NIC de la VM nueva puede utilizar la misma dirección IP que la máquina virtual original, lo que provoca conflictos.

Resultados

Un cuadro de diálogo de información confirma que la operación de restauración se inició correctamente. Puede supervisar el progreso de la restauración en el panel Tareas recientes.

Restaurar una máquina virtual en una nueva ubicación

Puede restaurar copias de seguridad de imágenes completas mediante el asistente **Restaurar copia de seguridad**.

Nota Este procedimiento se completa utilizando vSphere Data Protection 6.0. Si utiliza una versión diferente de vSphere Data Protection, los pasos a seguir pueden variar.

Requisitos previos

- Implemente y configure vSphere Data Protection Appliance.
- Haga una copia de seguridad de una máquina virtual con instancias de vCenter Server, vCenter Server Appliance o Platform Services Controller en ejecución. Consulte [Crear un trabajo de copia de seguridad en vSphere Data Protection](#).
- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.
- Compruebe que la máquina virtual que desea restaurar esté apagada.

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.
- 2 Haga clic en la pestaña **Restaurar**.

- 3 (opcional) Filtre las copias de seguridad para acotar la búsqueda.
- 4 Seleccione una máquina virtual de las que se enumeran en la columna Nombre y, a continuación, elija uno o más elementos de copia de seguridad que desee restaurar.

Al seleccionar una máquina virtual, puede ver la lista de las copias de seguridad realizadas para esa máquina.
- 5 Haga clic en **Restaurar** para iniciar el asistente **Restaurar copia de seguridad**.
- 6 En la página Seleccionar copia de seguridad, compruebe que la lista de copias de seguridad sea correcta, quite las copias de seguridad que desee excluir de la operación de restauración y haga clic en **Siguiente**.
- 7 En la página Establecer opciones de restauración, deselectione la casilla **Restaurar a la ubicación original** para establecer las opciones de restauración de cada copia de seguridad que esté restaurando a una ubicación nueva.
- 8 Introduzca el nombre de la VM nueva y haga clic en **Seleccionar** para seleccionar un host nuevo para la máquina virtual restaurada.
- 9 Seleccione el almacén de datos en el que desea restaurar la máquina virtual y haga clic en **Siguiente**.
- 10 (opcional) En **Opciones avanzadas**, seleccione un almacén de datos nueva para encender la VM después de que se restaure y reconecte a la NIC.
- 11 Haga clic en **Siguiente**.
- 12 En la página Listo para completar, examine el resumen de sus solicitudes de restauración y haga clic en **Finalizar** para iniciar la operación de restauración.

Nota Si en [Paso 10](#) seleccionó la opción para volver a conectar la NIC durante el proceso de restauración, confirme la configuración de red de la máquina virtual recientemente creada. La NIC de la VM nueva puede utilizar la misma dirección IP que la máquina virtual original, lo que provoca conflictos.

Resultados

Un cuadro de diálogo de información confirma que la operación de restauración se inició correctamente. Puede supervisar el progreso de la restauración en el panel Tareas recientes.

Restaurar una máquina virtual con la operación de restauración de emergencia directa a host

La restauración de emergencia directa a host permite restaurar la máquina virtual que contiene vCenter Server, vCenter Server Appliance o Platform Services Controller cuando vCenter Server deja de estar disponible o cuando el usuario no puede acceder a la interfaz de usuario de vSphere Data Protection mediante vSphere Web Client.

vSphere Data Protection depende de vCenter Server para muchas de las operaciones esenciales de vSphere Data Protection. Cuando vCenter Server deja de estar disponible, una operación de restauración de emergencia puede restaurar la máquina virtual que contiene vCenter Server, vCenter Server Appliance o Platform Services Controller directamente en el host ESXi que ejecuta vSphere Data Protection Appliance. La pestaña **Restauración de emergencia** muestra una lista de máquinas virtuales que cuentan con copias de seguridad realizadas por vSphere Data Protection Appliance. Estas máquinas virtuales que contienen instancias de vCenter Server o Platform Services Controller pueden restaurarse como nuevas máquinas virtuales en el host ESXi donde se está ejecutando vSphere Data Protection Appliance. Para conocer las prácticas recomendadas, las recomendaciones y las limitaciones de la operación de restauración de emergencia, consulte la documentación de *vSphere Data Protection*.

Nota Este procedimiento se completa utilizando vSphere Data Protection 6.0. Si utiliza una versión diferente de vSphere Data Protection, los pasos a seguir pueden variar.

Procedimiento

- 1 Inicie sesión como administrador en vSphere Client y haga clic en la pestaña **Resumen**.
 - a En Administración de host, seleccione **Desasociar host de vCenter Server**.
 - b Haga clic en **Sí** cuando se le solicite desasociar el host vCenter Server.
- 2 En un explorador web, desplácese hasta la utilidad de configuración de vSphere Data Protection.
https://ip_address_VDP_Appliance:8543/vdp-configure/.
- 3 En la pestaña **Restauración de emergencia**, seleccione la máquina virtual que servirá como punto de restauración y haga clic en **Restaurar**.
- 4 En el cuadro de diálogo Credenciales de host, ingrese credenciales de host válidas y haga clic en **Aceptar**.
- 5 En el cuadro de diálogo Restaurar una copia de seguridad, especifique un nombre nuevo.
- 6 Seleccione un almacén de datos como destino para la copia de seguridad y haga clic en **Restaurar**.

Precaución Se enumera el tamaño de capacidad del almacén de datos. Asegúrese de seleccionar un almacén de datos con suficiente espacio en disco para admitir la restauración. Si no hay espacio suficiente, fallará la restauración.

- 7 En el panel Tareas recientes, controle el avance para comprobar que la restauración se envíe correctamente.

Nota La máquina virtual restaurada aparece en el inventario en el nivel de host vSphere. No se admite la restauración en una ruta de acceso de inventario más específica.

Hacer copias de seguridad de vCenter Server con una instancia de Platform Services Controller integrada y restaurar

El entorno puede estar compuesto por vCenter Server o vCenter Server Appliance con una instancia de Platform Services Controller integrada. Puede utilizar vSphere Data Protection para hacer una copia de seguridad y una restauración de un entorno de vCenter Server con una instancia de Platform Services Controller integrada.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

El flujo de trabajo para hacer copias de seguridad de vCenter Server con una instancia de Platform Services Controller integrada y restaurar incluye las siguientes tareas:

- 1 Implemente vSphere Data Protection Appliance.
Consulte [Implementación de la plantilla de OVF de vSphere Data Protection](#).
- 2 Complete la configuración inicial de vSphere Data Protection.
Consulte [Configuración de vSphere Data Protection](#).
- 3 Haga copias de seguridad basadas en imagen de todas las instancias de vCenter Server.
Consulte [Crear un trabajo de copia de seguridad en vSphere Data Protection](#).
- 4 (Opcional) Para ejecutar un trabajo de copia de seguridad actual de inmediato, inicie el proceso de forma manual.
Consulte [Iniciar un trabajo de copia de seguridad de forma manual](#).
- 5 Restaure la instancia con errores de vCenter Server mediante uno de los métodos disponibles:
 - Restaure una máquina virtual en la ubicación original.
Consulte [Restaurar una máquina virtual a la ubicación original](#).
 - Restaure una máquina virtual en una nueva ubicación.
Consulte [Restaurar una máquina virtual en una nueva ubicación](#).
 - Restaure una máquina virtual directamente en el host ESXi que ejecuta vSphere Data Protection Appliance si el servicio de vCenter Server deja de estar disponible o si no puede acceder a la interfaz de usuario de vSphere Data Protection al utilizar vSphere Web Client.
Consulte [Restaurar una máquina virtual con la operación de restauración de emergencia directa a host](#).
- 6 Encienda la máquina virtual que contiene la instancia restaurada de vCenter Server.

Hacer copias de seguridad del entorno de vCenter Server con una instancia externa única de Platform Services Controller y restaurarlas

Es posible que el entorno consista en varias instancias de vCenter Server que se registran con una sola instancia de Platform Services Controller. Se puede utilizar vSphere Data Protection para hacer una copia de seguridad y una restauración de la máquina virtual que contiene Platform Services Controller. También se puede utilizar vSphere Data Protection para hacer copias de seguridad y restauraciones de máquinas virtuales que contienen instancias de vCenter Server o de vCenter Server Appliance que se registran con una sola instancia de Platform Services Controller externa.

Nota Si se generan errores en las instancias de vCenter Server y Platform Services Controller al mismo tiempo, primero debe restaurar las instancias de Platform Services Controller y después las de vCenter Server.

- **Hacer copias de seguridad de Platform Services Controller y restaurarlo**

Es posible instalar e implementar Platform Services Controller, así como registrar varias instancias de vCenter Server con la misma instancia de Platform Services Controller. Es posible utilizar vSphere Data Protection para hacer una copia de seguridad y una restauración del entorno si la instancia de Platform Services Controller externa genera errores.

- **Copia de seguridad y restauración de vCenter Server**

Es posible instalar e implementar Platform Services Controller, así como registrar varias instancias de vCenter Server con la misma instancia de Platform Services Controller. Puede utilizar vSphere Data Protection para hacer copias de seguridad de todo el entorno y restaurarlo, de modo que si alguna de las instancias de vCenter Server presenta errores, sea posible restaurar la instancia de vCenter Server con errores.

Hacer copias de seguridad de Platform Services Controller y restaurarlo

Es posible instalar e implementar Platform Services Controller, así como registrar varias instancias de vCenter Server con la misma instancia de Platform Services Controller. Es posible utilizar vSphere Data Protection para hacer una copia de seguridad y una restauración del entorno si la instancia de Platform Services Controller externa genera errores.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

1 Implemente vSphere Data Protection Appliance.

Consulte [Implementación de la plantilla de OVF de vSphere Data Protection](#).

- 2 Complete la configuración inicial de vSphere Data Protection.

Consulte [Configuración de vSphere Data Protection](#).

- 3 Haga copias de seguridad basadas en imagen de la instancia de Platform Services Controller externa y de todas las instancias de vCenter Server.

Consulte [Crear un trabajo de copia de seguridad en vSphere Data Protection](#).

Nota Haga copias de seguridad de todas las instancias de vCenter Server y Platform Services Controller simultáneamente.

- 4 (Opcional) Para ejecutar un trabajo de copia de seguridad actual de inmediato, inicie el proceso de forma manual.

Consulte [Iniciar un trabajo de copia de seguridad de forma manual](#).

- 5 Para restaurar la instancia con errores de Platform Services Controller desde su imagen de copia de seguridad, utilice la operación de restauración de emergencia directa a host.

Consulte, [Restaurar una máquina virtual con la operación de restauración de emergencia directa a host](#).

- 6 Encienda la máquina virtual que contiene la instancia de Platform Services Controller.

Importante Para las instancias de Platform Services Controller instaladas en Windows, si el sistema solicita reiniciar la máquina virtual, no la reinicie antes de ejecutar el script `pvc_restore`.

- 7 Inicie sesión en la instancia de Platform Services Controller.

- Para la instancia de Platform Services Controller implementada como dispositivo, inicie sesión en el shell de vCenter Server Appliance como **root**.
- Para la instancia de Platform Services Controller instalada en Windows, inicie sesión como administrador en la máquina virtual en la que instaló vCenter Server.

- 8 Compruebe que no haya ningún servicio de Platform Services Controller en ejecución.

- Para la instancia de Platform Services Controller implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para la instancia de Platform Services Controller instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

9 Ejecute el script `psc_restore` para restaurar Platform Services Controller.

Opción	Pasos
Para una instancia de Platform Services Controller implementada como un dispositivo	<p>Ejecute el script <code>psc_restore</code> en el shell del dispositivo.</p> <pre>psc_restore -u psc_administrator_username -p psc_administrator_password</pre> <p>Nota Si no se proporcionan argumentos, el script solicitará los argumentos necesarios tres veces antes de cerrarse.</p>
Para una instancia de Platform Services Controller instalada en Windows	<ol style="list-style-type: none"> 1 En el símbolo del sistema de Windows, desplácese hasta el script <code>psc_restore</code>. <p>De forma predeterminada, el script está ubicado en <code>C:\Archivos de programa\VMware\vCenter Server\</code>.</p> <ol style="list-style-type: none"> 2 Ejecute el script <code>psc_restore</code>. <pre>psc_restore -u psc_administrator_username -p psc_administrator_password</pre> <p>Nota Si no se proporcionan argumentos, el script se cierra después de notificar que no se especificaron los argumentos necesarios.</p>

10 Compruebe si se ejecutan todos los servicios de Platform Services Controller de la instancia restaurada de Platform Services Controller.

- Para la instancia de Platform Services Controller implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para la instancia de Platform Services Controller instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

11 Reinicie todos los servicios de vCenter Server.

Consulte *Administración de vCenter Server y hosts*.

Copia de seguridad y restauración de vCenter Server

Es posible instalar e implementar Platform Services Controller, así como registrar varias instancias de vCenter Server con la misma instancia de Platform Services Controller. Puede utilizar vSphere Data Protection para hacer copias de seguridad de todo el entorno y restaurarlo, de modo que si alguna de las instancias de vCenter Server presenta errores, sea posible restaurar la instancia de vCenter Server con errores.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

1 Implemente vSphere Data Protection Appliance.

Consulte [Implementación de la plantilla de OVF de vSphere Data Protection](#).

- 2 Complete la configuración inicial de vSphere Data Protection.

Consulte [Configuración de vSphere Data Protection](#).

- 3 Haga copias de seguridad basadas en imagen de la instancia de Platform Services Controller externa y de todas las instancias de vCenter Server.

Consulte [Crear un trabajo de copia de seguridad en vSphere Data Protection](#).

Nota Haga copias de seguridad de todas las instancias de vCenter Server y Platform Services Controller simultáneamente.

- 4 (Opcional) Para ejecutar un trabajo de copia de seguridad actual de inmediato, inicie el proceso de forma manual.

Consulte [Iniciar un trabajo de copia de seguridad de forma manual](#).

- 5 Restaure todas las instancias con errores de vCenter Server.

- Restaure una máquina virtual en la ubicación original.

Consulte [Restaurar una máquina virtual a la ubicación original](#).

- Restaure una máquina virtual en una nueva ubicación.

Consulte [Restaurar una máquina virtual en una nueva ubicación](#).

- Restaure una máquina virtual directamente en el host ESXi que ejecuta vSphere Data Protection Appliance si el servicio de vCenter Server deja de estar disponible o si no puede acceder a la interfaz de usuario de vSphere Data Protection al utilizar vSphere Web Client.

Consulte [Restaurar una máquina virtual con la operación de restauración de emergencia directa a host](#).

- 6 Encienda la máquina virtual que contiene la instancia restaurada de vCenter Server.

Hacer copias de seguridad del entorno de vCenter Server con varias instancias de Platform Services Controller y restaurarlo

Es posible utilizar vSphere Data Protection para hacer una copia de seguridad y una restauración de un entorno en el que las instancias de vCenter Server están registradas con distintas instancias

de Platform Services Controller y los datos de infraestructura se replican entre las instancias de Platform Services Controller.

Nota Si se generan errores en las instancias de vCenter Server y Platform Services Controller al mismo tiempo, primero debe restaurar las instancias de Platform Services Controller y después las de vCenter Server.

- **Hacer copias de seguridad de una instancia única de Platform Services Controller y restaurar**

El entorno puede contener varias instancias de vCenter Server registradas con diferentes instancias de Platform Services Controller externas que replican sus datos. Puede utilizar vSphere Data Protection para hacer copias de seguridad de todo el entorno y restaurarlo, de modo que si Platform Services Controller genera errores, sea posible restaurar la instancia de Platform Services Controller con errores.

- **Hacer copias de seguridad de varias instancias de Platform Services Controller y restaurar**

El entorno puede contener varias instancias de vCenter Server registradas con diferentes instancias de Platform Services Controller externas que replican sus datos. Es posible utilizar vSphere Data Protection para hacer copias de seguridad del entorno completo y restaurarlo, de modo que si varias instancias de Platform Services Controller generan un error, sea posible restaurarlas.

- **Hacer copias de seguridad de todas las instancias de Platform Services Controller y restaurarlas**

El entorno puede contener varias instancias de vCenter Server registradas con diferentes instancias de Platform Services Controller externas que replican sus datos. Puede utilizar vSphere Data Protection para hacer copias de seguridad de todo el entorno y restaurarlo. Si todas las instancias de Platform Services Controller generan errores, puede restaurar el entorno.

- **Copia de seguridad y restauración de vCenter Server**

Es posible que el entorno contenga varias instancias de vCenter Server registradas con distintas instancias externas de Platform Services Controller y que los datos de infraestructura se repliquen entre las instancias de Platform Services Controller. Es posible utilizar vSphere Data Protection para hacer copias de seguridad del entorno completo y restaurarlo, de modo que se puedan restaurar las instancias con errores de vCenter Server.

Hacer copias de seguridad de una instancia única de Platform Services Controller y restaurar

El entorno puede contener varias instancias de vCenter Server registradas con diferentes instancias de Platform Services Controller externas que replican sus datos. Puede utilizar vSphere Data Protection para hacer copias de seguridad de todo el entorno y restaurarlo, de modo que si

Platform Services Controller genera errores, sea posible restaurar la instancia de Platform Services Controller con errores.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

- 1 Implemente vSphere Data Protection Appliance.

Consulte [Implementación de la plantilla de OVF de vSphere Data Protection](#).

- 2 Complete la configuración inicial de vSphere Data Protection.

Consulte [Configuración de vSphere Data Protection](#).

- 3 Haga copias de seguridad basadas en imagen de la instancia de Platform Services Controller externa y de todas las instancias de vCenter Server.

Consulte [Crear un trabajo de copia de seguridad en vSphere Data Protection](#).

Nota Haga copias de seguridad de todas las instancias de vCenter Server y Platform Services Controller simultáneamente.

- 4 (Opcional) Para ejecutar un trabajo de copia de seguridad actual de inmediato, inicie el proceso de forma manual.

Consulte [Iniciar un trabajo de copia de seguridad de forma manual](#).

- 5 Redireccione las conexiones entre las instancias de vCenter Server registradas con Platform Services Controller hacia otra instancia externa funcional de Platform Services Controller.

Consulte [Redirigir vCenter Server a otra instancia de Platform Services Controller externa](#).

Importante Si redirecciona las conexiones entre vCenter Server y Platform Services Controller, es posible que se pierdan todos los trabajos de copia de seguridad y replicación. Los actuales puntos de restauración se mantienen intactos, pero se deben volver a crear los trabajos de copia de seguridad y replicación.

- 6 Restaurar la instancia de Platform Services Controller con errores:

- Restaure una máquina virtual en la ubicación original.

Consulte [Restaurar una máquina virtual a la ubicación original](#).

- Restaure una máquina virtual en una nueva ubicación.

Consulte [Restaurar una máquina virtual en una nueva ubicación](#).

- Restaure una máquina virtual directamente en el host ESXi que ejecuta vSphere Data Protection Appliance si el servicio de vCenter Server deja de estar disponible o si no puede acceder a la interfaz de usuario de vSphere Data Protection al utilizar vSphere Web Client.

Consulte [Restaurar una máquina virtual con la operación de restauración de emergencia directa a host](#).

- 7 Encienda la máquina virtual que contiene la instancia de Platform Services Controller.

Importante Para las instancias de Platform Services Controller instaladas en Windows, si el sistema solicita reiniciar la máquina virtual, no la reinicie antes de ejecutar el script `psc_restore`.

- 8 Inicie sesión en la instancia de Platform Services Controller.

- Para la instancia de Platform Services Controller implementada como dispositivo, inicie sesión en el shell de vCenter Server Appliance como **root**.
- Para la instancia de Platform Services Controller instalada en Windows, inicie sesión como administrador en la máquina virtual en la que instaló vCenter Server.

- 9 Compruebe que no haya ningún servicio de Platform Services Controller en ejecución.

- Para la instancia de Platform Services Controller implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
- Para la instancia de Platform Services Controller instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

- 10 Ejecute el script `psc_restore` para restaurar Platform Services Controller.

Opción	Pasos
Para una instancia de Platform Services Controller implementada como un dispositivo	<p>Ejecute el script <code>psc_restore</code> en el shell del dispositivo.</p> <pre>psc_restore -u psc_administrator_username -p psc_administrator_password</pre> <p>Nota Si no se proporcionan argumentos, el script solicitará los argumentos necesarios tres veces antes de cerrarse.</p>
Para una instancia de Platform Services Controller instalada en Windows	<ol style="list-style-type: none"> 1 En el símbolo del sistema de Windows, desplácese hasta el script <code>psc_restore</code>. <p>De forma predeterminada, el script está ubicado en <code>C:\Archivos de programa\VMware\vCenter Server\</code>.</p> <ol style="list-style-type: none"> 2 Ejecute el script <code>psc_restore</code>. <pre>psc_restore -u psc_administrator_username -p psc_administrator_password</pre> <p>Nota Si no se proporcionan argumentos, el script se cierra después de notificar que no se especificaron los argumentos necesarios.</p>

- 11 Compruebe si se ejecutan todos los servicios de Platform Services Controller de la instancia restaurada de Platform Services Controller.
 - Para la instancia de Platform Services Controller implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
 - Para la instancia de Platform Services Controller instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.
- 12 Vuelva a redireccionar las conexiones entre las instancias de vCenter Server a la instancia restaurada de Platform Services Controller.

Consulte [Redirigir vCenter Server a otra instancia de Platform Services Controller externa](#).

Importante Si redirecciona las conexiones entre vCenter Server y Platform Services Controller, es posible que se pierdan todos los trabajos de copia de seguridad y replicación. Los actuales puntos de restauración se mantienen intactos, pero se deben volver a crear los trabajos de copia de seguridad y replicación.

Hacer copias de seguridad de varias instancias de Platform Services Controller y restaurar

El entorno puede contener varias instancias de vCenter Server registradas con diferentes instancias de Platform Services Controller externas que replican sus datos. Es posible utilizar vSphere Data Protection para hacer copias de seguridad del entorno completo y restaurarlo, de modo que si varias instancias de Platform Services Controller generan un error, sea posible restaurarlas.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

- 1 Implemente vSphere Data Protection Appliance.

Consulte [Implementación de la plantilla de OVF de vSphere Data Protection](#).
- 2 Complete la configuración inicial de vSphere Data Protection.

Consulte [Configuración de vSphere Data Protection](#).
- 3 Haga copias de seguridad basadas en imagen de todas las instancias de Platform Services Controller y vCenter Server.

Consulte [Crear un trabajo de copia de seguridad en vSphere Data Protection](#).

Nota Haga copias de seguridad de todas las instancias de vCenter Server y Platform Services Controller simultáneamente.

- 4 (Opcional) Para ejecutar un trabajo de copia de seguridad actual de inmediato, inicie el proceso de forma manual.

Consulte [Iniciar un trabajo de copia de seguridad de forma manual](#).

- 5 Obtenga la topología de replicación de Platform Services Controller de una instancia funcional de Platform Services Controller.

Nota El comando de topología de replicación proporciona información únicamente sobre los partners de replicación directos de la instancia funcional de Platform Services Controller.

Opción	Pasos
Para una instancia de Platform Services Controller implementada como un dispositivo	<ol style="list-style-type: none"> 1 Inicie sesión en el shell del dispositivo como raíz. <ul style="list-style-type: none"> ■ Si tiene acceso directo a la consola del dispositivo, presione Alt+F1. ■ Si desea conectarse de forma remota, utilice SSH u otra conexión de consola remota para iniciar una sesión en el dispositivo. 2 (Opcional) Habilite el shell de Bash. <pre>shell.set --enabled true</pre> 3 Para acceder al shell de Bash, ejecute <code>shell</code>. 4 Ejecute el comando <code>vdcrepadmin</code>. <pre>/usr/lib/vmware-vmtoolsd/bin/vdcrepadmin -f showpartners -h localhost -u PSC_Administrator_username -w PSC_Administrator_password</pre>
Para una instancia de Platform Services Controller instalada en Windows	<ol style="list-style-type: none"> 1 Inicie sesión en el equipo Windows como administrador. 2 En el símbolo del sistema de Windows, ejecute el comando <code>vdcrepadmin</code>. <pre>C:\Program Files\VMware\VMware vCenter Server\vmtoolsd\bin\vdcrepadmin -f showpartners -h localhost -u psc_administrator_username -w psc_administrator_password</pre>

- 6 (Opcional) Si se registra una instancia de vCenter Server con Platform Services Controller con errores, redireccione las conexiones entre las instancias de vCenter Server y las instancias de Platform Services Controller con errores hacia otra instancia externa funcional de Platform Services Controller.

Consulte [Redirigir vCenter Server a otra instancia de Platform Services Controller externa](#).

Importante Si redirecciona las conexiones entre vCenter Server y Platform Services Controller, es posible que se pierdan todos los trabajos de copia de seguridad y replicación. Los actuales puntos de restauración se mantienen intactos, pero se deben volver a crear los trabajos de copia de seguridad y replicación.

7 Restaure los partners de replicación de una instancia funcional de Platform Services Controller.

- a Restaure la instancia con errores de Platform Services Controller desde su imagen de copia de seguridad.

- Restaure una máquina virtual en la ubicación original.

Consulte [Restaurar una máquina virtual a la ubicación original](#).

- Restaure una máquina virtual en una nueva ubicación.

Consulte [Restaurar una máquina virtual en una nueva ubicación](#).

- Restaure una máquina virtual directamente en el host ESXi que ejecuta vSphere Data Protection Appliance si el servicio de vCenter Server deja de estar disponible o si no puede acceder a la interfaz de usuario de vSphere Data Protection al utilizar vSphere Web Client.

Consulte [Restaurar una máquina virtual con la operación de restauración de emergencia directa a host](#).

- b Encienda la máquina virtual que contiene la instancia de Platform Services Controller.

Importante Para las instancias de Platform Services Controller instaladas en Windows, si el sistema solicita reiniciar la máquina virtual, no la reinicie antes de ejecutar el script `pvc_restore`.

- c Inicie sesión en la instancia de Platform Services Controller.

- Para la instancia de Platform Services Controller implementada como dispositivo, inicie sesión en el shell de vCenter Server Appliance como `root`.

- Para la instancia de Platform Services Controller instalada en Windows, inicie sesión como administrador en la máquina virtual en la que instaló vCenter Server.

- d Compruebe que no haya ningún servicio de Platform Services Controller en ejecución.

- Para la instancia de Platform Services Controller implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.

- Para la instancia de Platform Services Controller instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

- e Ejecute el script `psc_restore` para restaurar Platform Services Controller.

Opción	Pasos
Para una instancia de Platform Services Controller implementada como un dispositivo	<p>Ejecute el script <code>psc_restore</code> en el shell del dispositivo.</p> <pre>psc_restore -u psc_administrator_username -p psc_administrator_password</pre> <p>Nota Si no se proporcionan argumentos, el script solicitará los argumentos necesarios tres veces antes de cerrarse.</p>
Para una instancia de Platform Services Controller instalada en Windows	<ol style="list-style-type: none"> 1 En el símbolo del sistema de Windows, desplácese hasta el script <code>psc_restore</code>. <p>De forma predeterminada, el script está ubicado en <code>C:\Archivos de programa\VMware\vCenter Server\</code>.</p> <ol style="list-style-type: none"> 2 Ejecute el script <code>psc_restore</code>. <pre>psc_restore -u psc_administrator_username -p psc_administrator_password</pre> <p>Nota Si no se proporcionan argumentos, el script se cierra después de notificar que no se especificaron los argumentos necesarios.</p>

- 8 Compruebe si se ejecutan todos los servicios de Platform Services Controller de la instancia restaurada de Platform Services Controller.
- Para la instancia de Platform Services Controller implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
 - Para la instancia de Platform Services Controller instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.
- 9 Repita 5 hasta 9 para restaurar los partners de replicación de cada instancia de Platform Services Controller con errores que haya restaurado.

Nota Restaure primero las instancias de Platform Services Controller que tienen al menos un partner de replicación funcional.

- 10 (Opcional) Vuelva a redireccionar las conexiones entre las instancias de vCenter Server a las instancias de Platform Services Controller restauradas, redireccionadas anteriormente en 6, y reinicie las instancias de vCenter Server correspondientes.

Hacer copias de seguridad de todas las instancias de Platform Services Controller y restaurarlas

El entorno puede contener varias instancias de vCenter Server registradas con diferentes instancias de Platform Services Controller externas que replican sus datos. Puede utilizar vSphere

Data Protection para hacer copias de seguridad de todo el entorno y restaurarlo. Si todas las instancias de Platform Services Controller generan errores, puede restaurar el entorno.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

- 1 Implemente vSphere Data Protection Appliance.

Consulte [Implementación de la plantilla de OVF de vSphere Data Protection](#).

- 2 Complete la configuración inicial de vSphere Data Protection.

Consulte [Configuración de vSphere Data Protection](#).

- 3 Haga copias de seguridad basadas en imagen de todas las instancias de Platform Services Controller y vCenter Server.

Consulte [Crear un trabajo de copia de seguridad en vSphere Data Protection](#).

Nota Haga copias de seguridad de todas las instancias de vCenter Server y Platform Services Controller simultáneamente.

- 4 (Opcional) Para ejecutar un trabajo de copia de seguridad actual de inmediato, inicie el proceso de forma manual.

Consulte [Iniciar un trabajo de copia de seguridad de forma manual](#).

- 5 Restaure la instancia de Platform Services Controller con copia de seguridad más reciente mediante la restauración de emergencia directa a host.

Consulte [Restaurar una máquina virtual con la operación de restauración de emergencia directa a host](#).

- 6 Encienda la máquina virtual que contiene la instancia de Platform Services Controller.

Importante Para las instancias de Platform Services Controller instaladas en Windows, si el sistema solicita reiniciar la máquina virtual, no la reinicie antes de ejecutar el script `pvc_restore`.

- 7 Inicie sesión en la instancia de Platform Services Controller.

- Para la instancia de Platform Services Controller implementada como dispositivo, inicie sesión en el shell de vCenter Server Appliance como `root`.
- Para la instancia de Platform Services Controller instalada en Windows, inicie sesión como administrador en la máquina virtual en la que instaló vCenter Server.

- 8 Compruebe que no haya ningún servicio de Platform Services Controller en ejecución.

- Para la instancia de Platform Services Controller implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.

- Para la instancia de Platform Services Controller instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

9 Ejecute el script `psc_restore` con un argumento de línea de comandos `--ignore-sync` adicional.

Nota Debe utilizar el argumento de línea de comandos `--ignore-sync`, debido a que se restaura el primer nodo de la federación y no se puede sincronizar con ningún otro nodo.

Opción	Pasos
Para una instancia de Platform Services Controller implementada como un dispositivo	<p>Ejecute el script <code>psc_restore</code>.</p> <pre>psc_restore -u psc_administrator_username -p psc_administrator_password --ignore-sync</pre>
Para una instancia de Platform Services Controller instalada en Windows	<ol style="list-style-type: none"> 1 En el símbolo del sistema de Windows, desplácese hasta el script <code>psc_restore</code>. De forma predeterminada, el script está ubicado en <code>C:\Archivos de programa\VMware\vCenter Server\</code>. 2 Ejecute el script <code>psc_restore</code>. <pre>psc_restore -u psc_administrator_username -p psc_administrator-password --ignore-sync</pre>

- 10 Una vez completada la restauración, obtenga la topología de replicación de Platform Services Controller de una instancia funcional de Platform Services Controller.

Nota El comando de topología de replicación proporciona información únicamente sobre los partners de replicación directos de la instancia funcional de Platform Services Controller.

Opción	Pasos
Para una instancia de Platform Services Controller implementada como un dispositivo	<p>1 (Opcional) Habilite el shell de Bash.</p> <pre>shell.set --enabled true</pre> <p>2 Para acceder al shell de Bash, ejecute <code>shell</code>.</p> <p>3 Ejecute el comando para obtener la topología de la federación.</p> <pre>/usr/lib/vmware-vmtoolsd/bin/vdcrepadmin -f showpartners -h localhost -u PSC_administrator_username -w PSC_administrator_password</pre>
Para una instancia de Platform Services Controller instalada en Windows	<p>1 Inicie sesión en el equipo Windows como administrador.</p> <p>2 En el símbolo del sistema de Windows, ejecute el comando para obtener la topología de la federación.</p> <pre>C:\Program Files\VMware\VMware vCenter Server\vmtoolsd\bin\vdcrepadmin -f showpartners -h localhost -u psc_administrator_username -w psc_administrator_password</pre>

- 11 Restaure un partner de replicación con errores de la instancia restaurada de Platform Services Controller mediante uno de los métodos disponibles:

- Restaure una máquina virtual en la ubicación original.
Consulte [Restaurar una máquina virtual a la ubicación original](#).
- Restaure una máquina virtual en una nueva ubicación.
Consulte [Restaurar una máquina virtual en una nueva ubicación](#).
- Restaure una máquina virtual directamente en el host ESXi que ejecuta vSphere Data Protection Appliance si el servicio de vCenter Server deja de estar disponible o si no puede acceder a la interfaz de usuario de vSphere Data Protection al utilizar vSphere Web Client.
Consulte [Restaurar una máquina virtual con la operación de restauración de emergencia directa a host](#).

- 12 Encienda la máquina virtual que contiene la instancia de Platform Services Controller.

Importante Para las instancias de Platform Services Controller instaladas en Windows, si el sistema solicita reiniciar la máquina virtual, no la reinicie antes de ejecutar el script `psc_restore`.

- 13 Inicie sesión en la instancia de Platform Services Controller.
 - Para la instancia de Platform Services Controller implementada como dispositivo, inicie sesión en el shell de vCenter Server Appliance como **root**.
 - Para la instancia de Platform Services Controller instalada en Windows, inicie sesión como administrador en la máquina virtual en la que instaló vCenter Server.
- 14 Compruebe que no haya ningún servicio de Platform Services Controller en ejecución.
 - Para la instancia de Platform Services Controller implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.
 - Para la instancia de Platform Services Controller instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.
- 15 Ejecute el script `psc_restore` para restaurar Platform Services Controller.

Opción	Pasos
Para una instancia de Platform Services Controller implementada como un dispositivo	<p>Ejecute el script <code>psc_restore</code> en el shell del dispositivo.</p> <pre>psc_restore -u psc_administrator_username -p psc_administrator_password</pre> <p>Nota Si no se proporcionan argumentos, el script solicitará los argumentos necesarios tres veces antes de cerrarse.</p>
Para una instancia de Platform Services Controller instalada en Windows	<ol style="list-style-type: none"> 1 En el símbolo del sistema de Windows, desplácese hasta el script <code>psc_restore</code>. <p>De forma predeterminada, el script está ubicado en <code>C:\Archivos de programa\VMware\vCenter Server\</code>.</p> <ol style="list-style-type: none"> 2 Ejecute el script <code>psc_restore</code>. <pre>psc_restore -u psc_administrator_username -p psc_administrator_password</pre> <p>Nota Si no se proporcionan argumentos, el script se cierra después de notificar que no se especificaron los argumentos necesarios.</p>

- 16 Compruebe si se ejecutan todos los servicios de Platform Services Controller de la instancia restaurada de Platform Services Controller.
 - Para la instancia de Platform Services Controller implementada como dispositivo, ejecute el comando `service-control --status --all` en el shell del dispositivo.

- Para la instancia de Platform Services Controller instalada en Windows, en el menú **Inicio** de Windows, seleccione **Panel de control > Herramientas administrativas > Servicios**.

- 17 Repita [10](#) hasta [17](#) para restaurar los partners de replicación de cada instancia de Platform Services Controller con errores que haya restaurado.

Nota Restaure primero las instancias de Platform Services Controller que tienen al menos un partner de replicación funcional.

- 18 Reinicie todos los servicios de vCenter Server.

Consulte *Administración de vCenter Server y hosts*.

Copia de seguridad y restauración de vCenter Server

Es posible que el entorno contenga varias instancias de vCenter Server registradas con distintas instancias externas de Platform Services Controller y que los datos de infraestructura se repliquen entre las instancias de Platform Services Controller. Es posible utilizar vSphere Data Protection para hacer copias de seguridad del entorno completo y restaurarlo, de modo que se puedan restaurar las instancias con errores de vCenter Server.

Importante Es posible hacer copias de seguridad únicamente de máquinas virtuales que contienen instancias de vCenter Server, vCenter Server Appliance y Platform Services Controller, y restaurarlas. No puede hacer copias de seguridad y restaurar máquinas físicas que ejecutan vCenter Server a través de vSphere Data Protection.

- 1 Implemente vSphere Data Protection Appliance.

Consulte [Implementación de la plantilla de OVF de vSphere Data Protection](#).

- 2 Complete la configuración inicial de vSphere Data Protection.

Consulte [Configuración de vSphere Data Protection](#).

- 3 Haga copias de seguridad basadas en imagen de todas las instancias de Platform Services Controller y vCenter Server.

Consulte [Crear un trabajo de copia de seguridad en vSphere Data Protection](#).

Nota Haga copias de seguridad de todas las instancias de vCenter Server y Platform Services Controller simultáneamente.

- 4 (Opcional) Para ejecutar un trabajo de copia de seguridad actual de inmediato, inicie el proceso de forma manual.

Consulte [Iniciar un trabajo de copia de seguridad de forma manual](#).

- 5 Restaure todas las instancias con errores de vCenter Server.

- Restaure una máquina virtual en la ubicación original.

Consulte [Restaurar una máquina virtual a la ubicación original](#).

- Restaure una máquina virtual en una nueva ubicación.

Consulte [Restaurar una máquina virtual en una nueva ubicación](#).

- Restaure una máquina virtual directamente en el host ESXi que ejecuta vSphere Data Protection Appliance si el servicio de vCenter Server deja de estar disponible o si no puede acceder a la interfaz de usuario de vSphere Data Protection al utilizar vSphere Web Client.

Consulte [Restaurar una máquina virtual con la operación de restauración de emergencia directa a host](#).

- 6 Encienda la máquina virtual que contiene la instancia restaurada de vCenter Server.