

Instalación de vRealize Automation

vRealize Automation 7.0.1

Este documento admite la versión de todos los productos enumerados y admite todas las versiones posteriores hasta que el documento se reemplace por una edición nueva. Para buscar ediciones más recientes de este documento, consulte <http://www.vmware.com/es/support/pubs>.

ES-001835-04

vmware[®]

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

<http://www.vmware.com/es/support/>

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

Copyright © 2008–2016 VMware, Inc. Todos los derechos reservados. [Copyright e información de marca registrada.](#)

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

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.: + 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Instalación de vRealize Automation	7
Información actualizada	9
1 Descripción general de la instalación de vRealize Automation	11
Elegir la ruta de implementación	11
Descripción de una implementación mínima	12
Descripción de una implementación empresarial	13
Componentes de instalación de vRealize Automation	14
Dispositivo de vRealize Automation de VMware	15
Agentes de administración	15
Infraestructura como servicio de vRealize Automation	15
2 Preparar la instalación	19
DNS y resolución de nombres de host	19
Requisitos de hardware y máquinas virtuales	20
Consideraciones sobre los navegadores	20
Consideraciones sobre las contraseñas	20
Requisitos de Windows Server	21
Requisitos del servidor de la base de datos de IaaS	21
Requisitos del servidor de Model Management y el servicio web de IaaS	21
IaaS Manager Service	22
Requisitos de Distributed Execution Manager	23
Requisitos de puertos	24
Cuentas de usuario y credenciales necesarias para la instalación	26
Seguridad	28
Certificados	28
Extraer certificados y claves privadas	29
Frase de contraseña de seguridad	29
Software de terceros	29
Sincronización de hora	29
3 Instalar vRealize Automation con el Asistente de instalación	31
Implementar el dispositivo de vRealize Automation	31
Instalar una implementación mínima con el asistente de instalación	32
Ejecutar el asistente de instalación para una implementación mínima	33
Instalar el agente de administración	34
Sincronizar la hora de los servidores	37
Ejecutar el Comprobador de requisitos previos	37
Especificar los parámetros de configuración de la implementación	38
Crear snapshots antes de comenzar la instalación	38
Escenario: Finalizar la instalación	39

Fallos de instalación de dirección	39
Configurar las credenciales de la configuración de contenido inicial	40
Instalar una implementación empresarial con el asistente de instalación	41
Ejecutar el asistente de instalación para una implementación empresarial	41
Instalar el agente de administración	42
Sincronizar la hora de los servidores	44
Ejecutar el Comprobador de requisitos previos	44
Especificar los parámetros de configuración de la implementación	45
Crear snapshots antes de comenzar la instalación	45
Finalizar la instalación	46
Fallos de instalación de dirección	46
Configurar las credenciales de la configuración de contenido inicial	47
4 Instalar vRealize Automation mediante interfaces estándar	49
Implementación mínima	49
Lista de comprobación de implementación mínima	49
Implementar y configurar el dispositivo de vRealize Automation	50
Instalar componentes de IaaS	55
Implementación distribuida	61
Lista de comprobación de implementación distribuida	61
Componentes de la instalación distribuida	62
Requisitos de confianza de certificados en una implementación distribuida	63
Hojas de trabajo de instalación	63
Implementar el dispositivo de vRealize Automation	65
Configurar el equilibrador de carga	66
Configurar dispositivos para vRealize Automation	67
Instalar los componentes de IaaS en una configuración distribuida	73
Instalación de agentes	97
Establecer la política de ejecución de PowerShell en RemoteSigned	97
Elegir un escenario de instalación de agentes	98
Ubicación y requisitos de instalación de agentes	98
Instalar y configurar el agente de proxy de vSphere	98
Instalar el agente de proxy de Hyper-V o XenServer	103
Instalar el agente de VDI de XenDesktop	107
Instalar el agente de EPI de Citrix	111
Instalar el agente de EPI de Visual Basic Scripting	114
Instalar el agente de WMI para solicitudes de WMI remotas	117
5 Configurar el acceso al tenant predeterminado	121
6 Reemplazar los certificados autofirmados por certificados proporcionados por una entidad	123
7 Solucionar problemas	125
Ubicaciones de logs predeterminadas	125
Revertir una instalación fallida	126
Revertir una instalación mínima	127
Revertir una instalación distribuida	127

Crear un paquete de soporte para vRealize Automation	128
Solucionar problemas de instalación general	128
Error de tiempo de espera agotado de un equilibrador de carga al instalar o actualizar	128
Horas de servidor no sincronizadas	129
Pueden aparecer páginas en blanco al utilizar Internet Explorer 9 o 10 en Windows 7	129
No se puede establecer una relación de confianza para el canal seguro SSL/TLS	130
Conectarse a la red mediante un servidor proxy	130
El servidor proxy impide el inicio de sesión de usuario de VMware Identity Manager	131
Solucionar problemas de dispositivos de vRealize Automation	132
Error de descarga de los instaladores	132
El archivo Encryption.key tiene permisos incorrectos	132
Identity Manager no puede iniciarse después del reinicio de Horizon-Workspace	133
Solucionar problemas con componentes de IaaS	133
Validar certificados de servidor para IaaS	133
Error de credenciales al ejecutar el instalador de IaaS	134
Se muestra una advertencia de configuración no guardada durante la instalación de IaaS	134
Error al instalar el servidor de sitios web y Distributed Execution Managers	135
La autenticación de IaaS genera un error durante la instalación de administración de modelo y web de IaaS	135
Error al instalar los componentes web y Model Manager Data	135
Error interno al añadir un endpoint de XaaS	137
Error al desinstalar un agente de proxy	137
Error de solicitudes de máquinas cuando las transacciones remotas están deshabilitadas	138
Error en la comunicación de Manager Service	139
El comportamiento de personalización de correo electrónico ha cambiado	139
Solucionar problemas de errores de inicio de sesión	140
Error sin explicación al intentar iniciar sesión como administrador de IaaS con credenciales con formato de UPN incorrecto	140
No se puede iniciar sesión en un tenant o los almacenes de identidades de tenants desaparecen	140
Índice	143

Instalación de vRealize Automation

En *Instalación de vRealize Automation* se explica cómo instalar VMware vRealize™ Automation.

NOTA: No todas las características y funcionalidades de vRealize Automation están disponibles en todas las ediciones. Para ver una comparación de los conjuntos de características de cada edición, vaya a <https://www.vmware.com/products/vrealize-automation/>.

Público objetivo

Esta información está destinada a los administradores de sistemas Windows o Linux con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Glosario de publicaciones técnicas de VMware

El departamento de Publicaciones técnicas de VMware ofrece un glosario con términos que quizá usted desconozca. Para consultar las definiciones de términos tal como se utilizan en la documentación técnica de VMware, visite <http://www.vmware.com/support/pubs>.

Información actualizada

Instalar vRealize Automation 7.0 se actualiza con cada versión del producto o cuando resulta necesario.

Esta tabla proporciona el historial de actualización de la publicación *Instalar vRealize Automation 7.0*.

Revisión	Descripción
ES-001835-04	Actualizaciones en los requisitos previos de SQL Server. Consulte “Requisitos del servidor de la base de datos de IaaS,” página 21.
ES-001835-03	Procedimientos de solución de problemas adicionales.
ES-001835-02	Se han eliminado procedimientos desactualizados sobre las conmutaciones por error de bases de datos del capítulo 4.
ES-001835-01	<ul style="list-style-type: none">■ Adición de un nuevo escenario de implementación para instalar y configurar un entorno de desarrollo y una prueba de concepto de vRealize Automation. Para ver una descripción general del escenario de ejemplo, consulte “Elegir la ruta de implementación,” página 11. Para ver el escenario completo, consulte <i>Instalación y configuración de vRealize Automation para el escenario de Rainpole</i>.■ Varias pequeñas actualizaciones para dejar constancia de que la alta disponibilidad no se configura del todo hasta que los administradores de tenant configuren Administración de directorios para la alta disponibilidad.■ Actualizaciones de la versión 7.0.1 de vRealize Automation.
ES-001835-00	Versión del documento inicial.

Descripción general de la instalación de vRealize Automation

1

vRealize Automation puede implementarse en diversas configuraciones. Para garantizar una implementación correcta, es conveniente que comprenda las opciones de implementación y configuración, y la secuencia de tareas.

Si está familiarizado con versiones anteriores de vRealize Automation, puede resultar útil tener en cuenta los siguientes cambios antes de iniciar la instalación:

- En esta versión de vRealize Automation se incluye el Asistente de instalación, el método recomendado para instalaciones sin scripts. Con el asistente, puede elegir una implementación mínima o empresarial. Las implementaciones empresariales se basan en arquitecturas distribuidas y pueden incluir equilibradores de carga para implementaciones de alta disponibilidad. Puede instalar dispositivos de vRealize Automation solos o con componentes de IaaS.
- La compatibilidad con Single Sign-On y la administración de identidad se logra mediante un VMware Identity Manager integrado que se administra mediante la nueva función de administración de directorios. Esto sustituye el uso de implementaciones SSO de VMware Identity Appliance y vSphere de las versiones anteriores del producto.
- Ya no se admite Open LDAP.

Tras la instalación, los administradores del sistema pueden personalizar el entorno de instalación y configurar uno o más tenants, para así configurar el acceso al aprovisionamiento de autoservicio y a la administración del ciclo de vida de los servicios de nube.

A través de la interfaz web de portal seguro, los administradores, desarrolladores o usuarios empresariales pueden solicitar servicios de TI y administrar recursos de TI y de nube específicos, en función de sus funciones y privilegios. Los usuarios pueden solicitar servicios de infraestructura, aplicación, escritorio y TI a través de un catálogo de servicios común.

Este capítulo cubre los siguientes temas:

- [“Elegir la ruta de implementación,”](#) página 11
- [“Componentes de instalación de vRealize Automation,”](#) página 14

Elegir la ruta de implementación

En función de los requisitos de implementación, podrá instalar y configurar componentes de vRealize Automation mediante el uso de tutoriales de instalación de Rainpole, el asistente de instalación o a través de la consola de administración.

Elija una instalación mínima para implementar una prueba de concepto (PoC) o un entorno de desarrollo con una topología básica. Elija una instalación empresarial para implementar un entorno de producción con la topología más adecuada para las necesidades de su organización.

Tabla 1-1. Elegir el método de instalación

Método de instalación	Detalles
Asistente de instalación	<p>El asistente de instalación proporciona la ruta de instalación más rápida para la mayoría de las implementaciones. Puede optar por una implementación mínima o empresarial para prestar soporte a componentes distribuidos con o sin equilibradores de carga. Complete y compruebe todos los requisitos previos antes de iniciar el asistente.</p> <p>Para obtener más información, consulte Capítulo 2, “Preparar la instalación,” página 19.</p>
Instalación manual	<p>La instalación mediante la consola de administración también es compatible con instalaciones mínimas, distribuidas y de gran disponibilidad. Complete y compruebe todos los requisitos previos antes de iniciar la instalación.</p> <p>Para obtener más información, consulte Capítulo 2, “Preparar la instalación,” página 19.</p> <p>NOTA: Si utiliza la consola de administración para iniciar o configurar cualquier parte de la instalación, no podrá iniciar o seguir utilizando el asistente de instalación.</p>
<i>Instalación y configuración de vRealize Automation para el escenario de Rainpole</i>	<p>Como administrador de vSphere, quiere instalar una implementación de vRealize Automation mínima en el entorno de vSphere existente. Use el asistente de instalación de vRealize Automation y cree elementos del catálogo de contenido inicial que lo ayuden a configurar rápidamente un entorno para usar una prueba de concepto.</p> <p>Una implementación de prueba de concepto no es apropiada para producción. Al completar la implementación de prueba de concepto, la configura como un entorno de desarrollo en el que usted y su equipo de TI crean y prueban blueprints. Puede exportar blueprints y otros elementos de diseño fuera de su entorno de desarrollo y dentro de su entorno de producción.</p> <p>Para comenzar con este escenario, consulte <i>Instalación y configuración de vRealize Automation para el escenario de Rainpole</i>.</p>

Tabla 1-2. Elegir el tipo de implementación

Propósito de la implementación	Elegir este tipo de implementación
Implementar una prueba de concepto (PoC) o un entorno de desarrollo con una topología básica.	<p>Instale una implementación mínima.</p> <p>Para ello, implemente una única instancia de el dispositivo de vRealize Automation e instale todos los componentes de IaaS en una sola máquina servidor de Windows. Las bases de datos se pueden instalar en la misma máquina de Windows o en un servidor SQL Server dedicado.</p>
Implementar un entorno de producción con la topología que cubra de mejor forma las necesidades de su organización.	<p>Instale una implementación empresarial.</p> <p>Distribuya los componentes por varios servidores.</p> <p>Como alternativa, puede implementar equilibradores de carga para distribuir el trabajo entre los servidores y ofrecer funciones de conmutación por error y redundancia en un entorno de alta disponibilidad.</p>

Para obtener información sobre la escalabilidad y la alta disponibilidad, consulte la *arquitectura de referencia de VMware vRealize Automation*, disponible como documento técnico en <https://www.vmware.com/support/pubs/vcac-pubs.html>.

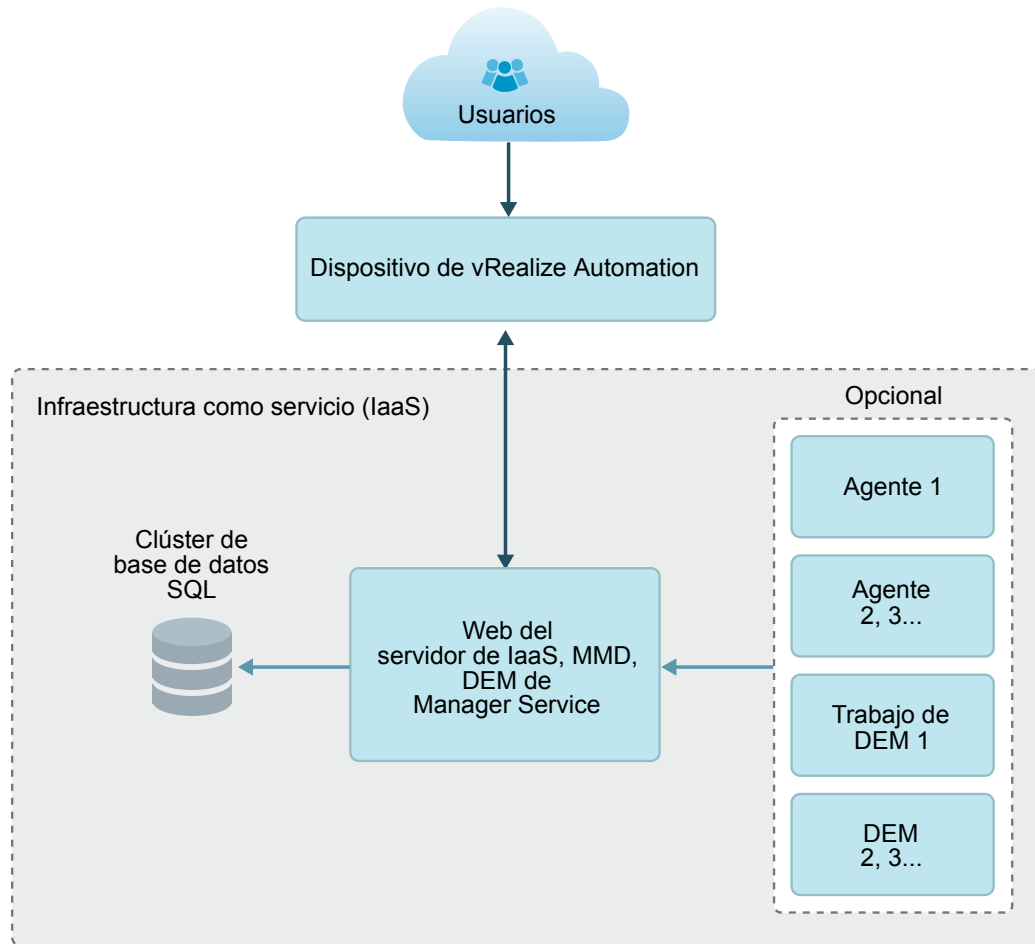
Descripción de una implementación mínima

Para realizar una implementación mínima, un administrador del sistema instala los componentes el dispositivo de vRealize Automation y de infraestructura como servicio (IaaS).

- el dispositivo de vRealize Automation incluye la interfaz de consola web y compatibilidad con funciones de single sign-on. Se instala como un dispositivo virtual.
- La infraestructura como servicio (IaaS) se instala en una máquina de Windows Server.

- IaaS utiliza una base de datos SQL que se puede instalar en la misma máquina como IaaS o en su propio servidor.

En la siguiente figura se muestra la relación y la finalidad de los componentes de una instalación mínima.



Descripción de una implementación empresarial

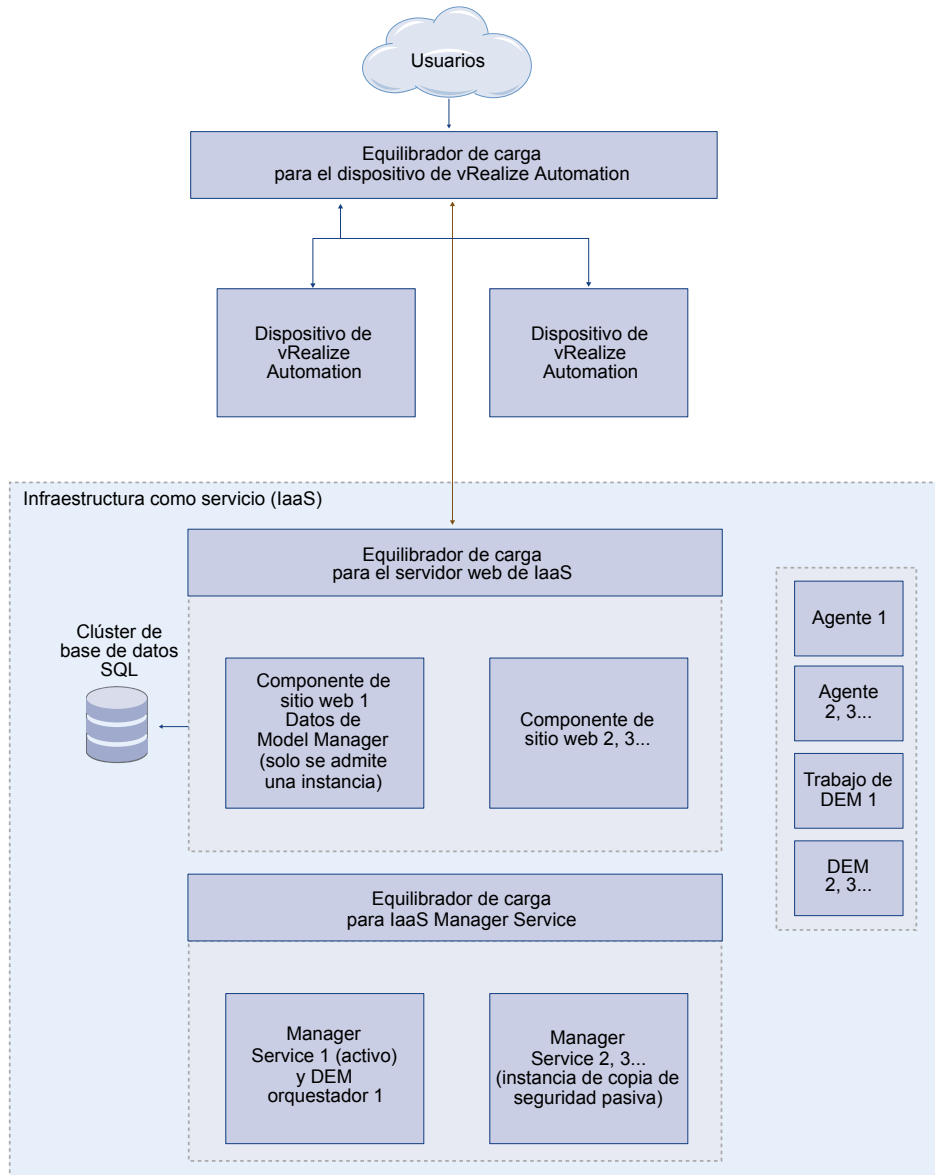
El administrador del sistema puede implementar e instalar varias instancias de el dispositivo de vRealize Automationy componentes individuales de IaaS para garantizar la escala, la redundancia, la alta disponibilidad y la recuperación ante desastres.

En una arquitectura típica, los componentes de IaaS se distribuyen en varias máquinas.

Para las implementaciones de alta disponibilidad, los equilibradores de carga distribuyen la carga de trabajo en el entorno informático. Los administradores del sistema configuran los equilibradores de carga fuera del marco de trabajo de vRealize Automation.

La siguiente figura muestra los componentes de una implementación empresarial con componentes distribuidos, redundancia y equilibradores de carga.

Figura 1-1. Configuración de implementación para instalaciones empresariales



Componentes de instalación de vRealize Automation

Una instalación de vRealize Automation conlleva instalar y configurar las funciones de single sign-on (SSO), el portal de interfaz de usuario y los componentes de infraestructura como servicio (IaaS).

Una instalación consta de los siguientes componentes.

- el dispositivo de vRealize Automation, que implementa la consola de administración, administra capacidades de Single Sign-On (SSO) para la autorización y la autenticación, e incluye una instancia de vRealize Orchestrator.
- Componentes de infraestructura como servicio (IaaS), que se instalan en una máquina de Windows (virtual o física) y que aparecen recogidos en la pestaña **Infraestructura** en la consola.
- Una base de datos de MS SQL Server, que se implementa durante la instalación de IaaS.

Dispositivo de vRealize Automation de VMware

el dispositivo de vRealize Automation es un dispositivo virtual preconfigurado que contiene el servidor de vRealize Automation. vRealize Automation se entrega como una plantilla de formato de virtualización abierta (OVF). El administrador del sistema implementa el dispositivo virtual en una infraestructura virtualizada existente.

El servidor incluye la consola del producto el dispositivo de vRealize Automation, que ofrece un portal único para el aprovisionamiento de autoservicio y la administración de servicios de nube, creación, administración y control.

Base de datos de dispositivo

Durante la implementación de dispositivos virtuales, se crea automáticamente una base de datos de dispositivos PostgreSQL en el primer el dispositivo de vRealize Automation. Se puede instalar una base de datos de réplica en un segundo dispositivo de vRealize Automation para crear un entorno de alta disponibilidad.

Agentes de administración

Los agentes de administración son componentes de IaaS independientes que registran nodos de IaaS con dispositivos vRealize Automation, automatizan la instalación y administración de componentes de IaaS, y recopilan la información de soporte y telemetría.

Se debe instalar un agente de administración en cada máquina de Windows que aloje componentes de IaaS.

Infraestructura como servicio de vRealize Automation

Infraestructura como servicio (IaaS) permite crear modelos de servidores y escritorios y aprovisionarlos rápidamente en infraestructuras privadas, públicas o de nube híbridas.

El administrador del sistema instala componentes de IaaS en una máquina de Windows. La funcionalidad de IaaS también se encuentra disponible en la pestaña **Infraestructura** de la consola de administración. IaaS tiene varios componentes que puede instalar en una configuración personalizada para satisfacer las necesidades de su organización.

Sitio web de IaaS

El componente Sitio web de IaaS proporciona a la consola de vRealize Automation funcionalidades de autoría de servicio y administración de infraestructura. El componente de sitio web se comunica con Manager Service, que le ofrece actualizaciones de Distributed Execution Manager (DEM), agentes de proxy y bases de datos.

Model Manager

Los modelos de vRealize Automation facilitan la integración con bases de datos y sistemas externos. Implementan la lógica empresarial que un Distributed Execution Manager (DEM) emplea.

Model Manager proporciona servicios y utilidades dirigidos a la persistencia, control de versiones, protección y distribución de los elementos de modelo. Se comunica con la base de datos, los DEM y el sitio web de la consola.

Manager Service de vCloud Automation Center

Manager Service coordina la comunicación entre los DEM, los agentes y la base de datos. Manager Service se comunica con el sitio web de la consola a través de Model Manager. Este servicio requiere privilegios administrativos para poder ejecutarse.

Base de datos de IaaS

El componente IaaS de vRealize Automation utiliza una base de datos de Microsoft SQL Server para conservar la información sobre las máquinas que administra, así como sobre sus propios elementos y políticas. Normalmente, durante la instalación se crea una base de datos para usted. Sin embargo, el administrador del sistema también puede crear una base de datos por separado.

Distributed Execution Managers

Un Distributed Execution Manager (DEM) ejecuta la lógica empresarial de los modelos personalizados, para lo cual interactúa con la base de datos y con los sistemas y bases de datos externos según sea necesario.

Cada instancia de DEM actúa como una función de trabajo o una función de orquestador. La función de trabajo es responsable de ejecutar flujos de trabajo, mientras que la función de orquestador se encarga de supervisar las instancias de DEM de trabajo, de preprocesar los flujos de trabajo que se van a ejecutar y de programar esos flujos de trabajo.

El DEM orquestador realiza las siguientes tareas específicas.

- Supervisa el estado de los DEM de trabajo y procura que, si una instancia de trabajo se detiene o pierde la conexión con Model Manager, sus flujos de trabajo van a volver a ponerse en cola para que otro DEM de trabajo se encargue de ellos.
- Administra los flujos de trabajo programados creando instancias en el momento programado.
- Garantiza que solo una instancia de un flujo de trabajo programado concreto se ejecute en un momento determinado.
- Preprocesa los flujos de trabajo antes de que se ejecuten, incluido comprobar las condiciones previas de los flujos de trabajo (usadas en la implementación de la función RunOneOnly) y crear el historial de ejecución de flujos de trabajo.

Una instancia de DEM orquestador está designada como el orquestador activo que lleva a cabo estas tareas. Dado que el DEM orquestador es imprescindible para ejecutar flujos de trabajo, debe haber al menos una instancia de orquestador más en otra máquina para poder disponer de redundancia. El orquestador se instala automáticamente en la máquina que también ejecuta Manager Service. Este DEM orquestador adicional supervisa el estado del orquestador activo, así podrá sustituirlo en caso de que se desconecte.

Agentes de vRealize Automation

vRealize Automation utiliza agentes para la integración con sistemas externos y para administrar información entre componentes de vRealize Automation.

El agente de vSphere se suele instalar como parte de una implementación. Además, se pueden instalar agentes adicionales según las necesidades del sitio.

Agentes de integración

Los agentes de Virtual Desktop Integration (VDI) PowerShell permiten la integración de vRealize Automation con sistemas de escritorio virtual externos. Actualmente, las máquinas virtuales que aprovisiona vRealize Automation pueden registrarse con XenDesktop en un Citrix Desktop Delivery Controller (DDC) y sus propietarios pueden acceder a la interfaz web de XenDesktop desde vRealize Automation.

Los agentes de External Provisioning Integration (EPI) PowerShell permiten que vRealize Automation integre sistemas externos en el proceso de aprovisionamiento de máquinas. Por ejemplo, la integración con Citrix Provisioning Server permite el aprovisionamiento de máquinas mediante streaming de disco a petición, y un agente de EPI permite ejecutar scripts de Visual Basic como pasos adicionales durante el proceso de aprovisionamiento.

Los agentes de VDI y EPI requieren acceso de nivel de administrador a los sistemas externos con los que interactúan.

Agentes de proxy de virtualización

Las máquinas virtuales que administra vRealize Automation se crean en nodos de virtualización. vRealize Automation usa agentes de proxy de virtualización para enviar comandos y recopilar datos de vSphere ESX Server, XenServer, los hosts de virtualización de Hyper-V y las máquinas virtuales aprovisionadas en ellos. Un agente de proxy se caracteriza por lo siguiente.

- Suele requerir acceso de nivel de administrador a la plataforma de virtualización que administra
- Se comunica con Manager Service
- Se instala de forma independiente con su propio archivo de configuración

Agente de Instrumental de administración de Windows

El agente de Instrumental de administración de Windows (WMI) de vRealize Automation mejora la capacidad de supervisar y controlar la información del sistema, y permite administrar servidores remotos desde una ubicación centralizada. Permite recopilar datos de máquinas con Windows administradas por vRealize Automation.

Preparar la instalación

Los administradores del sistema instalarán vRealize Automation en los entornos de virtualización existentes. Antes de iniciar una instalación, prepare el entorno de implementación para satisfacer los requisitos del sistema.

Este capítulo cubre los siguientes temas:

- [“DNS y resolución de nombres de host,”](#) página 19
- [“Requisitos de hardware y máquinas virtuales,”](#) página 20
- [“Consideraciones sobre los navegadores,”](#) página 20
- [“Consideraciones sobre las contraseñas,”](#) página 20
- [“Requisitos de Windows Server,”](#) página 21
- [“Requisitos de puertos,”](#) página 24
- [“Cuentas de usuario y credenciales necesarias para la instalación,”](#) página 26
- [“Seguridad,”](#) página 28
- [“Sincronización de hora,”](#) página 29

DNS y resolución de nombres de host

En vRealize Automation, el administrador del sistema debe identificar todos los hosts mediante un nombre de dominio completo (FQDN).

En una implementación distribuida, todos los componentes de vRealize Automation deben poder resolverse entre sí usando un FQDN.

El servicio web de Model Manager, Manager Service y la base de datos de Microsoft SQL Server también deben poder resolverse entre sí por medio de sus nombres de Servicio de nombres Internet de Windows (WINS). Para que estos nombres de host se puedan resolver en su entorno, debe configurar el Sistema de nombres de dominio (DNS).

IMPORTANTE: vRealize Automation no permite desplazarse a hosts cuyo nombre de host contenga el carácter de subrayado (_).

Requisitos de hardware y máquinas virtuales

La implementación requiere unos recursos del sistema mínimos para instalar los dispositivos virtuales y unos requisitos de hardware mínimos para instalar los componentes de IaaS en el servidor de Windows.

Para obtener información sobre los requisitos del sistema operativo y el entorno de alto nivel, incluida la información relativa a navegadores y sistemas operativos admitidos, consulte *Matriz de soporte de vRealize Automation*.

La tabla Requisitos de hardware muestra los requisitos de configuración mínimos para la implementación de dispositivos virtuales y la instalación de componentes de IaaS. Los dispositivos son máquinas virtuales configuradas previamente que se añaden al inventario de vCenter Server o ESXi. Los componentes de IaaS se instalan en servidores Windows 2008 R2 SP1 o Windows 2012 R2 físicos o virtuales.

Active Directory se considera pequeño cuando hay hasta 25.000 usuarios en la OU que se sincronizará en la configuración del almacén de identificadores. Active Directory se considera grande cuando hay más de 25.000 usuarios en la OU.

Tabla 2-1. Requisitos de hardware

el dispositivo de vRealize Automation para instancias de Active Directory pequeñas	el dispositivo de vRealize Automation para instancias de Active Directory grandes	Componentes de IaaS (servidor de Windows).
<ul style="list-style-type: none"> ■ 4 CPU ■ 18 GB de memoria ■ 60 GB de almacenamiento en disco 	<ul style="list-style-type: none"> ■ 4 CPU ■ 22 GB de memoria ■ 60 GB de almacenamiento en disco 	<ul style="list-style-type: none"> ■ 2 CPU ■ 8 GB de memoria ■ 30 GB de almacenamiento en disco <p>Cuando se incluye un servidor SQL en un host de Windows, se necesitan recursos adicionales.</p>

Consideraciones sobre los navegadores

Existen algunas restricciones relativas al uso de navegadores con vRealize Automation.

- No se admite el uso de varias pestañas y ventanas del navegador. vRealize Automation admite una sesión por usuario.
- Las consolas remotas de VMware provisionadas en vSphere admiten un subconjunto de navegadores que admite vRealize Automation.

Para obtener información sobre los requisitos del sistema operativo y el entorno de alto nivel, incluida la información relativa a navegadores y sistemas operativos admitidos, consulte *Matriz de soporte de vRealize Automation*.

Consideraciones sobre las contraseñas

Algunas contraseñas tienen restricciones de caracteres.

La contraseña de administrador de vRealize Automation que se define durante la instalación no debe contener caracteres especiales. A partir de esta versión de vRealize Automation, se sabe que los siguientes caracteres especiales causan errores:

- Comillas dobles (")
- Comas (,)
- Signo igual al final (=)
- Espacios en blanco

- Caracteres que no son ASCII o caracteres ASCII extendidos

Puede que las contraseñas que contienen caracteres especiales se acepten cuando las asigna, pero pueden causar errores cuando realiza operaciones como guardar endpoints o cuando la máquina intenta unirse al clúster de vRealize Automation.

Requisitos de Windows Server

La máquina de Windows física o virtual que aloja los componentes de IaaS debe cumplir los requisitos de configuración de la base de datos de IaaS, los componentes del servidor de IaaS, el IaaS Manager Service y los Distributed Execution Manager.

Como práctica recomendada, todos los servidores deben estar en el mismo dominio.

El asistente para la instalación ejecuta el vRealize Automation en todos los servidores de Windows antes de iniciar el proceso de instalación para asegurarse de que los servidores cumplan las configuraciones necesarias.

Requisitos del servidor de la base de datos de IaaS

El servidor de Windows que aloja la base de datos SQL Server de IaaS de vRealize Automation debe cumplir ciertos requisitos.

Los requisitos se aplican si se ejecuta el asistente de instalación o el instalador de `setup_vrealize-automation-appliance-URL.exe` heredado y se seleccione la función de base de datos para la instalación. Los requisitos previos también se aplican si se crea una base de datos SQL Server por separado para usarla con IaaS.

- Use una versión de SQL Server compatible de *Matriz de soporte de vRealize Automation*.
- Configure SQL Server en el puerto 1433 (valor predeterminado). No utilice un puerto distinto al predeterminado.
- Habilite el protocolo TCP/IP para SQL Server.
- Habilite el servicio del Coordinador de transacciones distribuidas (DTC) en todos los servidores de Windows de IaaS y en la máquina que aloja SQL Server. IaaS usa DTC para poder realizar acciones y transacciones de base de datos, como la creación de flujos de trabajo.

NOTA: Si clona una máquina para crear un servidor de Windows de IaaS, instale DTC en el clon tras la clonación. Si clona una máquina que ya tenga DTC, su identificador único se copiará al clon y se producirá un problema de comunicación. Consulte [“Error en la comunicación de Manager Service,”](#) página 139.

Para obtener más información sobre la autorización de DTC, consulte [el artículo de la Base de conocimientos de VMware 2038943](#).

- Abra puertos entre todos los servidores de Windows de IaaS y la máquina que aloja SQL Server. Consulte [“Requisitos de puertos,”](#) página 24.

Por otro lado, si lo permite la política del sitio, deshabilite los firewalls entre los servidores de Windows de IaaS y SQL Server.

Requisitos del servidor de Model Management y el servicio web de IaaS

Un entorno debe cumplir los requisitos previos de software y configuración que permiten la instalación de los componentes de servidor de IaaS.

Requisitos de base de datos y entorno para IaaS

Su configuración de host y base de datos MS SQL deben cumplir con los siguientes requisitos.

Tabla 2-2. Requisitos de IaaS

Área	Requisitos
Configuración de host	<p>Para poder instalar IaaS, los siguientes componentes deben estar instalados en el host:</p> <ul style="list-style-type: none"> ■ Microsoft .NET Framework 4.5.2 o posterior. ■ Microsoft PowerShell 2.0 (incluido a partir de Windows Server 2008 R2 SP1) o Microsoft PowerShell 3.0 en Windows Server 2012 R2. ■ Microsoft Internet Information Services 7.5. ■ Debe instalar Java en la máquina que ejecute el componente web principal para admitir la implementación de la base de datos MS SQL durante la instalación.
Requisitos de base de datos de Microsoft SQL	<p>La base de datos de Microsoft SQL puede estar en el host del servidor de IaaS (Windows) o en un host remoto.</p> <p>Estos requisitos relativos a Java se aplican a las bases de datos en el host del servidor de IaaS (Windows). No se aplican a las bases de datos externas.</p> <ul style="list-style-type: none"> ■ Debe haber instalada una versión de 64 bits de Java 1.7 o posterior. Las versiones de 32 bits no son compatibles. ■ La variable de entorno JAVA_HOME debe estar establecida en la carpeta de instalación de Java. ■ El archivo %JAVA_HOME%\bin\java.exe debe estar disponible.

Requisitos de Microsoft Internet Information Services

Microsoft Internet Information Services (IIS) debe cumplir con los siguientes requisitos de configuración.

Tabla 2-3. Configuración necesaria de Microsoft Internet Information Services

Componente de IIS	Configuración
Módulos de Internet Information Services (IIS) instalados	<ul style="list-style-type: none"> ■ WindowsAuthentication ■ StaticContent ■ DefaultDocument ■ ASPNET 4.5 ■ ISAPIExtensions ■ ISAPIFilter
Configuración de autenticación de IIS	<ul style="list-style-type: none"> ■ Autenticación de Windows habilitada ■ Autenticación anónima deshabilitada ■ Proveedor Negotiate habilitado ■ Proveedor NTLM habilitado ■ Modo kernel de autenticación de Windows habilitado ■ Protección ampliada de autenticación de Windows deshabilitada ■ En los certificados que usan SHA512, TLS1.2 debe estar deshabilitado en los servidores de Windows 2012 o Windows 2012 R2
Funciones de Servicio de activación de procesos de Windows de IIS	<ul style="list-style-type: none"> ■ ConfigurationApi ■ NetEnvironment ■ ProcessModel ■ WcfActivation (solo Windows 2008) ■ HttpActivation ■ NonHttpActivation

IaaS Manager Service

Un entorno debe cumplir algunos requisitos generales que permiten la instalación de IaaS Manager Service.

- Microsoft .NET Framework 4.5.2 está instalado.

- Microsoft PowerShell 2.0 o Microsoft PowerShell 3.0. PowerShell 2.0 se incluye en Windows Server 2008 R2 SP1 en adelante. Microsoft PowerShell 3.0 se ejecuta en Windows Server 2012 R2.
- SecondaryLogOnService está en funcionamiento.
- No deben existir firewalls entre el host de DEM y Windows Server. Para obtener información sobre el puerto, consulte [“Requisitos de puertos,”](#) página 24.
- IIS está instalado y configurado.

Requisitos de Distributed Execution Manager

Un entorno debe cumplir algunos requisitos generales que permiten la instalación de Distributed Execution Managers (DEM).

- Microsoft .NET Framework 4.5.2 está instalado.
- Microsoft PowerShell 2.0 o Microsoft PowerShell 3.0. PowerShell 2.0 se incluye en Windows Server 2008 R2 SP1 en adelante. Microsoft PowerShell 3.0 se ejecuta en Windows Server 2012 R2.
- SecondaryLogOnService está en funcionamiento.
- No hay cortafuegos entre el host del DEM y el servidor de Windows ni tampoco puertos abiertos, según se describe en [“Requisitos de puertos,”](#) página 24.

Los servidores que alojan instancias de DEM de trabajo pueden plantear más requisitos en función de los recursos de aprovisionamiento con los que interactúen.

Requisitos de Amazon Web Services EC2

El servidor de IaaS de Windows se comunica con una cuenta de Amazon EC2 y recopila datos de ella.

Cuando utiliza Amazon Web Services para el aprovisionamiento, los servidores que alojan los trabajos de DEM deben cumplir con los siguientes requisitos de configuración.

- Los hosts donde estén instalados los DEM deben tener acceso a Internet.
Si hay un firewall, debe permitirse el tráfico HTTPS con `aws.amazon.com` y con las URL que representan todas las regiones de EC2 a las que tienen acceso sus cuentas de AWS, por ejemplo, `ec2.us-east-1.amazonaws.com` para la región Este de Estados Unidos. Cada URL se resuelve en un intervalo de direcciones IP, por lo que es posible que necesite usar una herramienta, como la disponible en el sitio web de Network Solutions, para obtener una lista de estas direcciones IP y configurarlas.
- El acceso a Internet desde el host de DEM se realiza a través de un servidor proxy, y el servicio de DEM debe ejecutarse con credenciales que puedan autenticarse en el servidor proxy.

Requisitos de KVM de Red Hat Enterprise Virtualization (RHEV)

Cuando se usa Red Hat Enterprise Virtualization para el aprovisionamiento, el servidor de IaaS de Windows se comunica con esa cuenta y recopila datos de ella.

El entorno debe cumplir los siguientes requisitos de Red Hat Enterprise.

- Cada entorno de KVM (RHEV) debe estar unido al dominio que contiene el servidor de IaaS.
- Las credenciales utilizadas para administrar el endpoint que representa un entorno de KVM (RHEV) deben tener privilegios de administrador en el entorno de RHEV. Estas credenciales también deben tener privilegios suficientes para crear objetos en los hosts del entorno.

Requisitos de SCVMM

Cualquier DEM de trabajo que se use para administrar máquinas virtuales a través de SCVMM debe instalarse en un host donde ya esté instalada la consola de SCVMM.

Además, deben cumplirse los siguientes requisitos:

- DEM debe tener acceso al módulo PowerShell de SCVMM instalado con la consola.
- La política de ejecución de MS PowerShell debe estar establecida en RemoteSigned o Unrestricted.
Para obtener más información sobre la política de ejecución de PowerShell, emita uno de los siguientes comandos en el símbolo del sistema de PowerShell:

```
help about_signing
help Set-ExecutionPolicy
```

- Si todos los DEM de trabajo de la instancia no están incluidos en recursos informáticos que cumplan estos requisitos, debe utilizarse Aptitudes para dirigir todos los flujos de trabajo relacionados con SCVMM a los que sí están incluidos.

Los siguientes requisitos adicionales también se aplican a SCVMM.

- Debe instalar la consola de SCVMM antes de instalar los DEM de trabajo que consumen los elementos de trabajo de SCVMM.

Si instala el DEM de trabajo antes de la consola de SCVMM, verá errores de log similares a este:

```
Workflow 'ScvmmEndpointDataCollection' failed with the following exception: The term 'Get-
VMMServer' is not recognized as the name of a cmdlet, function, script file, or operable
program. Check the spelling of the name, or if a path was included, verify that the path is
correct and try again.
```

Para solucionar este problema, compruebe que la consola de SCVMM está instalada y reinicie el servicio de DEM de trabajo.

- Todas las instancias de SCVMM deben unirse al dominio que contiene el servidor.
- Las credenciales que se usan para administrar el endpoint que representa una instancia de SCVMM deben tener privilegios de administrador en el servidor de SCVMM. Estas credenciales también deben tener privilegios de administrador en los servidores de Hyper-V en la instancia.
- Los servidores de Hyper-V en una instancia de SCVMM que vaya a administrarse deben ser servidores de Windows Server 2008 R2 SP1 y deben tener instalado Hyper-V. El procesador debe estar equipado con las extensiones de virtualización necesarias; .NET Framework 4.5.1 o posterior debe estar instalado; y Windows Management Instrumentation (WMI) debe estar habilitado.
- Para aprovisionar máquinas en un recurso informático de SCVMM, debe añadirse un usuario en al menos una función de seguridad de la instancia de SCVMM.

Requisitos de puertos

vRealize Automation utiliza puertos designados para comunicarse y acceder a los datos.

Aunque vRealize Automation solamente usa el puerto 443 para las comunicaciones, puede haber otros puertos abiertos en el sistema. Los puertos abiertos y poco protegidos pueden dar origen a vulnerabilidades de seguridad, de modo que revíselos todos en el sistema y procure que estén abiertos solo los puertos que sean necesarios en las aplicaciones empresariales.

Dispositivo de vRealize Automation

el dispositivo de vRealize Automation utiliza los siguientes puertos.

Tabla 2-4. Puertos entrantes de el dispositivo de vRealize Automation

Puerto	Protocolo	Comentarios
22	TCP	Opcional. SSH.
80	TCP	Opcional. Redirige a 443.
111	TCP, UDP	RPC.
443	TCP	Accede a la consola de vRealize Automation y a las llamadas API.
5480	TCP	Accede a la interfaz de administración web del dispositivo virtual.
5480	TCP	Utilizado por el agente de administración.
5488, 5489	TCP	Interno. Utilizado por el dispositivo de vRealize Automation en las actualizaciones.
4369, 25672,5671,5672	TCP	Mensajes de RabbitMQ.
8230, 8280, 8281	TCP	Instancia de vRealize Orchestrator interna.
8444	TCP	Comunicación de proxy de consola para las conexiones de VMware Remote Console de vSphere.

Tabla 2-5. Puertos salientes del dispositivo de vRealize Automation

Puerto	Protocolo	Comentarios
25, 587	TCP, UDP	SMTP para enviar correos electrónicos de notificación salientes.
53	TCP, UDP	DNS.
67, 68, 546, 547	TCP, UDP	DHCP.
80	TCP	Opcional. Para obtener actualizaciones de software. Las actualizaciones se pueden descargar y aplicar por separado.
110, 995	TCP, UDP	POP para recibir correos electrónicos de notificación entrantes.
143, 993	TCP, UDP	IMAP para recibir correos electrónicos de notificación entrantes.
123	TCP, UDP	Opcional. Para conectarse directamente a NTP en vez de usar la hora del host.
443	TCP	IaaS Manager Service sobre HTTPS. Comunicación con hosts de virtualización sobre HTTPS.
902	TCP	Operaciones de copia de archivo de red de ESXi y conexiones con VMware Remote Console (VMRC).
5432	TCP, UDP	Opcional. Para comunicarse con una base de datos de dispositivo.
7444	TCP	Comunicación con el servicio de SSO sobre HTTPS.
8281	TCP	Opcional. Para comunicarse con una instancia de vRealize Orchestrator externa.

Puede que algunos complementos de vRealize Orchestrator necesiten otros puertos para comunicarse con sistemas externos. Consulte la documentación correspondiente al complemento de vRealize Orchestrator.

Infraestructura como servicio

Los puertos de las tablas Puertos entrantes de componentes de infraestructura como servicio y Puertos salientes de componentes de infraestructura como servicio deben estar disponibles para el servidor de Windows de IaaS.

Tabla 2-6. Puertos entrantes de componentes de infraestructura como servicio

Componente	Puerto	Protocolo	Comentarios
Instancia de SQL Server	1433	TCP	MSSQL.
Manager Service	443*	TCP	Comunicación con los componentes de IaaS y el dispositivo de vRealize Automation sobre HTTPS.
el dispositivo de vRealize Automation	443	TCP	Comunicación con los componentes de IaaS y el dispositivo de vRealize Automation sobre HTTPS.

*Todos los hosts de virtualización administrados por agentes de proxy también deben tener el puerto TCP 443 abierto para el tráfico entrante.

Tabla 2-7. Puertos salientes de componentes de infraestructura como servicio

Componente	Puerto	Protocolo	Comentarios
Todo	53	TCP, UDP	DNS.
Todo	67, 68, 546, 547	TCP, UDP	DHCP.
Todo	123	TCP, UDP	Opcional. NTP.
Manager Service	443	TCP	Comunicación con el dispositivo de vRealize Automation sobre HTTPS.
Sitio web	443	TCP	Comunicación con Manager Service sobre HTTPS.
Distributed Execution Managers	443	TCP	Comunicación con Manager Service sobre HTTPS.
Agentes de proxy	443	TCP	Comunicación con Manager Service y con los hosts de virtualización sobre HTTPS.
Agente invitado	443	TCP	Comunicación con Manager Service sobre HTTPS.
Manager Service, sitio web	1433	TCP	MSSQL.

Servicio Coordinador de transacciones distribuidas de Microsoft

Además de constatar que los puertos reflejados en las tablas anteriores están libres para su uso, también debe habilitar la comunicación del Servicio Coordinador de transacciones distribuidas de Microsoft (MS DTC) entre todos los servidores de la implementación. MS DTC requiere el uso del puerto 135 sobre TCP y de un puerto aleatorio entre 1024 y 65535.

El Comprobador de requisitos previos valida si MS DTC se está ejecutando y si los puertos necesarios están abiertos.

Cuentas de usuario y credenciales necesarias para la instalación

Debe comprobar que cuenta con las funciones y las credenciales necesarias para instalar componentes de vRealize Automation.

Cuenta de servicio de vCenter

Si tiene previsto usar un endpoint de vSphere, necesita una cuenta de dominio o local que tenga el nivel de acceso adecuado configurado en vCenter.

Instalación de dispositivos virtuales

Para implementar el dispositivo de vRealize Automation, debe tener privilegios adecuados en la plataforma de implementación (por ejemplo, credenciales de administrador de vSphere).

Durante el proceso de implementación, se especifica la contraseña para la cuenta de administrador del dispositivo virtual. Esta cuenta proporciona acceso a la consola de administración de el dispositivo de vRealize Automation desde la que se configuran y administran los dispositivos virtuales.

Instalación de IaaS

Antes de instalar componentes de IaaS, añada el usuario con el que tiene previsto ejecutar los programas de instalación de IaaS al grupo de administrador en el host de instalación.

Credenciales de base de datos de IaaS

Se puede crear la base de datos durante la instalación del producto o manualmente en el servidor de SQL.

Cuando se crea o se rellena una base de datos de MS SQL con vRealize Automation, ya sea mediante el Asistente de instalación o la consola de administración, se aplican los siguientes requisitos:

- Si utiliza la opción **Usar autenticación de Windows**, la función **sysadmin** de SQL Server se debe conceder al usuario que ejecuta el agente de administración en el servidor web de IaaS principal para crear y modificar el tamaño de la base de datos.
- Si no selecciona la opción **Usar autenticación de Windows**, la función **sysadmin** de SQL Server también se debe conceder al usuario que ejecuta el agente de administración en el servidor web de IaaS principal. Las credenciales se usan en tiempo de ejecución.
- Si rellena una base de datos creada previamente con vRealize Automation, las credenciales de usuario que proporcione (ya sea el usuario de Windows actual o el usuario de SQL especificado) solo necesitarán privilegios de **dbo** para la base de datos de IaaS.

NOTA: Los usuarios de vRealize Automation también necesitan el nivel correcto de acceso de autenticación de Windows para iniciar sesión en vRealize Automation y utilizarlo.

Credenciales de usuario del servicio de IaaS

IaaS instala varios servicios de Windows que comparten un mismo usuario de servicio.

Se aplican los siguientes requisitos al usuario de servicio de los servicios de IaaS:

- El usuario debe ser un usuario de dominio.
- El usuario debe tener privilegios de administrador local en todos los hosts en los que esté instalado el componente Manager Service o Website. No realice una instalación de grupo de trabajo.
- El usuario está configurado con privilegios **Iniciar sesión como servicio**. Este privilegio garantiza que Manager Service se inicie y genere archivos log.
- El usuario debe tener privilegios **dbo** para la base de datos de IaaS. Si utiliza el instalador para crear la base de datos, asegúrese de que se añada el inicio de sesión de usuario de servicio a SQL Server antes de ejecutar el instalador. El instalador concede privilegios **dbo** al usuario de servicio después de crear la base de datos.
- El instalador se ejecuta en la cuenta que ejecuta el agente de administración en el servidor web principal. Si desea utilizar el instalador para crear una base de datos de MS SQL durante la instalación, debe tener la función **sysadmin** habilitada en MS SQL. Esto no es un requisito si decide usar una base de datos vacía creada previamente.
- La cuenta de usuario de dominio que tiene previsto usar como identidad del grupo de aplicaciones de IIS para Model Manager Web Service se configura con privilegios **Iniciar sesión como un trabajo por lotes**.

Especificaciones del servidor de Model Manager

Especifique el nombre del servidor de Model Manager con un nombre de dominio completo (FQDN). No utilice una dirección IP para especificar el servidor.

Seguridad

vRealize Automation usa SSL para asegurar la comunicación segura entre los componentes. Las frases de contraseña se usan para el almacenamiento de bases de datos seguro.

Para obtener más información, consulte [“Requisitos de confianza de certificados en una implementación distribuida,”](#) página 63.

Certificados

vRealize Automation usa certificados SSL para garantizar la comunicación segura entre los componentes e instancias de IaaS de el dispositivo de vRealize Automation. Los dispositivos y las máquinas que tienen instalado Windows intercambian estos certificados para establecer una conexión de confianza. Puede obtener certificados de una entidad de certificación interna o externa, o generar certificados autofirmados durante el proceso de implementación de cada componente.

Para obtener información importante sobre la solución de problemas, la compatibilidad y los requisitos de confianza de los certificados, consulte el artículo de la base de conocimientos de VMware en <http://kb.vmware.com/kb/2106583>.

Puede actualizar o reemplazar certificados después de la implementación. Por ejemplo, puede ser que un certificado caduque o que elija utilizar certificados autofirmados durante la implementación inicial, pero que quiera obtener los certificados de una entidad de certificación de confianza antes de poner en marcha la implementación de vRealize Automation.

Tabla 2-8. Implementaciones de certificados

Componente	Implementación mínima (no para producción)	Implementación distribuida (lista para producción)
Dispositivo de vRealize Automation	Genere un certificado autofirmado durante la configuración de dispositivos.	Puede usar un certificado de una autoridad de certificación interna o externa para cada clúster de dispositivos. Los certificados multiuso y de comodín son compatibles.
Componentes de IaaS	Durante la instalación, acepte los certificados autofirmados que se han generado o seleccione la supresión de certificados.	Obtenga un certificado multiuso, como un certificado SAN (nombre alternativo del firmante), de una entidad de certificación interna o externa en la que confíe su cliente web.

Cadenas de certificados

Si utiliza cadenas de certificados, especifique los certificados en el siguiente orden:

- Certificado de cliente/servidor firmado por un certificado de CA intermedia
- Uno o más certificados intermedios
- Un certificado de CA raíz

Incluya el encabezado BEGIN CERTIFICATE y el pie de página END CERTIFICATE en todos los certificados cuando los importe.

Extraer certificados y claves privadas

Los certificados que se usan con los dispositivos virtuales deben tener el formato de archivo PEM.

Los ejemplos recogidos en la siguiente tabla emplean comandos `openssl` de Gnu para extraer la información de certificado necesaria para configurar los dispositivos virtuales.

Tabla 2-9. Comandos y valores de certificados de ejemplo (openssl)

La entidad de certificación proporciona	Comando	Entradas de dispositivo virtual
Clave privada RSA	<code>openssl pkcs12 -in <i>path_to_pfx_certificate_file</i> -nocerts -out key.pem</code>	Clave privada RSA
Archivo PEM	<code>openssl pkcs12 -in <i>path_to_pfx_certificate_file</i> -clcerts -nokeys -out cert.pem</code>	Cadena de certificados
(Opcional) Frase de contraseña	No disponible	Frase de contraseña

Frase de contraseña de seguridad

vRealize Automation utiliza frases de contraseña de seguridad para proteger la base de datos. Una frase de contraseña es una serie de palabras que forman una frase que genera la clave de cifrado que protege los datos almacenados en la base de datos.

Siga estas directrices la primera vez que cree una frase de contraseña de seguridad.

- Utilice la misma frase de contraseña en toda la instalación para asegurarse de que todos los componentes tengan la misma clave de cifrado.
- Utilice una frase con más de ocho caracteres.
- Incluya caracteres en mayúscula y minúscula, números y símbolos.
- Memorice la frase de contraseña o guárdela en un lugar seguro. La frase de contraseña es obligatoria para restaurar la información de la base de datos si se produce un fallo del sistema o si se añaden componentes tras la instalación. Sin la frase de contraseña no será posible realizar la restauración correctamente.

Software de terceros

Algunos componentes de vRealize Automation dependen de software de terceros, como Microsoft Windows y SQL Server. Para protegerse frente a las vulnerabilidades de seguridad de los productos de terceros, asegúrese de que el software está actualizado con las últimas revisiones del proveedor.

Sincronización de hora

Un administrador del sistema debe configurar el cronometraje de forma precisa como parte de la instalación de vRealize Automation.

La instalación no se realiza correctamente si la configuración de la sincronización de hora no es correcta.

El cronometraje debe ser coherente y estar sincronizado en todos los servidores de Windows y el dispositivo de vRealize Automation. Para lograr esta coherencia, utilice el mismo método de cronometraje en todos los componentes.

En máquinas virtuales, puede utilizar los siguientes métodos:

- Configuración mediante el protocolo de hora de red (directamente)

- Configuración mediante el protocolo de hora de red a través de ESXi con VMware Tools. El protocolo de hora de red debe estar configurado en ESXi.

En lo referente a servidores de Windows, consulte las [prácticas recomendadas sobre cronometraje para Windows, incluido el protocolo de hora de red](#).

Instalar vRealize Automation con el Asistente de instalación

3

El Asistente de instalación de vRealize Automation proporciona una forma sencilla y rápida de instalar implementaciones mínimas o empresariales.

Antes de iniciar el asistente, debe implementar un el dispositivo de vRealize Automation, configurar los servidores de Windows para cumplir los requisitos previos de instalación y comprobar que todos los dispositivos y los servidores usen el mismo método de cronometraje.

Desplazamiento por el asistente

El asistente de instalación aparece la primera vez que se inicia sesión en el dispositivo de vRealize Automation. Si desea detener el asistente y volver más tarde, cierre sesión con el botón **Cerrar sesión** que aparece en cada pantalla. Use el botón **Cancelar** para salir del asistente e instalar a través de la consola de administración. El asistente se deshabilita al hacer clic en **Cancelar**, o cuando se cierra la sesión en el asistente y se inicia la instalación en la consola de administración.

Use los botones **Anterior** y **Siguiente** para desplazarse por las pantallas del asistente.

Este capítulo cubre los siguientes temas:

- [“Implementar el dispositivo de vRealize Automation,”](#) página 31
- [“Instalar una implementación mínima con el asistente de instalación,”](#) página 32
- [“Instalar una implementación empresarial con el asistente de instalación,”](#) página 41

Implementar el dispositivo de vRealize Automation

Para implementar el dispositivo de vRealize Automation, un administrador del sistema debe iniciar sesión en el cliente de vSphere y seleccionar una configuración de implementación.

Existen algunas restricciones para la contraseña raíz que se crea para el administrador de vRealize Automation. Consulte [“Consideraciones sobre las contraseñas,”](#) página 20.

Prerequisitos

- Descargue el dispositivo de vRealize Automation del sitio web de VMware.
- Inicie sesión en el cliente de vSphere como usuario con privilegios de administrador del sistema.

Procedimiento

- 1 Seleccione **Archivo > Implementar plantilla de OVF** en el cliente de vSphere.
- 2 Vaya al archivo de el dispositivo de vRealize Automation que descargó y haga clic en **Abrir**.
- 3 Haga clic en **Siguiente**.

- 4 Haga clic en **Siguiente** en la página de detalles de plantilla de OVF.
- 5 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 6 En el cuadro de texto **Nombre**, especifique un nombre único de dispositivo virtual respetando la convención de nomenclatura de TI de su organización, seleccione el centro de datos y la ubicación donde quiera implementar el dispositivo y haga clic en **Siguiente**.
- 7 Siga las indicaciones hasta que se abra la página Formato de disco.
- 8 Compruebe en esta página que hay espacio en disco suficiente para implementar el dispositivo virtual y haga clic en **Siguiente**.
- 9 Siga las indicaciones hasta llegar a la página Propiedades.
Las opciones que aparecen dependen de la configuración de vSphere.
- 10 Configure los valores en la página Propiedades.
 - a Especifique la contraseña raíz que va a usar para iniciar sesión en la consola de dispositivo virtual en los cuadros de texto **Escribir contraseña** y **Confirmar contraseña**.
 - b Active o desactive la casilla **Servicio de SSH** para determinar si el servicio de SSH va a estar habilitado en el dispositivo.

Este valor se usa para establecer el estado inicial del servicio de SSH en el dispositivo. Si va a realizar la instalación con el asistente de instalación, habilítelo antes de iniciar el asistente. Puede cambiar este valor desde la consola de administración del dispositivo después de la instalación.
 - c Especifique el nombre de dominio completo de la máquina virtual en el cuadro de texto **Nombre de host**, aun cuando esté usando DHCP.
 - d Configure las propiedades de la red.
- 11 Haga clic en **Siguiente**.
- 12 Según la configuración de vCenter y DNS, la resolución de DNS podría tardar bastante tiempo. Para acelerar este proceso, lleve a cabo los siguientes pasos.
 - Si **Encender tras implementación** está disponible en la página Listo para completar:
 - a Seleccione **Encender tras implementación** y haga clic en **Finalizar**.
 - b Haga clic en **Cerrar** cuando el archivo termine de implementarse en vCenter.
 - c Espere a que la máquina se inicie.
Esto puede tardar hasta cinco minutos.
 - Si **Encender tras implementación** no está disponible en la página Listo para completar:
 - a Haga clic en **Cerrar** cuando el archivo termine de implementarse en vCenter.
 - b Encienda la máquina virtual y espere un rato hasta que esta se inicie.
 - c Compruebe que puede hacer ping al DNS de la máquina virtual. Si no puede hacer ping al DNS, reinicie la máquina virtual.
 - d Espere a que la máquina se inicie. Esto puede tardar hasta cinco minutos.
- 13 Abra un símbolo del sistema y haga ping al FQDN para confirmar que el nombre de dominio completo se puede resolver en la dirección IP de el dispositivo de vRealize Automation.

Instalar una implementación mínima con el asistente de instalación

Ejecutar el asistente de instalación para una implementación mínima

Instale una implementación mínima para un trabajo de prueba de concepto. El asistente para la instalación mínima presupone que se están instalando todos los componentes de IaaS en una sola máquina Windows.

Las implementaciones mínimas suelen admitir un solo el dispositivo de vRealize Automation, un servidor de IaaS y utilizan un agente de vSphere para admitir los endpoints.

Prerequisitos

- Compruebe que cumpla los requisitos previos descritos en [Capítulo 2, “Preparar la instalación,”](#) página 19
- [“Implementar el dispositivo de vRealize Automation,”](#) página 65
-

Procedimiento

- 1 Abra un navegador web.
- 2 Vaya a la consola de administración de el dispositivo de vRealize Automation utilizando su nombre de dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 3 Inicie sesión con el nombre de usuario **root** y la contraseña que especificó cuando se implementó el dispositivo.
- 4 Cuando aparezca el asistente de instalación, haga clic en **Siguiente**.
- 5 Acepte el Contrato de licencia para el usuario final y haga clic en **Siguiente**.
- 6 Seleccione **Implementación mínima e Instalar infraestructura como servicio** en la pantalla Tipo de implementación, y haga clic en **Siguiente**.
- 7 Compruebe que se cumplan los requisitos previos enumerados en la página de requisitos previos de la instalación y que los servidores de Windows en los que haya instalado un agente de administración aparecen en la lista.
- 8 Si es necesario, puede cambiar el método de cronometraje de su dispositivo vRealize Automation. Haga clic en **Cambiar configuración de tiempo** si realiza cambios.
- 9 Haga clic en **Siguiente**.
- 10 Haga clic en **Ejecutar** en la pantalla Ejecutar el Comprobador de requisitos previos para comprobar que los servidores de Windows de su implementación estén correctamente configurados para el uso de vRealize Automation.
Este paso puede tardar unos minutos en ejecutarse, ya que se ejecuta de forma remota.
 - a Si una máquina devuelve un estado de error, haga clic en **Corregir** para iniciar las correcciones automáticas o haga clic en **Mostrar detalles** y siga las instrucciones. Las correcciones automáticas también se reinician.
 - b Haga clic en **Ejecutar** para volver a ejecutar el comprobador.
 - c Cuando todos los estados sean correctos, haga clic en **Siguiente**.
- 11 Continúe con las siguientes pantallas y proporcione la información requerida para configurar los componentes de la implementación, como los datos del servidor web, Manager Service, Distributed Execution Manager, agente de proxy de vSphere y los certificados.

Los botones de ayuda proporcionan información adicional.

Qué hacer a continuación

[“Crear snapshots antes de comenzar la instalación,”](#) página 38

Instalar el agente de administración

Debe instalar un agente de administración en cada máquina de Windows que aloje componentes de IaaS.

Las instalaciones empresariales no necesitan un agente de administración para el host MS SQL.

Si se produce un error en el dispositivo principal de vRealize Automation, deberá volver a instalar los agentes de administración.

Los agentes de administración no se eliminan automáticamente al desinstalar un componente de IaaS. Para desinstalar el agente de administración, utilice la herramienta Agregar o quitar programas, tal y como haría para desinstalar cualquier programa de Windows.

Procedimiento

- 1 [Buscar la huella digital del certificado de SSL para el servicio del sitio de administración](#) página 34
Al instalar un agente de administración, debe validar la huella digital del certificado de SSL para el servicio del sitio de administración.
- 2 [Descargar e instalar un agente de administración](#) página 35
El administrador descarga e instala un agente de administración en las máquinas de IaaS de la implementación. El agente de administración debe instalarse en todos los servidores IaaS, salvo en aquellos que se usen exclusivamente para la base de datos de MS SQL.

Buscar la huella digital del certificado de SSL para el servicio del sitio de administración

Al instalar un agente de administración, debe validar la huella digital del certificado de SSL para el servicio del sitio de administración.

Puede obtener la huella digital en el símbolo del sistema en el dispositivo de vRealize Automation.

Procedimiento

- 1 Inicie sesión en la consola del dispositivo de vRealize Automation como raíz.
- 2 Escriba el siguiente comando:

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```

Aparece la huella digital de SHA1. Por ejemplo:

```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```
- 3 Copie el UID de la huella digital. Es posible que deba eliminar los dos puntos para realizar la validación.

Qué hacer a continuación

Conserve la huella digital que ha copiado para usarla con el instalador del agente de administración.

Descargar e instalar un agente de administración

El administrador descarga e instala un agente de administración en las máquinas de IaaS de la implementación. El agente de administración debe instalarse en todos los servidores IaaS, salvo en aquellos que se usen exclusivamente para la base de datos de MS SQL.

El agente de administración registra los nodos de IaaS con el dispositivo de vRealize Automation, automatiza la instalación y la administración de componentes de IaaS, y recopila información de soporte y telemetría. El agente de administración se ejecuta como un servicio de Windows en la máquina de IaaS y se necesitan derechos de administrador local para poder instalar el agente.

Prerequisitos

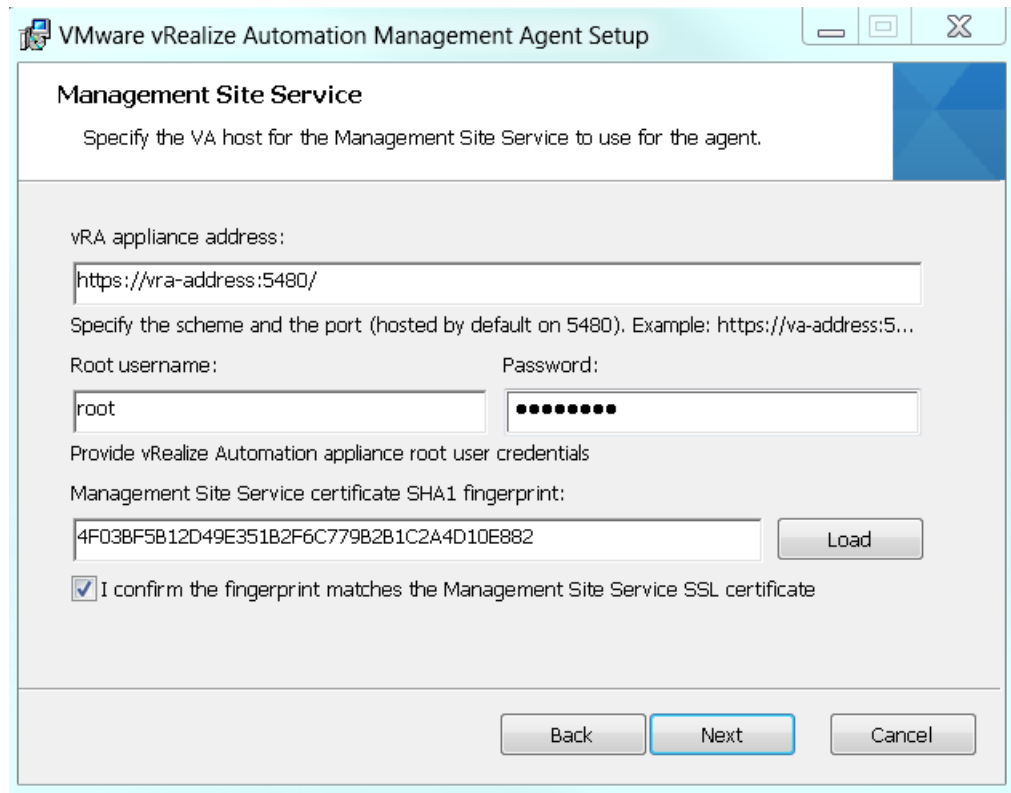
- [“Buscar la huella digital del certificado de SSL para el servicio del sitio de administración,”](#) página 34
- Compruebe que el usuario de la cuenta del servicio o el usuario de dominio formen parte del grupo de administradores local de cada máquina de IaaS.

Procedimiento

- 1 Abra el dispositivo de vRealize Automation especificando una dirección con el siguiente formato en un navegador web, donde *vra-va-hostname.domain.name* es el nombre de dominio completo de su el dispositivo de vRealize Automation. No use una dirección de equilibrador de carga.
`https://vra-va-hostname.domain.name:5480/installer`
- 2 Haga clic en el **instalador del agente de administración** para descargar el instalador.
- 3 Ejecute el instalador del agente de administración: vCAC-IaaSManagementAgent-Setup.msi.
La ubicación predeterminada es *%Program Files(x86)%\VMware\vCAC\Management Agent*
- 4 Haga clic en **Siguiente** en la página de bienvenida.
- 5 Acepte el CLUF y haga clic en **Siguiente**.
- 6 Indique una ruta de instalación alternativa o acepte el valor predeterminado.
- 7 Haga clic en **Siguiente**.
- 8 Escriba los detalles del servicio del sitio de administración para los siguientes campos y haga clic en **Siguiente**.

Cuadro de texto	Entrada
Dirección del dispositivo vRA	<code>https://vra-va-hostname.domain.name:5480</code> Debe especificar el número de puerto.
Nombre de usuario raíz	El usuario raíz para el el dispositivo de vRealize Automation.
Contraseña	La contraseña del usuario raíz para el el dispositivo de vRealize Automation.

Cuadro de texto	Entrada
Certificado del servidor del sitio de administración	La huella digital SHA1 para el certificado del servicio del sitio de administración. El servicio del sitio de administración se aloja en el dispositivo de vRealize Automation. Muestra de una huella digital SHA1: DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78.
Cargar	Haga clic en Cargar para cargar la huella digital predeterminada.



- 9 Seleccione la casilla **Confirmación de coincidencia de huella digital** después de confirmar que la huella digital que se muestra coincide con la huella digital del certificado SSL del sitio de administración.
Si las huellas digitales no coinciden, compruebe si es correcta la dirección en el cuadro de texto **Dirección del dispositivo vRA**.
- 10 Haga clic en **Siguiente**.
- 11 Escriba el nombre de usuario y la contraseña de la cuenta de servicio.
- 12 Haga clic en **Siguiente**.
- 13 Haga clic en **Instalar**.
- 14 Haga clic en **Finalizar**.
- 15 Repita estos pasos para cada host de Windows IaaS.

Después de instalar el agente de administración, el servidor de Windows se muestra en la página Requisitos previos de instalación del asistente de instalación.

Sincronizar la hora de los servidores

Los relojes de los servidores de vRealize Automation y de Windows deben estar sincronizados para que la instalación se realice correctamente.

Las opciones de la página Requisitos previos del Asistente de instalación le permiten seleccionar un método de sincronización de hora para los dispositivos virtuales. La tabla del host de IaaS le informa de los desplazamientos de hora.

Procedimiento

- 1 Seleccione una opción del menú **Modo de sincronización de hora**.

Opción	Acción
Usar servidor horario	Seleccione Usar servidor horario del menú Modo de sincronización de hora para usar el protocolo de tiempo de redes. Por cada servidor horario que utilice, especifique la dirección IP o el nombre de host correspondiente en el cuadro de texto Servidor horario .
Usar hora de host	Seleccione Usar hora de host del menú Modo de sincronización de hora para usar la sincronización de hora de VMware Tools. Para poder usar la sincronización de hora de VMware Tools, deberá configurar las conexiones con los servidores del protocolo de tiempo de redes.

- 2 Haga clic en **Cambiar configuración de hora**.
- 3 Haga clic en **Siguiente**.

Qué hacer a continuación

Compruebe que los servidores de IaaS se han configurado correctamente.

Ejecutar el Comprobador de requisitos previos

Ejecute el Comprobador de requisitos previos para verificar que el servidor de Windows para los componentes de IaaS se ha configurado correctamente.

Procedimiento

- 1 Haga clic en **Ejecutar** en la pantalla del Comprobador de requisitos previos.
A medida que finalizan las comprobaciones, cada servidor de Windows para los componentes de IaaS se muestra con un estado.
- 2 Si ve una advertencia, puede obtener más información sobre el error o decidir si desea solucionarlo automáticamente.
 - ◆ Haga clic en **Mostrar detalles** para obtener más información sobre el error y sobre los pasos que debe seguir para solucionarlo.
 - ◆ Haga clic en **Corregir** para solucionar el error automáticamente. También se reiniciará la máquina con Windows si es necesario.
- 3 Haga clic en **Ejecutar** para verificar las correcciones.
- 4 Haga clic en **Siguiente** cuando se hayan resuelto todos los errores.

Los servidores de Windows se han configurado correctamente para la instalación de los componentes de IaaS.

Qué hacer a continuación

Vaya a la página del host de vRealize Automation.

Especificar los parámetros de configuración de la implementación

Especifique los parámetros de configuración para los componentes de la implementación.

Prerequisitos

Procedimiento

- 1 En la página del host de vRealize Automation, especifique el host.
 - Haga clic en Resolver automáticamente para que vRealize Automation proporcione la dirección predeterminada.
 - Haga clic en Introducir host y escriba el alias DNS o el FQDN de otro host.
- 2 Haga clic en Siguiente.
- 3 En la página Single Sign-On, escriba la contraseña del administrador del sistema de la cuenta de tenant predeterminada; para confirmarla vuelva a escribirla.
- 4 Haga clic en Siguiente.
- 5 Avance por las siguientes pantallas y utilice la ayuda contextual si necesita información adicional.
- 6 Haga clic en Siguiente cuando haya completado la pantalla de validación.

Qué hacer a continuación

Cree un snapshot de las máquinas antes de iniciar la instalación del producto.

Crear snapshots antes de comenzar la instalación

Tome snapshots de todos los dispositivos y los servidores de Windows. Si la instalación no se realiza correctamente, podrá volver a dichos snapshots e intentar la instalación de nuevo.

Los snapshots conservan el trabajo de configuración. Asegúrese de incluir un snapshot del el dispositivo de vRealize Automation en el que ejecute el asistente.

Se proporcionan instrucciones para los usuarios de vSphere.

NOTA: No salga del asistente de instalación ni cancele la instalación.

Procedimiento

- 1 Abra otro navegador e inicie sesión en vSphere Client.
- 2 Busque el servidor o el dispositivo en el inventario de vSphere Client.
- 3 Haga clic con el botón derecho en el servidor en el inventario y seleccione **Tomar snapshot**.
- 4 Especifique un nombre de snapshot.
- 5 Active la casilla **Crear snapshot de la memoria de la máquina virtual** para capturar la memoria del servidor y haga clic en **Aceptar**.

El snapshot se ha creado.

Repita estos pasos para crear snapshots de cada uno de los servidores o dispositivos.

Qué hacer a continuación

["Finalizar la instalación,"](#) página 60

Escenario: Finalizar la instalación

El administrador de vSphere es el último eslabón en el proceso de instalación. Es quien inicia la instalación de vRealize Automation y espera a que finalice correctamente.

Procedimiento

- 1 Vuelva al asistente de instalación.
- 2 Revise el resumen de la instalación y haga clic en **Siguiente**.
- 3 Escriba la clave de licencia del producto y haga clic en **Siguiente**.
- 4 Acepte o cambie la configuración de telemetría predeterminada y haga clic en **Siguiente**.
- 5 Haga clic en **Siguiente**.
- 6 Haga clic en **Finalizar**.

De este modo, se inicia la instalación. Según cuál sea la configuración de red, la instalación puede tardar entre quince minutos y una hora.

Cuando la instalación finalice, se mostrará un mensaje de confirmación.

Qué hacer a continuación

Ya está listo para configurar la implementación.

Fallos de instalación de dirección

Cuando instale desde la página de Detalles de instalación, se le informará de los problemas que impidan que la instalación finalice.

Cuando se detectan problemas, se marca el componente y se le ofrece información detallada acerca del fallo, junto con los pasos para investigar las soluciones. Cuando haya solucionado el problema, deberá reintentar el paso de instalación. En función del tipo de fallo, debe seguir diferentes pasos de resolución.

Procedimiento

- 1 Si el botón **Error al reintentar** está habilitado, siga estos pasos.
 - a Revise el error.
 - b Evalúe qué se debe cambiar y haga los cambios necesarios.
 - c Vuelva a la pantalla de instalación y haga clic en **Error al reintentar**.
El instalador no intentará volver a instalar todos los componentes que hayan fallado.
- 2 Si el botón **Reintentar todos IaaS** está habilitado, siga estos pasos.
 - a Revise el error.
 - b Evalúe qué se debe cambiar.
 - c Devuelva todos los servidores de IaaS a los snapshots que ha creado anteriormente.
 - d Elimine la base de datos MS SQL si usa una base de datos externa.
 - e Realice los cambios necesarios.
 - f Haga clic en **Reintentar todos IaaS**.

- 3 Si el error está en los componentes de dispositivos virtuales, siga estos pasos.
 - a Revise el error.
 - b Evalúe qué se debe cambiar.
 - c Revierta todos los servidores a snapshots, incluido el servidor en el que esté ejecutando el asistente.
 - d Realice los cambios necesarios.
 - e Actualice la página del asistente.
 - f Inicie sesión y vuelva a ejecutar el asistente.

El asistente se abrirá en el paso anterior a la instalación.

Configurar las credenciales de la configuración de contenido inicial

Además, si lo desea, puede iniciar un flujo de trabajo de contenido inicial para un endpoint de vSphere.

El proceso utiliza un usuario local llamado configurationadmin al que se asignan derechos de administrador.

Procedimiento

- 1 Cree y escriba una contraseña para la cuenta configurationadmin en el cuadro de texto **Contraseña**.
- 2 Vuelva a escribir la contraseña en el cuadro de texto **Confirmar contraseña**. Tome nota de la contraseña para usarla más tarde.
- 3 Haga clic en **Crear contenido inicial**.
- 4 Haga clic en **Siguiente**.

Se crearán un usuario administrador de configuración y un elemento del catálogo de configuración en el tenant predeterminado. El administrador de configuración ostenta los siguientes derechos:

- Administrador de aprobaciones
- Administrador del catálogo
- Administrador de IaaS
- Arquitecto de infraestructura
- Administrador de tenants
- Arquitecto XaaS

Qué hacer a continuación

- Cuando finalice el asistente, podrá iniciar sesión en el tenant predeterminado como el usuario configurationadmin y solicitar los elementos del catálogo de contenido inicial. Para ver un ejemplo de cómo solicitar el elemento y completar la acción de usuario manual, consulte *Instalación y configuración de vRealize Automation para el escenario de Rainpole*.
- Configure el acceso al tenant predeterminado para otros usuarios. Consulte [Capítulo 5, “Configurar el acceso al tenant predeterminado,”](#) página 121.

Instalar una implementación empresarial con el asistente de instalación

Puede adecuar la implementación empresarial a las necesidades de su organización. Una implementación empresarial puede constar de componentes distribuidos o de implementaciones de alta disponibilidad configuradas con equilibradores de carga.

Las implementaciones empresariales se han diseñado para estructuras de instalación más complejas con componentes distribuidos y redundantes, y suelen incluir equilibradores de carga. La instalación de componentes de IaaS es opcional en cualquier tipo de implementación.

Para implementaciones con equilibrio de carga, la existencia de varias instancias de servidores web activos y dispositivos de el dispositivo de vRealize Automation puede generar errores en la instalación. Durante la instalación, solo deben estar activos una instancia de servidor web y un solo el dispositivo de vRealize Automation.

Ejecutar el asistente de instalación para una implementación empresarial

Las implementaciones empresariales se utilizan para entornos de producción. Puede utilizar el asistente de instalación para implementar una instalación distribuida o una instalación distribuida con equilibradores de carga para alta disponibilidad y conmutación por error.

Si realiza una instalación distribuida con equilibradores de carga para alta disponibilidad y conmutación por error, notifique al equipo responsable de configurar su entorno de vRealize Automation. Sus administradores de tenants deben configurar la administración de directorios para alta disponibilidad cuando configuren el vínculo a Active Directory.

Prerequisitos

- Compruebe que cumpla los requisitos previos descritos en [Capítulo 2, “Preparar la instalación,”](#) página 19
- [“Implementar el dispositivo de vRealize Automation,”](#) página 65.

Procedimiento

- 1 Abra un navegador web.
- 2 Vaya a la consola de administración de el dispositivo de vRealize Automation utilizando su nombre de dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 3 Inicie sesión con el nombre de usuario **root** y la contraseña que especificó cuando se implementó el dispositivo.
- 4 El asistente de instalación aparece la primera vez que se inicia sesión en el dispositivo.
- 5 Acepte el Contrato de licencia para el usuario final y haga clic en **Siguiente**.
- 6 Seleccione **Implementación empresarial** e **Instalar infraestructura como servicio** en la pantalla Tipo de implementación y haga clic en **Siguiente**.
- 7 Compruebe que se cumplan los requisitos previos enumerados en la página de requisitos previos de la instalación y que los servidores de Windows en los que haya instalado un agente de administración aparecen en la lista.
- 8 Si es necesario, puede cambiar el método de cronometraje de su dispositivo vRealize Automation. Haga clic en **Cambiar configuración de tiempo** si realiza cambios.
- 9 Haga clic en **Siguiente**.

Instalar el agente de administración

Debe instalar un agente de administración en cada máquina de Windows que aloje componentes de IaaS.

Si se produce un error en el dispositivo principal de vRealize Automation, deberá volver a instalar los agentes de administración.

Los agentes de administración no se eliminan automáticamente al desinstalar un componente de IaaS. Para desinstalar el agente de administración, utilice la herramienta Agregar o quitar programas, tal y como haría para desinstalar cualquier programa de Windows.

Buscar la huella digital del certificado de SSL para el servicio del sitio de administración

Al instalar un agente de administración, debe validar la huella digital del certificado de SSL para el servicio del sitio de administración.

Puede obtener la huella digital en el símbolo del sistema en el dispositivo de vRealize Automation.

Procedimiento

- 1 Inicie sesión en la consola del dispositivo de vRealize Automation como raíz.
- 2 Escriba el siguiente comando:


```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```

 Aparece la huella digital de SHA1. Por ejemplo:


```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```
- 3 Copie el UID de la huella digital. Es posible que deba eliminar los dos puntos para realizar la validación.

Qué hacer a continuación

Conserve la huella digital que ha copiado para usarla con el instalador del agente de administración.

Descargar e instalar un agente de administración

El administrador descarga e instala un agente de administración en las máquinas de IaaS de la implementación. El agente de administración debe instalarse en todos los servidores IaaS, salvo en aquellos que se usen exclusivamente para la base de datos de MS SQL.

El agente de administración registra los nodos de IaaS con el dispositivo de vRealize Automation, automatiza la instalación y la administración de componentes de IaaS, y recopila información de soporte y telemetría. El agente de administración se ejecuta como un servicio de Windows en la máquina de IaaS y se necesitan derechos de administrador local para poder instalar el agente.

Prerequisitos

- [“Buscar la huella digital del certificado de SSL para el servicio del sitio de administración,”](#) página 34
- Compruebe que el usuario de la cuenta del servicio o el usuario de dominio formen parte del grupo de administradores local de cada máquina de IaaS.

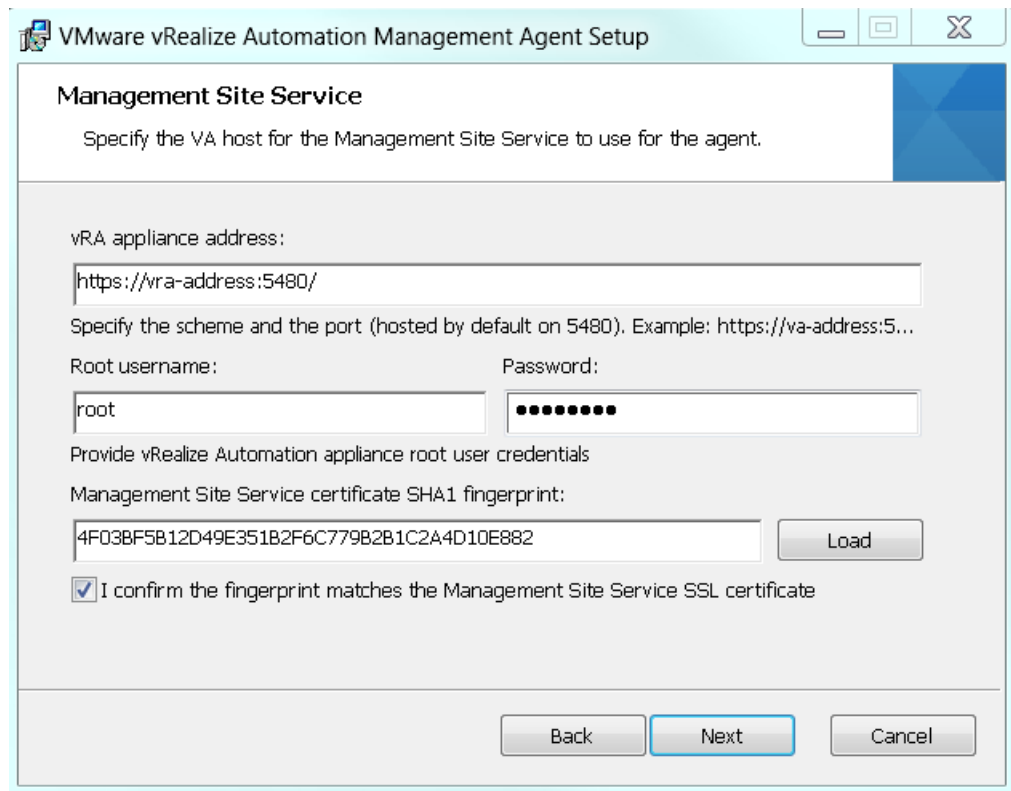
Procedimiento

- 1 Abra el dispositivo de vRealize Automation especificando una dirección con el siguiente formato en un navegador web, donde *vra-va-hostname.domain.name* es el nombre de dominio completo de su dispositivo de vRealize Automation. No use una dirección de equilibrador de carga.

```
https://vra-va-hostname.domain.name:5480/installer
```

- 2 Haga clic en el **instalador del agente de administración** para descargar el instalador.
- 3 Ejecute el instalador del agente de administración: vCAC-IaaSManagementAgent-Setup.msi.
La ubicación predeterminada es %Program Files(x86)%\VMware\vCAC\Management Agent\
4 Haga clic en **Siguiente** en la página de bienvenida.
- 5 Acepte el CLUF y haga clic en **Siguiente**.
- 6 Indique una ruta de instalación alternativa o acepte el valor predeterminado.
- 7 Haga clic en **Siguiente**.
- 8 Escriba los detalles del servicio del sitio de administración para los siguientes campos y haga clic en **Siguiente**.

Cuadro de texto	Entrada
Dirección del dispositivo vRA	https://vra-va-hostname.domain.name:5480 Debe especificar el número de puerto.
Nombre de usuario raíz	El usuario raíz para el el dispositivo de vRealize Automation.
Contraseña	La contraseña del usuario raíz para el el dispositivo de vRealize Automation.
Certificado del servidor del sitio de administración	La huella digital SHA1 para el certificado del servicio del sitio de administración. El servicio del sitio de administración se aloja en el dispositivo de vRealize Automation. Muestra de una huella digital SHA1: DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78.
Cargar	Haga clic en Cargar para cargar la huella digital predeterminada.



- 9 Seleccione la casilla **Confirmación de coincidencia de huella digital** después de confirmar que la huella digital que se muestra coincide con la huella digital del certificado SSL del sitio de administración.
Si las huellas digitales no coinciden, compruebe si es correcta la dirección en el cuadro de texto **Dirección del dispositivo vRA**.
- 10 Haga clic en **Siguiente**.
- 11 Escriba el nombre de usuario y la contraseña de la cuenta de servicio.
- 12 Haga clic en **Siguiente**.
- 13 Haga clic en **Instalar**.
- 14 Haga clic en **Finalizar**.
- 15 Repita estos pasos para cada host de Windows IaaS.

Después de instalar el agente de administración, el servidor de Windows se muestra en la página Requisitos previos de instalación del asistente de instalación.

Sincronizar la hora de los servidores

Los relojes de los servidores de vRealize Automation y de Windows deben estar sincronizados para que la instalación se realice correctamente.

Las opciones de la página Requisitos previos del Asistente de instalación le permiten seleccionar un método de sincronización de hora para los dispositivos virtuales. La tabla del host de IaaS le informa de los desplazamientos de hora.

Procedimiento

- 1 Seleccione una opción del menú **Modo de sincronización de hora**.

Opción	Acción
Usar servidor horario	Seleccione Usar servidor horario del menú Modo de sincronización de hora para usar el protocolo de tiempo de redes. Por cada servidor horario que utilice, especifique la dirección IP o el nombre de host correspondiente en el cuadro de texto Servidor horario .
Usar hora de host	Seleccione Usar hora de host del menú Modo de sincronización de hora para usar la sincronización de hora de VMware Tools. Para poder usar la sincronización de hora de VMware Tools, deberá configurar las conexiones con los servidores del protocolo de tiempo de redes.

- 2 Haga clic en **Cambiar configuración de hora**.
- 3 Haga clic en **Siguiente**.

Qué hacer a continuación

Compruebe que los servidores de IaaS se han configurado correctamente.

Ejecutar el Comprobador de requisitos previos

Ejecute el Comprobador de requisitos previos para verificar que los servidores de Windows para los componentes de IaaS se han configurado correctamente.

Procedimiento

- 1 Haga clic en **Ejecutar** en la pantalla del Comprobador de requisitos previos.

A medida que finalizan las comprobaciones, cada servidor de Windows para los componentes de IaaS se muestra con un estado.

- 2 Si ve una advertencia, puede obtener más información sobre el error o decidir si desea solucionarlo automáticamente.
 - ◆ Haga clic en **Mostrar detalles** para obtener más información sobre el error y sobre los pasos que debe seguir para solucionarlo.
 - ◆ Haga clic en **Corregir** para solucionar el error automáticamente. También se reiniciará la máquina con Windows si es necesario.
- 3 Haga clic en **Ejecutar** para verificar las correcciones.
- 4 Haga clic en **Siguiente** cuando se hayan resuelto todos los errores.

Los servidores de Windows se han configurado correctamente para la instalación de los componentes de IaaS.

Qué hacer a continuación

Vaya a la página del host de vRealize Automation.

Especificar los parámetros de configuración de la implementación

Especifique los parámetros de configuración para los componentes de la implementación.

Prerequisitos

Procedimiento

- 1 En la página del host de vRealize Automation, especifique el host.
 - Haga clic en Resolver automáticamente para que vRealize Automation proporcione la dirección predeterminada.
 - Haga clic en Introducir host y escriba el alias DNS o el FQDN de otro host.
- 2 Haga clic en Siguiente.
- 3 En la página Single Sign-On, escriba la contraseña del administrador del sistema de la cuenta de tenant predeterminada; para confirmarla vuelva a escribirla.
- 4 Haga clic en Siguiente.
- 5 Avance por las siguientes pantallas y utilice la ayuda contextual si necesita información adicional.
- 6 Haga clic en Siguiente cuando haya completado la pantalla de validación.

Qué hacer a continuación

Cree un snapshot de las máquinas antes de iniciar la instalación del producto.

Crear snapshots antes de comenzar la instalación

Tome snapshots de todos los dispositivos y los servidores de Windows. Si la instalación no se realiza correctamente, podrá volver a dichos snapshots e intentar la instalación de nuevo.

Los snapshots conservan el trabajo de configuración. Asegúrese de incluir un snapshot del dispositivo de vRealize Automation en el que ejecute el asistente.

Se proporcionan instrucciones para los usuarios de vSphere.

NOTA: No salga del asistente de instalación ni cancele la instalación.

Procedimiento

- 1 Abra otro navegador e inicie sesión en vSphere Client.

- 2 Busque el servidor o el dispositivo en el inventario de vSphere Client.
- 3 Haga clic con el botón derecho en el servidor en el inventario y seleccione **Tomar snapshot**.
- 4 Especifique un nombre de snapshot.
- 5 Active la casilla **Crear snapshot de la memoria de la máquina virtual** para capturar la memoria del servidor y haga clic en **Aceptar**.

El snapshot se ha creado.

Repita estos pasos para crear snapshots de cada uno de los servidores o dispositivos.

Qué hacer a continuación

[“Finalizar la instalación,”](#) página 60

Finalizar la instalación

Tras la creación de los snapshots, inicie la instalación de vRealize Automation y espere a que finalice correctamente.

Procedimiento

- 1 Vuelva al asistente de instalación.
- 2 Revise el resumen de la instalación y haga clic en **Siguiente**.
- 3 Haga clic en **Siguiente**.
- 4 Haga clic en **Finalizar**.

De este modo, se inicia la instalación. Según cuál sea la configuración de red, la instalación puede tardar entre quince minutos y una hora.

Cuando la instalación finalice, se mostrará un mensaje de confirmación.

Qué hacer a continuación

Ya está listo para configurar la implementación.

Fallos de instalación de dirección

Cuando instale desde la página de Detalles de instalación, se le informará de los problemas que impidan que la instalación finalice.

Cuando se detectan problemas, se marca el componente y se le ofrece información detallada acerca del fallo, junto con los pasos para investigar las soluciones. Cuando haya solucionado el problema, deberá reintentar el paso de instalación. En función del tipo de fallo, debe seguir diferentes pasos de resolución.

Procedimiento

- 1 Si el botón **Error al reintentar** está habilitado, siga estos pasos.
 - a Revise el error.
 - b Evalúe qué se debe cambiar y haga los cambios necesarios.
 - c Vuelva a la pantalla de instalación y haga clic en **Error al reintentar**.

El instalador no intentará volver a instalar todos los componentes que hayan fallado.

- 2 Si el botón **Reintentar todos IaaS** está habilitado, siga estos pasos.
 - a Revise el error.
 - b Evalúe qué se debe cambiar.
 - c Devuelva todos los servidores de IaaS a los snapshots que ha creado anteriormente.
 - d Elimine la base de datos MS SQL si usa una base de datos externa.
 - e Realice los cambios necesarios.
 - f Haga clic en **Reintentar todos IaaS**.
- 3 Si el error está en los componentes de dispositivos virtuales, siga estos pasos.
 - a Revise el error.
 - b Evalúe qué se debe cambiar.
 - c Revierta todos los servidores a snapshots, incluido el servidor en el que esté ejecutando el asistente.
 - d Realice los cambios necesarios.
 - e Actualice la página del asistente.
 - f Inicie sesión y vuelva a ejecutar el asistente.

El asistente se abrirá en el paso anterior a la instalación.

Configurar las credenciales de la configuración de contenido inicial

Además, si lo desea, puede iniciar un flujo de trabajo de contenido inicial para un endpoint de vSphere.

El proceso utiliza un usuario local llamado configurationadmin al que se asignan derechos de administrador.

Procedimiento

- 1 Cree y escriba una contraseña para la cuenta configurationadmin en el cuadro de texto **Contraseña**.
- 2 Vuelva a escribir la contraseña en el cuadro de texto **Confirmar contraseña**. Tome nota de la contraseña para usarla más tarde.
- 3 Haga clic en **Crear contenido inicial**.
- 4 Haga clic en **Siguiente**.

Se crearán un usuario administrador de configuración y un elemento del catálogo de configuración en el tenant predeterminado. El administrador de configuración ostenta los siguientes derechos:

- Administrador de aprobaciones
- Administrador del catálogo
- Administrador de IaaS
- Arquitecto de infraestructura
- Administrador de tenants
- Arquitecto XaaS

Qué hacer a continuación

- Cuando finalice el asistente, podrá iniciar sesión en el tenant predeterminado como el usuario configurationadmin y solicitar los elementos del catálogo de contenido inicial. Para ver un ejemplo de cómo solicitar el elemento y completar la acción de usuario manual, consulte *Instalación y configuración de vRealize Automation para el escenario de Rainpole*.

- Configure el acceso al tenant predeterminado para otros usuarios. Consulte [Capítulo 5, “Configurar el acceso al tenant predeterminado,”](#) página 121.

Instalar vRealize Automation mediante interfaces estándar

4

Como alternativa al asistente de instalación, puede instalar vRealize Automation mediante la consola de administración del dispositivo de vRealize Automation y el instalador manual de IaaS.

La instalación mediante la interfaz estándar está destinada principalmente a

Este capítulo cubre los siguientes temas:

- [“Implementación mínima,”](#) página 49
- [“Implementación distribuida,”](#) página 61
- [“Instalación de agentes,”](#) página 97

Implementación mínima

Puede instalar una implementación mínima independiente para utilizarla en un entorno de desarrollo o como prueba de concepto. Las implementaciones mínimas no son aptas en entornos de producción.

Lista de comprobación de implementación mínima

Un administrador del sistema puede implementar un vRealize Automation completo en una configuración mínima. Las implementaciones mínimas se suelen usar en entornos de desarrollo o como pruebas de concepto y requieren menos pasos de instalación.

La Lista de comprobación de implementación mínima proporciona un resumen de alto nivel de la secuencia de tareas que se deben llevar a cabo para completar una instalación mínima.

Imprima una copia de la lista de comprobación y utilícela para realizar un seguimiento de su trabajo a medida que se completa la instalación. Complete las tareas en el orden en que aparecen.

Tabla 4-1. Lista de comprobación de implementación mínima

Tarea	Detalles
<input type="checkbox"/> Planear y preparar el entorno de instalación, y comprobar que se cumplen todos los requisitos previos de instalación.	Capítulo 2, “Preparar la instalación,” página 19
<input type="checkbox"/> Configurar el dispositivo de vRealize Automation.	“Implementar y configurar el dispositivo de vRealize Automation,” página 50
<input type="checkbox"/> Instalar los componentes de IaaS en un solo servidor de Windows.	“Instalar componentes de IaaS,” página 55
<input type="checkbox"/> Instalar agentes adicionales, si corresponde.	“Instalación de agentes,” página 97
<input type="checkbox"/> Llevar a cabo tareas posteriores a la instalación como la configuración del tenant predeterminado.	

Implementar y configurar el dispositivo de vRealize Automation

el dispositivo de vRealize Automation es un dispositivo virtual preconfigurado que implementa la consola web (el portal de usuario) y el servidor de el dispositivo de vRealize Automation. Se proporciona como una plantilla de formato de virtualización abierta (OVF). El administrador del sistema descarga el dispositivo y lo implementa en vCenter Server o en el inventario de ESX/ESXi.

1 [Implementar el dispositivo de vRealize Automation](#) página 50

Para implementar el dispositivo de vRealize Automation, un administrador del sistema debe iniciar sesión en el cliente de vSphere y seleccionar una configuración de implementación.

2 [Habilitar la sincronización de hora en el dispositivo de vRealize Automation](#) página 51

Los relojes en el servidor de vRealize Automation y en los servidores de Windows deben estar sincronizados para que la instalación se realice correctamente.

3 [Configurar el dispositivo de vRealize Automation](#) página 52

Para preparar el el dispositivo de vRealize Automation para utilizarlo, un administrador del sistema tiene que definir la configuración del host, generar un certificado SSL y suministrar la información de conexión de SSO.

Implementar el dispositivo de vRealize Automation

Para implementar el dispositivo de vRealize Automation, un administrador del sistema debe iniciar sesión en el cliente de vSphere y seleccionar una configuración de implementación.

Existen algunas restricciones para la contraseña raíz que se crea para el administrador de vRealize Automation. Consulte [“Consideraciones sobre las contraseñas,”](#) página 20.

Prerequisitos

- Descargue el dispositivo de vRealize Automation del sitio web de VMware.
- Inicie sesión en el cliente de vSphere como usuario con privilegios de administrador del sistema.

Procedimiento

- 1 Seleccione **Archivo > Implementar plantilla de OVF** en el cliente de vSphere.
- 2 Vaya al archivo de el dispositivo de vRealize Automation que descargó y haga clic en **Abrir**.
- 3 Haga clic en **Siguiente**.
- 4 Haga clic en **Siguiente** en la página de detalles de plantilla de OVF.
- 5 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 6 En el cuadro de texto **Nombre**, especifique un nombre único de dispositivo virtual respetando la convención de nomenclatura de TI de su organización, seleccione el centro de datos y la ubicación donde quiera implementar el dispositivo y haga clic en **Siguiente**.
- 7 Siga las indicaciones hasta que se abra la página Formato de disco.
- 8 Compruebe en esta página que hay espacio en disco suficiente para implementar el dispositivo virtual y haga clic en **Siguiente**.
- 9 Siga las indicaciones hasta llegar a la página Propiedades.
Las opciones que aparecen dependen de la configuración de vSphere.

- 10 Configure los valores en la página Propiedades.
 - a Especifique la contraseña raíz que va a usar para iniciar sesión en la consola de dispositivo virtual en los cuadros de texto **Escribir contraseña** y **Confirmar contraseña**.
 - b Active o desactive la casilla **Servicio de SSH** para determinar si el servicio de SSH va a estar habilitado en el dispositivo.

Este valor se usa para establecer el estado inicial del servicio de SSH en el dispositivo. Si va a realizar la instalación con el asistente de instalación, habilítelo antes de iniciar el asistente. Puede cambiar este valor desde la consola de administración del dispositivo después de la instalación.
 - c Especifique el nombre de dominio completo de la máquina virtual en el cuadro de texto **Nombre de host**, aun cuando esté usando DHCP.
 - d Configure las propiedades de la red.
- 11 Haga clic en **Siguiente**.
- 12 Según la configuración de vCenter y DNS, la resolución de DNS podría tardar bastante tiempo. Para acelerar este proceso, lleve a cabo los siguientes pasos.
 - Si **Encender tras implementación** está disponible en la página Listo para completar:
 - a Seleccione **Encender tras implementación** y haga clic en **Finalizar**.
 - b Haga clic en **Cerrar** cuando el archivo termine de implementarse en vCenter.
 - c Espere a que la máquina se inicie.

Esto puede tardar hasta cinco minutos.
 - Si **Encender tras implementación** no está disponible en la página Listo para completar:
 - a Haga clic en **Cerrar** cuando el archivo termine de implementarse en vCenter.
 - b Encienda la máquina virtual y espere un rato hasta que esta se inicie.
 - c Compruebe que puede hacer ping al DNS de la máquina virtual. Si no puede hacer ping al DNS, reinicie la máquina virtual.
 - d Espere a que la máquina se inicie. Esto puede tardar hasta cinco minutos.
- 13 Abra un símbolo del sistema y haga ping al FQDN para confirmar que el nombre de dominio completo se puede resolver en la dirección IP de el dispositivo de vRealize Automation.

Habilitar la sincronización de hora en el dispositivo de vRealize Automation

Los relojes en el servidor de vRealize Automation y en los servidores de Windows deben estar sincronizados para que la instalación se realice correctamente.

Si aparecen advertencias de certificado durante este proceso, continúe sin problemas hasta finalizar la instalación.

Prerequisitos

[“Implementar el dispositivo de vRealize Automation,”](#) página 31.

Procedimiento

- 1 Vaya a la consola de administración de el dispositivo de vRealize Automation utilizando su nombre de dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 2 Inicie sesión con el nombre de usuario **root** y la contraseña que especificó cuando se implementó el dispositivo.
- 3 Seleccione **Administración > Configuración de hora**.

- 4 Seleccione una opción del menú **Modo de sincronización de hora**.

Opción	Acción
Usar servidor horario	Seleccione Usar servidor horario del menú Modo de sincronización de hora para usar el protocolo de tiempo de redes. Por cada servidor horario que utilice, especifique la dirección IP o el nombre de host correspondiente en el cuadro de texto Servidor horario .
Usar hora de host	Seleccione Usar hora de host del menú Modo de sincronización de hora para usar la sincronización de hora de VMware Tools. Para poder usar la sincronización de hora de VMware Tools, deberá configurar las conexiones con los servidores del protocolo de tiempo de redes.

- 5 Haga clic en **Guardar configuración**.
- 6 Haga clic en **Actualizar**.
- 7 Compruebe que el valor reflejado en **Hora actual** es correcto.
Puede cambiar la zona horaria cuando lo desee en la página Configuración de zona horaria de la pestaña **Sistema**.
- 8 (Opcional) Haga clic en **Zona horaria** en la pestaña **Sistema** y seleccione una zona horaria del sistema de entre las distintas opciones del menú.
El valor predeterminado es Etc/UTC.
- 9 Haga clic en **Guardar configuración**.

Configurar el dispositivo de vRealize Automation

Para preparar el el dispositivo de vRealize Automation para utilizarlo, un administrador del sistema tiene que definir la configuración del host, generar un certificado SSL y suministrar la información de conexión de SSO.

Prerequisitos

[“Habilitar la sincronización de hora en el dispositivo de vRealize Automation,”](#) página 51.

Procedimiento

- 1 Vaya a la consola de administración de el dispositivo de vRealize Automation utilizando su nombre de dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 2 Continúe aunque aparezca la advertencia de certificado.
- 3 Inicie sesión con el nombre de usuario raíz y la contraseña que especificó al implementar el dispositivo de vRealize Automation.

4 Seleccione **Configuración de vRA > Configuración del host**.

Opción	Acción
Resolver automáticamente	Seleccione Resolver automáticamente para especificar el nombre del host actual para el dispositivo de vRealize Automation.
Actualizar host	<p>En los hosts nuevos, seleccione Actualizar host. Escriba el nombre de dominio completo del dispositivo de vRealize Automation, <i>vra-hostname.domain.name</i>, en el cuadro de texto Nombre del host.</p> <p>En implementaciones distribuidas que usan equilibradores de carga, seleccione Actualizar host. Escriba el nombre de dominio completo del servidor de equilibrador de carga, <i>vra-loadbalancername.domain.name</i>, en el cuadro de texto Nombre del host.</p>

NOTA: Establezca la configuración de SSO tal y como se describe más tarde en este procedimiento cuando utilice **Actualizar host** para cambiar un nombre de host.

5

- 6 Seleccione el tipo de certificado en el menú **Acción de certificado**.

Si usa un certificado con codificación PEM (para un entorno distribuido, por ejemplo), seleccione **Importar**.

Los certificados que importe deben ser de confianza y, asimismo, válidos para todas las instancias de el dispositivo de vRealize Automation y para cualquier equilibrador de carga mediante el uso de certificados de nombre alternativo del firmante (SAN).

NOTA: Si utiliza cadenas de certificados, especifique los certificados en el siguiente orden:

- a Certificado de cliente/servidor firmado por un certificado de CA intermedia
 - b Uno o más certificados intermedios
 - c Un certificado de CA raíz
-

Opción	Acción
Mantener existente	No modifique la configuración SSL actual. Seleccione esta opción para cancelar los cambios.
Generar certificado	<ol style="list-style-type: none"> a El valor mostrado en el cuadro de texto Nombre común es el nombre de host tal como aparece en la parte superior de la página. Si hay instancias adicionales disponibles del el dispositivo de vRealize Automation, sus nombres de dominio completos se incluirán en el atributo SAN del certificado. b Especifique el nombre de la organización (como el nombre de su compañía) en el cuadro de texto Organización. c Especifique la unidad organizativa (como la ubicación o el nombre del departamento) en el cuadro de texto Unidad organizativa. d Especifique un código de país ISO 3166 de dos letras, como ES, en el cuadro de texto País.
Importar	<ol style="list-style-type: none"> a Copie los valores de certificado desde BEGIN PRIVATE KEY a END PRIVATE KEY (encabezado y pie de página incluidos) y péguelos en el cuadro de texto Clave privada RSA. b Copie los valores de certificado desde BEGIN CERTIFICATE a END CERTIFICATE (encabezado y pie de página incluidos) y péguelos en el cuadro de texto Cadena de certificados. Si hay varios valores de certificado, incluya un encabezado BEGIN CERTIFICATE y un pie de página END CERTIFICATE por cada uno de ellos. NOTA: En el caso de certificados encadenados, puede haber atributos adicionales disponibles. c (Opcional) Si el certificado utiliza una frase de contraseña para cifrar la clave de certificado, cópiela y péguela en el cuadro de texto Frase de contraseña.

- 7 Haga clic en **Guardar configuración** para guardar la información de host y la configuración de SSL.
- 8 Defina la configuración de SSO.
- 9 Haga clic en **Mensajes**. Se muestran las opciones de configuración y el estado de los mensajes de su dispositivo. No cambie estas opciones de configuración.
- 10 Haga clic en la pestaña **Telemetría** para determinar si desea unirse al Programa de mejora de la experiencia del cliente de VMware (Customer Experience Improvement Program, CEIP).

Se brindan detalles sobre los datos recopilados a través del CEIP y los fines para los que VMware los usa en el Centro de Seguridad y Confianza en <http://www.vmware.com/trustvmware/ceip.html>.

- Seleccione **Unirse al programa de mejora de la experiencia del cliente de VMware** para participar en el programa.
- Anule la selección de **Unirse al programa de mejora de la experiencia del cliente de VMware** para no participar.

- 11 Haga clic en **Servicios** y compruebe que se han registrado los servicios.

En función de la configuración del sitio, esto puede tardar unos 10 minutos.

NOTA: Puede iniciar sesión en el dispositivo y ejecutar `tail -f /var/log/vcac/catalina.out` para supervisar el inicio de los servicios.

- 12 Introduzca la información de licencia.

- a Haga clic en **Configuración de vRA > Licencias**.
- b Haga clic en **Licencias**.
- c Introduzca la clave de licencia de vRealize Automation válida que obtuvo al descargar los archivos de instalación y haga clic en **Enviar clave**.

NOTA: Si se produce un error de conexión, podría tener problemas con el equilibrador de carga. Compruebe la conectividad de red con el equilibrador de carga.

- 13 Confirme que puede iniciar sesión en la consola de vRealize Automation.

- a Abra un navegador y vaya a `https://vcac-hostname.domain.name/vcac`.
- b Acepte el certificado de vRealize Automation.
- c Acepte el certificado de SSO.
- d Inicie sesión con `administrator@vsphere.local` y la contraseña que especificó durante la configuración de SSO.

Se abre la consola en la pestaña **Administración** de la página Tenants. La lista contiene un solo tenant denominado `vsphere.local`.

Ya ha terminado la implementación y configuración de su el dispositivo de vRealize Automation. Si el dispositivo no funciona correctamente tras la configuración, vuelva a implementar y configurar el dispositivo. No realice cambios en el dispositivo existente.

Qué hacer a continuación

[“Instalar los componentes de la infraestructura,”](#) página 56

Instalar componentes de IaaS

El administrador instala un conjunto completo de componentes de infraestructura (IaaS) en una máquina con Windows (física o virtual). Para realizar este tipo de tareas se necesitan derechos de administrador.

Con una instalación mínima se instalan todos los componentes en el mismo servidor de Windows, salvo la base de datos SQL, que se puede instalar en un servidor aparte.

Habilitar la sincronización de hora en el servidor de Windows

Los relojes en el servidor de vRealize Automation y en los servidores de Windows deben estar sincronizados para que la instalación se realice correctamente.

Los siguientes pasos describen cómo habilitar la sincronización de hora con el host ESX/ESXi usando VMware Tools. Si instala componentes de IaaS en un host físico o prefiere no usar VMware Tools para sincronizar la hora, utilice el método de su elección para asegurarse de que la hora del servidor es exacta.

Procedimiento

- 1 Abra un símbolo del sistema en la máquina de instalación de Windows.

- 2 Escriba el siguiente comando para ir al directorio de VMware Tools.

```
cd C:\Program Files\VMware\VMware Tools
```

- 3 Escriba el siguiente comando para ver el estado de la sincronización de hora.

```
VMwareToolboxCmd.exe timesync status
```

- 4 Si la sincronización de hora está deshabilitada, escriba el siguiente comando para habilitarla.

```
VMwareToolboxCmd.exe timesync enable
```

Certificados de IaaS

Los componentes de IaaS de vRealize Automation hacen uso de certificados y SSL para proteger las comunicaciones entre los componentes. En una instalación mínima con fines de prueba de concepto se pueden usar certificados autofirmados.

En un entorno distribuido, obtenga un certificado de dominio de una entidad de certificación de confianza. Para obtener información sobre cómo instalar certificados de dominio para los componentes de IaaS, consulte [“Instalar certificados de IaaS,”](#) página 75 en el capítulo sobre la implementación distribuida.

Instalar los componentes de la infraestructura

El administrador del sistema inicia sesión en la máquina de Windows y sigue el asistente de instalación para instalar los componentes de infraestructura (IaaS) en la máquina física o virtual de Windows.

Prerequisitos

- Compruebe que la máquina de instalación reúne los requisitos descritos en [“Requisitos del servidor de Model Management y el servicio web de IaaS,”](#) página 21.
- [“Habilitar la sincronización de hora en el servidor de Windows,”](#) página 55.
- Confirme que ha implementado y configurado completamente el dispositivo de vRealize Automation y, asimismo, que los servicios necesarios se están ejecutando (plugin-service, catalog-service, iaas-proxy-provider).

Procedimiento

- 1 [Descargar el instalador de IaaS](#) página 57
Un administrador del sistema descarga el instalador en una máquina física o virtual de Windows 2008 o Windows 2012.
- 2 [Seleccionar el tipo de instalación](#) página 57
El administrador del sistema ejecuta el asistente del programa de instalación desde máquina que tiene instalado Windows 2008 o 2012.
- 3 [Comprobar los requisitos previos](#) página 58
El Comprobador de requisitos previos confirma si la máquina reúne los requisitos de instalación de IaaS.
- 4 [Especificar la configuración de cuenta y servidor](#) página 58
El administrador del sistema de vRealize Automation especifica la configuración de servidor y cuenta del servidor de instalación de Windows y selecciona una instancia de servidor de base de datos de SQL y un método de autenticación.
- 5 [Especificar administradores y agentes](#) página 59
La instalación mínima instala los Distributed Execution Managers necesarios y el agente de proxy de vSphere predeterminado. El administrador del sistema puede instalar agentes de proxy adicionales (por ejemplo, XenServer o Hyper-V) después de la instalación, mediante el instalador personalizado.

- 6 [Registrar los componentes de IaaS](#) página 60
El administrador del sistema instala el certificado de IaaS y registra los componentes de IaaS con el SSO.
- 7 [Finalizar la instalación](#) página 60
El administrador del sistema finaliza la instalación de IaaS.

Descargar el instalador de IaaS

Un administrador del sistema descarga el instalador en una máquina física o virtual de Windows 2008 o Windows 2012.

Si aparecen advertencias de certificado durante este proceso, continúe sin problemas hasta finalizar la instalación.

Prerequisitos

- Microsoft .NET Framework 4.5.1 o posterior debe estar instalado en la máquina de instalación de IaaS. El instalador de .NET se puede descargar de la página web del instalador.
- Si usa Internet Explorer para la descarga, asegúrese de que la configuración de seguridad mejorada no está habilitada. Consulte `res://iesetup.dll/SoftAdmin.htm`.
- Inicie sesión en el servidor de Windows como administrador local.

Procedimiento

- 1 Inicie sesión en la máquina de Windows donde vaya a realizar la instalación.
- 2 Abra un navegador web.
- 3 Escriba la URL de la página de descarga del instalador de IaaS de VMware vRealize Automation.
Por ejemplo, `https://vra-va-hostname.domain.name:5480/installer`, donde `vra-va-hostname.domain.name` es el nombre del host de el dispositivo de vRealize Automation.
- 4 Descargue el instalador haciendo clic en el vínculo **Instalador de IaaS**.
- 5 Cuando se le pida, guarde el archivo del instalador (`setup__vra-va-hostname.domain.name@5480`) en el escritorio.

No modifique el nombre de archivo, ya que sirve para conectar la instalación a el dispositivo de vRealize Automation.

Seleccionar el tipo de instalación

El administrador del sistema ejecuta el asistente del programa de instalación desde máquina que tiene instalado Windows 2008 o 2012.

Prerequisitos

[“Descargar el instalador de IaaS,”](#) página 75.

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 2 Haga clic en **Siguiente**.
- 3 Acepte el acuerdo de licencia y haga clic en **Siguiente**.

- 4 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 5 Seleccione **Aceptar certificado**.
- 6 Haga clic en **Siguiente**.
- 7 Seleccione **Instalación completa** en la página Tipo de instalación si está creando una implementación mínima y haga clic en **Siguiente**.

Comprobar los requisitos previos

El Comprobador de requisitos previos confirma si la máquina reúne los requisitos de instalación de IaaS.

Prerequisitos

[“Seleccionar el tipo de instalación,”](#) página 57.

Procedimiento

- 1 Complete la comprobación de requisitos previos.

Opción	Descripción
Sin errores	Haga clic en Siguiente .
Sin errores críticos	Haga clic en Omitir .
Errores críticos	Si se omiten errores críticos, la instalación no se llevará a cabo. Si aparecen advertencias, seleccione la advertencia en el panel izquierdo y siga las instrucciones que se muestran a la derecha. Aborde todos los errores críticos y haga clic en Comprobar de nuevo para confirmar que se han solucionado.

- 2 Haga clic en **Siguiente**.

La máquina reúne los requisitos de instalación.

Especificar la configuración de cuenta y servidor

El administrador del sistema de vRealize Automation especifica la configuración de servidor y cuenta del servidor de instalación de Windows y selecciona una instancia de servidor de base de datos de SQL y un método de autenticación.

Prerequisitos

[“Comprobar los requisitos previos,”](#) página 58.

Procedimiento

- 1 En la página Configuración de servidor y cuenta o la página Configuración detectada, especifique el nombre de usuario y la contraseña de un usuario con privilegios de administrador de SQL o un administrador local.

- 2 Escriba una frase en el cuadro de texto **Frase de contraseña**.

La frase de contraseña es una serie de palabras que genera una clave de cifrado que se usa para proteger los datos de la base de datos.

NOTA: Guarde la frase de contraseña para poder usarla en instalaciones futuras o para recuperar el sistema en caso necesario.

- 3 En el cuadro de texto **Servidor** de la sección de instalación de base de datos de SQL Server, acepte el servidor predeterminado para instalar la instancia de base de datos en el mismo servidor con los componentes de IaaS, o escriba un nombre de servidor distinto si la base de datos está en otra máquina.

Si especifica otro servidor, debe suministrar el nombre de servidor y el número de puerto, con el formato *servername,portnumber*.

- 4 Acepte el valor predeterminado del cuadro de texto **Nombre de base de datos** o escriba un nombre adecuado si es necesario.

- 5 Seleccione el método de autenticación.

- ◆ Seleccione **Usar autenticación de Windows** si desea crear la base de datos utilizando las credenciales de Windows del usuario actual. El usuario debe tener privilegios sys_admin de SQL.
- ◆ Desactive la opción **Usar autenticación de Windows** si desea crear la base de datos utilizando la autenticación de SQL. Escriba el **Nombre de usuario** y la **Contraseña** de SQL Server con privilegios sys_admin de SQL en la instancia de SQL Server.

- 6 (Opcional) Active la casilla **Usar SSL para la conexión de base de datos**.

Esta casilla está activada de forma predeterminada. SSL ofrece una conexión mucho más segura entre el servidor de IaaS y la base de datos SQL. Sin embargo, para admitir esta opción primero debe configurar SSL en SQL Server. Para obtener información relacionada sobre cómo configurar SSL en el servidor SQL, consulte el artículo de la base de conocimientos 316898 sobre *cómo habilitar el cifrado SSL para una instancia de SQL Server mediante Microsoft Management Console* en el sitio de soporte de Microsoft.

- 7 Haga clic en **Siguiente**.

Especificar administradores y agentes

La instalación mínima instala los Distributed Execution Managers necesarios y el agente de proxy de vSphere predeterminado. El administrador del sistema puede instalar agentes de proxy adicionales (por ejemplo, XenServer o Hyper-V) después de la instalación, mediante el instalador personalizado.

Prerequisitos

[“Especificar la configuración de cuenta y servidor,”](#) página 58.

Procedimiento

- 1 En la página Distributed Execution Managers y agente de proxy de vSphere, acepte los valores predeterminados o cambie los nombres en caso necesario.

- 2 Acepte la opción predeterminada para instalar un agente de vSphere para permitir el aprovisionamiento con vSphere, o desactive la opción en caso necesario.

- a Seleccione **Instalar y configurar agente de vSphere**.
- b Acepte el agente y endpoint predeterminados, o escriba un nombre.

Tome nota del nombre de endpoint. Debe escribir esta información correctamente cuando configure el endpoint de vSphere en la consola de vRealize Automation para evitar que se produzca un error de configuración.

- 3 Haga clic en **Siguiente**.

Registrar los componentes de IaaS

El administrador del sistema instala el certificado de IaaS y registra los componentes de IaaS con el SSO.

Prerequisitos

[“Descargar el instalador de IaaS,”](#) página 57.

Procedimiento

- 1 Acepte el valor del **Servidor** predeterminado, que se rellena con el nombre de dominio completo del servidor de el dispositivo de vRealize Automation del que descargó el programa de instalación. Compruebe que se ha usado un nombre de dominio completo para identificar el servidor, no una dirección IP.

Si dispone de varios dispositivos virtuales que utilizan un equilibrador de carga, introduzca la ruta del dispositivo virtual de equilibrador de carga.
- 2 Haga clic en **Cargar** para rellenar el valor de **Tenant predeterminado de SSO** (vsphere.local).
- 3 Haga clic en **Descargar** para recuperar el certificado del el dispositivo de vRealize Automation. Puede hacer clic en **Ver certificado** para ver la información del certificado.
- 4 Seleccione **Aceptar certificado** para instalar el certificado SSO.
- 5 En el panel del administrador de SSO, escriba **administrador** en el cuadro de texto **Nombre de usuario** y la contraseña que definió para este usuario cuando configuró SSO en **Contraseña** y **Confirmar contraseña**.
- 6 Haga clic en el vínculo de prueba a la derecha del campo **Nombre de usuario** para validar la contraseña introducida.
- 7 Acepte el valor predeterminado en **Servidor de IaaS**, que contiene el nombre de host de la máquina Windows donde se realiza la instalación.
- 8 Haga clic en el vínculo de prueba a la derecha del campo **Servidor de IaaS** para validar la conectividad.
- 9 Haga clic en **Siguiente**.

Si se produce algún error tras hacer clic en **Siguiente**, resuélvalo antes de continuar.

Finalizar la instalación

El administrador del sistema finaliza la instalación de IaaS.

Prerequisitos

- [“Registrar los componentes de IaaS,”](#) página 60.
- Compruebe que la máquina en la que está realizando la instalación está conectada a la red y se puede conectar al el dispositivo de vRealize Automation del que se descarga el instalador de IaaS.

Procedimiento

- 1 Repase la información en la página Listo para instalar y haga clic en **Instalar**.

De este modo, se inicia la instalación. Según cuál sea la configuración de red, la instalación puede tardar entre cinco minutos y una hora.
- 2 Cuando aparezca el mensaje que indica que todo está correcto, deje activada la casilla **Guiarme por la configuración inicial** y haga clic en **Siguiente** y en **Finalizar**.
- 3 Cierre el cuadro del mensaje **Configurar el sistema**.

La instalación se ha completado.

Qué hacer a continuación

[“Comprobar los servicios de IaaS,”](#) página 96.

Implementación distribuida

En una implementación distribuida, el administrador del sistema instala los componentes en varias máquinas del entorno de implementación.

Lista de comprobación de implementación distribuida

Un administrador del sistema puede implementar vRealize Automation en una configuración distribuida, lo que ofrece protección de conmutación por error y una alta disponibilidad por medio de la redundancia.

La lista de comprobación de implementación distribuida ofrece una descripción de alto nivel de los pasos necesarios para realizar una instalación distribuida.

Tabla 4-2. Lista de comprobación de implementación distribuida

Tarea	Detalles
<input type="checkbox"/> Planear y preparar el entorno de instalación, y comprobar que se cumplen todos los requisitos previos de instalación.	Capítulo 2, “Preparar la instalación,” página 19
<input type="checkbox"/> Prever y obtener los certificados SSL.	“Requisitos de confianza de certificados en una implementación distribuida,” página 63
<input type="checkbox"/> Implementar el servidor principal de el dispositivo de vRealize Automation, así como cualquier otro dispositivo adicional que necesite para disponer de redundancia y alta disponibilidad.	“Implementar el dispositivo de vRealize Automation,” página 65
<input type="checkbox"/> Configurar el equilibrador de carga para controlar el tráfico de dispositivos de vRealize Automation.	
<input type="checkbox"/> Configurar el servidor principal de el dispositivo de vRealize Automation, así como cualquier otro dispositivo adicional que haya implementado para disponer de redundancia y alta disponibilidad.	“Configurar dispositivos para vRealize Automation,” página 67
<input type="checkbox"/> Configurar el equilibrador de carga para controlar el tráfico de componentes de IaaS de vRealize Automation e instalar los componentes de IaaS de vRealize Automation.	“Instalar los componentes de IaaS en una configuración distribuida,” página 73
<input type="checkbox"/> Si lo precisa, instalar los agentes que se van a integrar con sistemas externos.	“Instalación de agentes,” página 97
<input type="checkbox"/> Configurar el tenant predeterminado y proporcionar la licencia de IaaS.	

vRealize Orchestrator

Utilice implementaciones externas de vRealize Orchestrator con implementaciones de alta disponibilidad. Si usa un servidor de vRealize Orchestrator en el dispositivo de vRealize Automation, configúrelo de forma que sea externo. No utilice nunca versiones integradas.

Administración de directorios

Si realiza una instalación distribuida con equilibradores de carga para alta disponibilidad y conmutación por error, notifique al equipo responsable de configurar su entorno de vRealize Automation. Sus administradores de tenants deben configurar la administración de directorios para alta disponibilidad cuando configuren el vínculo a Active Directory.

Para obtener más información acerca de cómo configurar la administración de directorios para alta disponibilidad, consulte *Configuración de vRealize Automation*.

Componentes de la instalación distribuida

En una instalación distribuida, el administrador del sistema implementa dispositivos virtuales y sus componentes relacionados que complementen el entorno de implementación.

Tabla 4-3. Dispositivos virtuales y base de datos de dispositivo

Componente	Descripción
el dispositivo de vRealize Automation	Dispositivo virtual preconfigurado que implementa el servidor de vRealize Automation. El servidor incluye la consola de vRealize Automation, que es un portal único para realizar tareas de aprovisionamiento de autoservicio y administración de servicios en la nube, así como de autoría y administración.
Base de datos de dispositivo	Almacena la información que necesitan los dispositivos virtuales. La base de datos se integra en una o dos instancia de el dispositivo de vRealize Automation.

Puede seleccionar los componentes de IaaS individuales que quiera instalar, así como especificar la ubicación de instalación.

Tabla 4-4. Componentes de IaaS

Componente	Descripción
Sitio web	Provee a la consola de vRealize Automation de capacidades de autoría de servicio y administración de infraestructura. El componente de sitio web se comunica con Model Manager, que le proporciona actualizaciones de Distributed Execution Manager (DEM), con los agentes de proxy y con la base de datos.
Manager Service	Manager Service coordina la comunicación entre los agentes, la base de datos, Active Directory y SMTP. Manager Service se comunica con el sitio web de la consola a través de Model Manager. Este servicio requiere privilegios administrativos para poder ejecutarse.
Model Manager	Model Manager se comunica con la base de datos, los DEM y el sitio web del portal. Model Manager se divide en dos componentes instalables por separado: el servicio web de Model Manager y el componente de datos de Model Manager.
Distributed Execution Managers (orquestador y trabajo)	Un Distributed Execution Manager (DEM) ejecuta la lógica empresarial de los modelos personalizados, para lo cual interactúa con la base de datos de IaaS y con las bases de datos externas. Los DEM también administran las máquinas físicas y en la nube.
Agentes	Agentes de virtualización, integración y WMI que se comunican con los recursos de la infraestructura.

Requisitos de confianza de certificados en una implementación distribuida

Para garantizar una comunicación segura, vRealize Automation utiliza certificados para crear relaciones de confianza entre los componentes.

La implementación específica de los certificados necesarios para lograr esta confianza depende del entorno.

Para proporcionar alta disponibilidad y admitir la conmutación por error, se pueden implementar clústeres de componentes con equilibrio de carga. En tal caso, se obtiene un certificado multiusuario que incluye el componente web de IaaS del clúster y, a continuación, se copia dicho certificado multiusuario en cada uno de los componentes del clúster. Puede usar certificados de nombre alternativo del firmante (SAN), certificados comodín o cualquier otro método de certificación multiusuario apropiado para su entorno, siempre y cuando se cumplan los requisitos de confianza. En función de la configuración del equilibrador de carga, quizás sea necesario certificar el equilibrador de carga como parte del certificado multiusuario del clúster.

Por ejemplo, si la configuración del equilibrador de carga requiere un certificado en el equilibrador de carga y en sus componentes, podría obtener un certificado SAN que sirva para certificar `web-load-balancer.eng.mycompany.com`, `web-component-1.eng.mycompany.com` y `web-component-2.eng.mycompany.com`. Copiaría ese único certificado multiusuario en el equilibrador de carga y en cada uno de los dispositivos y, a continuación, registraría el certificado en las máquinas de componentes web.

En la tabla Importación y registro de certificados se resumen los requisitos de registro de diversos certificados importados.

Tabla 4-5. Importación y registro de certificados

Importar	Registrar
Clúster de el dispositivo de vRealize Automation	Clúster de componentes web
Clúster de componentes web	<ul style="list-style-type: none"> ■ Clúster de el dispositivo de vRealize Automation ■ Clúster de componentes de Manager Service ■ Componentes de orquestador de DEM y trabajo de DEM
Clúster de componentes de Manager Service	<ul style="list-style-type: none"> ■ Componentes de orquestador de DEM y trabajo de DEM ■ Agentes y agentes de proxy

Hojas de trabajo de instalación

Puede usar estas hojas de trabajo para registrar la información importante y, de este modo, poder tenerla como referencia durante el proceso de instalación.

Aquí se proporciona una copia de cada hoja de trabajo. Puede ir creando más a medida que las vaya necesitando. En los valores de configuración se distinguen mayúsculas de minúsculas.

Tabla 4-6. Información de el dispositivo de vRealize Automation de clúster de encabezado

Variable	Valor	Ejemplo
Nombre de host (FQDN)		<code>vcac-va.mycompany.com</code>
Puerto de salida del servicio de SSO sobre HTTPS (predeterminado)	7444 (no cambiar)	7444
IP		192.168.1.105
Nombre de usuario	administrador@vsphere.local (predeterminado)	administrador@vsphere.local
Contraseña		vmware

Tabla 4-7. Información de el dispositivo de vRealize Automation adicional

Variable	Valor	Ejemplo
Nombre de host (FQDN)		vcac-va2.mycompany.com
Puerto de salida del servicio de SSO sobre HTTPS (predeterminado)	7444 (no cambiar)	7444
IP		192.168.1.110
Nombre de usuario	administrador@vsphere.local (predeterminado)	administrador@vsphere.local
Contraseña		vmware

Tabla 4-8. Frase de contraseña de base de datos de IaaS

Variable	Valor	Ejemplo
Frase de contraseña (reutilizada en el instalador, actualización y migración de IaaS)		MiFraseDeContraseña

Tabla 4-9. Sitio web de IaaS

Variable	Valor	Ejemplo
Nombre de host (FQDN)		iaas-web.mycompany.com
Puerto de salida del servicio de SSO sobre HTTPS (predeterminado)		
IP		192.168.1.106
Nombre de usuario		
Contraseña		

Tabla 4-10. Model Manager Data de IaaS

Variable	Valor	Ejemplo
Nombre de host (FQDN)		iaas-model-man.mycompany.com
Puerto de salida del servicio de SSO sobre HTTPS (predeterminado)		
IP		192.168.1.107
Nombre de usuario		
Contraseña		

Tabla 4-11. Manager Service de IaaS

Variable	Valor	Ejemplo
Nombre de host (FQDN)		iaas-model-service.mycompany.com
Puerto de salida del servicio de SSO sobre HTTPS (predeterminado)		
IP		192.168.1.108
Nombre de usuario		
Contraseña		

Tabla 4-12. Distributed Execution Managers

Nombre único	Orquestador/Trabajo
ex.myuniqueorchestratorname	Orquestador: Trabajo:
	Orquestador: Trabajo:
	Orquestador: Trabajo:
	Orquestador: Trabajo:

Implementar el dispositivo de vRealize Automation

Para implementar el dispositivo de vRealize Automation, un administrador del sistema debe iniciar sesión en el cliente de vSphere y seleccionar una configuración de implementación.

Existen algunas restricciones para la contraseña raíz que se crea para el administrador de vRealize Automation. Consulte [“Consideraciones sobre las contraseñas,”](#) página 20.

Prerequisitos

- Descargue el dispositivo de vRealize Automation del sitio web de VMware.
- Inicie sesión en el cliente de vSphere como usuario con privilegios de administrador del sistema.

Procedimiento

- 1 Seleccione **Archivo > Implementar plantilla de OVF** en el cliente de vSphere.
- 2 Vaya al archivo de el dispositivo de vRealize Automation que descargó y haga clic en **Abrir**.
- 3 Haga clic en **Siguiente**.
- 4 Haga clic en **Siguiente** en la página de detalles de plantilla de OVF.
- 5 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 6 En el cuadro de texto **Nombre**, especifique un nombre único de dispositivo virtual respetando la convención de nomenclatura de TI de su organización, seleccione el centro de datos y la ubicación donde quiera implementar el dispositivo y haga clic en **Siguiente**.
- 7 Siga las indicaciones hasta que se abra la página Formato de disco.
- 8 Compruebe en esta página que hay espacio en disco suficiente para implementar el dispositivo virtual y haga clic en **Siguiente**.
- 9 Siga las indicaciones hasta llegar a la página Propiedades.

Las opciones que aparecen dependen de la configuración de vSphere.

- 10 Configure los valores en la página Propiedades.
 - a Especifique la contraseña raíz que va a usar para iniciar sesión en la consola de dispositivo virtual en los cuadros de texto **Escribir contraseña** y **Confirmar contraseña**.
 - b Active o desactive la casilla **Servicio de SSH** para determinar si el servicio de SSH va a estar habilitado en el dispositivo.

Este valor se usa para establecer el estado inicial del servicio de SSH en el dispositivo. Si va a realizar la instalación con el asistente de instalación, habilítelo antes de iniciar el asistente. Puede cambiar este valor desde la consola de administración del dispositivo después de la instalación.

- c Especifique el nombre de dominio completo de la máquina virtual en el cuadro de texto **Nombre de host**, aun cuando esté usando DHCP.
 - d Configure las propiedades de la red.
- 11 Haga clic en **Siguiente**.
 - 12 Según la configuración de vCenter y DNS, la resolución de DNS podría tardar bastante tiempo. Para acelerar este proceso, lleve a cabo los siguientes pasos.
 - Si **Encender tras implementación** está disponible en la página Listo para completar:
 - a Seleccione **Encender tras implementación** y haga clic en **Finalizar**.
 - b Haga clic en **Cerrar** cuando el archivo termine de implementarse en vCenter.
 - c Espere a que la máquina se inicie.
Esto puede tardar hasta cinco minutos.
 - Si **Encender tras implementación** no está disponible en la página Listo para completar:
 - a Haga clic en **Cerrar** cuando el archivo termine de implementarse en vCenter.
 - b Encienda la máquina virtual y espere un rato hasta que esta se inicie.
 - c Compruebe que puede hacer ping al DNS de la máquina virtual. Si no puede hacer ping al DNS, reinicie la máquina virtual.
 - d Espere a que la máquina se inicie. Esto puede tardar hasta cinco minutos.

Para confirmar que el dispositivo se ha implementado correctamente, abra un símbolo del sistema y haga ping en el FQDN de el dispositivo de vRealize Automation.

Qué hacer a continuación

Repita este procedimiento para implementar más instancias de el dispositivo de vRealize Automation para disponer de redundancia en un entorno de alta disponibilidad.

Configurar el equilibrador de carga

Tras implementar los dispositivos para vRealize Automation, se puede definir un equilibrador de carga que distribuya el tráfico entre diversas instancias del el dispositivo de vRealize Automation.

En la siguiente lista se describen los pasos generales necesarios para configurar un equilibrador de carga para el tráfico de vRealize Automation:

- 1 Instale el equilibrador de carga.
- 2 Permita la afinidad de sesiones, también conocida sesiones temporales.
- 3 Procure que el tiempo de espera del equilibrador de carga sea de 100 segundos como mínimo.
- 4 Si la red o el equilibrador de carga lo precisan, importe un certificado al equilibrador de carga. Para obtener información sobre las relaciones de confianza y los certificados, consulte [“Requisitos de confianza de certificados en una implementación distribuida,”](#) página 63. Para obtener información sobre cómo extraer certificados, consulte [“Extraer certificados y claves privadas,”](#) página 29.
- 5 Configure el equilibrador de carga para el tráfico de el dispositivo de vRealize Automation.
- 6 Configure los dispositivos para vRealize Automation. Consulte [“Configurar dispositivos para vRealize Automation,”](#) página 67.

NOTA: Cuando defina dispositivos virtuales en el equilibrador de carga, hágalo exclusivamente en el caso de los dispositivos virtuales que se hayan configurado para su uso con vRealize Automation. Si se definen dispositivos sin configurar, se producirán respuestas fallidas.

Para obtener información sobre la escalabilidad y la alta disponibilidad, consulte la *arquitectura de referencia de VMware vRealize Automation*, disponible como documento técnico en <https://www.vmware.com/support/pubs/vcac-pubs.html>.

Configurar dispositivos para vRealize Automation

Tras implementar los dispositivos y configurar el equilibrio de carga, hay que configurar los dispositivos para vRealize Automation.

Configurar el dispositivo de vRealize Automation principal

el dispositivo de vRealize Automation es un dispositivo virtual preconfigurado que implementa la consola web (el portal de usuario) y el servidor de vRealize Automation. Se proporciona como una plantilla de formato de virtualización abierta (OVF). El administrador del sistema descarga el dispositivo y lo implementa en vCenter Server o en el inventario de ESX/ESXi.

Si la red o el equilibrador de carga lo precisan, el certificado que configure para la instancia principal del dispositivo se copiará en el equilibrador de carga y en otras instancias de dispositivo adicionales en procedimientos posteriores.

Prerequisitos

- [“Implementar el dispositivo de vRealize Automation,”](#) página 65.
- Obtenga un certificado de dominio para el dispositivo de vRealize Automation.

Procedimiento

- 1 [Habilitar la sincronización de hora en el dispositivo de el dispositivo de vRealize Automation](#) página 67

Los relojes en el servidor de el dispositivo de vRealize Automation y en los servidores de Windows deben estar sincronizados para que la instalación se realice correctamente.

- 2 [Configurar el dispositivo de vRealize Automation](#) página 68

Para preparar el el dispositivo de vRealize Automation para utilizarlo, un administrador del sistema tiene que definir la configuración del host, generar un certificado SSL y suministrar la información de conexión de SSO.

Habilitar la sincronización de hora en el dispositivo de el dispositivo de vRealize Automation

Los relojes en el servidor de el dispositivo de vRealize Automation y en los servidores de Windows deben estar sincronizados para que la instalación se realice correctamente.

Si aparecen advertencias de certificado durante este proceso, continúe sin problemas hasta finalizar la instalación.

Procedimiento

- 1 Vaya a la consola de administración de el dispositivo de vRealize Automation utilizando su nombre de dominio completo, <https://vra-va-hostname.domain.name:5480/>.
- 2 Inicie sesión con el nombre de usuario **root** y la contraseña que especificó cuando se implementó el dispositivo.
- 3 Seleccione **Administración > Configuración de hora**.

- 4 Seleccione una opción del menú **Modo de sincronización de hora**.

Opción	Acción
Usar servidor horario	Seleccione Usar servidor horario del menú Modo de sincronización de hora para usar el protocolo de tiempo de redes. Por cada servidor horario que utilice, especifique la dirección IP o el nombre de host correspondiente en el cuadro de texto Servidor horario .
Usar hora de host	Seleccione Usar hora de host del menú Modo de sincronización de hora para usar la sincronización de hora de VMware Tools. Para poder usar la sincronización de hora de VMware Tools, deberá configurar las conexiones con los servidores del protocolo de tiempo de redes.

- 5 Haga clic en **Guardar configuración**.
- 6 Compruebe que el valor reflejado en **Hora actual** es correcto.
Puede cambiar la zona horaria cuando lo desee en la página Configuración de zona horaria de la pestaña **Sistema**.

Configurar el dispositivo de vRealize Automation

Para preparar el el dispositivo de vRealize Automation para utilizarlo, un administrador del sistema tiene que definir la configuración del host, generar un certificado SSL y suministrar la información de conexión de SSO.

Procedimiento

- 1 Vaya a la consola de administración de el dispositivo de vRealize Automation utilizando su nombre de dominio completo, <https://vra-va-hostname.domain.name:5480/>.
- 2 Continúe aunque aparezca la advertencia de certificado.
- 3 Inicie sesión con el nombre de usuario raíz y la contraseña que especificó al implementar el dispositivo de vRealize Automation.
- 4 Seleccione **Configuración de vRA > Configuración del host**.

Opción	Acción
Resolver automáticamente	Seleccione Resolver automáticamente para especificar el nombre del host actual para el el dispositivo de vRealize Automation.
Actualizar host	En los hosts nuevos, seleccione Actualizar host . Escriba el nombre de dominio completo del el dispositivo de vRealize Automation, <i>vra-hostname.domain.name</i> , en el cuadro de texto Nombre del host . En implementaciones distribuidas que usan equilibradores de carga, seleccione Actualizar host . Escriba el nombre de dominio completo del servidor de equilibrador de carga, <i>vra-loadbalancername.domain.name</i> , en el cuadro de texto Nombre del host .

NOTA: Establezca la configuración de SSO tal y como se describe más tarde en este procedimiento cuando utilice **Actualizar host** para cambiar un nombre de host.

5 Seleccione el tipo de certificado en el menú **Acción de certificado**.

Si usa un certificado con codificación PEM (para un entorno distribuido, por ejemplo), seleccione **Importar**.

Los certificados que importe deben ser de confianza y, asimismo, válidos para todas las instancias de el dispositivo de vRealize Automation y para cualquier equilibrador de carga mediante el uso de certificados de nombre alternativo del firmante (SAN).

NOTA: Si utiliza cadenas de certificados, especifique los certificados en el siguiente orden:

- a Certificado de cliente/servidor firmado por un certificado de CA intermedia
- b Uno o más certificados intermedios
- c Un certificado de CA raíz

Opción	Acción
Mantener existente	No modifique la configuración SSL actual. Seleccione esta opción para cancelar los cambios.
Generar certificado	<ul style="list-style-type: none"> a El valor mostrado en el cuadro de texto Nombre común es el nombre de host tal como aparece en la parte superior de la página. Si hay instancias adicionales disponibles del el dispositivo de vRealize Automation, sus nombres de dominio completos se incluirán en el atributo SAN del certificado. b Especifique el nombre de la organización (como el nombre de su compañía) en el cuadro de texto Organización. c Especifique la unidad organizativa (como la ubicación o el nombre del departamento) en el cuadro de texto Unidad organizativa. d Especifique un código de país ISO 3166 de dos letras, como ES, en el cuadro de texto País.
Importar	<ul style="list-style-type: none"> a Copie los valores de certificado desde BEGIN PRIVATE KEY a END PRIVATE KEY (encabezado y pie de página incluidos) y péguelos en el cuadro de texto Clave privada RSA. b Copie los valores de certificado desde BEGIN CERTIFICATE a END CERTIFICATE (encabezado y pie de página incluidos) y péguelos en el cuadro de texto Cadena de certificados. Si hay varios valores de certificado, incluya un encabezado BEGIN CERTIFICATE y un pie de página END CERTIFICATE por cada uno de ellos. NOTA: En el caso de certificados encadenados, puede haber atributos adicionales disponibles. c (Opcional) Si el certificado utiliza una frase de contraseña para cifrar la clave de certificado, cópiela y péguela en el cuadro de texto Frase de contraseña.

6 Haga clic en **Guardar configuración** para guardar la información de host y la configuración de SSL.

7 Si la red o el equilibrador de carga lo requieren, copie el certificado importado o recién creado en el equilibrador de carga del dispositivo virtual.

Puede que sea necesario habilitar el acceso SSH raíz para exportar el certificado.

- a Si aún no ha iniciado sesión, iníciela en la consola de administración del dispositivo vRealize Automation como usuario raíz.
- b Haga clic en la pestaña **Administración**.
- c Haga clic en el submenú **Administración**.
- d Seleccione la casilla de verificación **Servicio SSH habilitado**.

Anule la selección de la casilla de verificación para deshabilitar SSH cuando haya terminado.

- e Seleccione la casilla de verificación **Inicio de sesión SSH de administrador habilitado**.
Anule la selección de la casilla de verificación para deshabilitar SSH cuando haya terminado.
 - f Haga clic en **Guardar configuración**.
- 8 Defina la configuración de SSO.
- 9 Haga clic en **Servicios**.

Para instalar una licencia o un log en la consola, todos los servicios deben estar en ejecución. Normalmente, tardan unos 10 minutos en iniciarse.

NOTA: También puede iniciar sesión en el dispositivo y ejecutar `tail -f /var/log/vcac/catalina.out` para supervisar el inicio de los servicios.

- 10 Introduzca la información de licencia.
- a Haga clic en **Configuración de vRA > Licencias**.
 - b Haga clic en **Licencias**.
 - c Introduzca la clave de licencia de vRealize Automation válida que obtuvo al descargar los archivos de instalación y haga clic en **Enviar clave**.

NOTA: Si se produce un error de conexión, podría tener problemas con el equilibrador de carga. Compruebe la conectividad de red con el equilibrador de carga.

- 11 Haga clic en **Mensajes**. Se muestran las opciones de configuración y el estado de los mensajes de su dispositivo. No cambie estas opciones de configuración.
- 12 Haga clic en la pestaña **Telemetría** para determinar si desea unirse al Programa de mejora de la experiencia del cliente de VMware (Customer Experience Improvement Program, CEIP).
- Se brindan detalles sobre los datos recopilados a través del CEIP y los fines para los que VMware los usa en el Centro de Seguridad y Confianza en <http://www.vmware.com/trustvmware/ceip.html>.
- Seleccione **Unirse al programa de mejora de la experiencia del cliente de VMware** para participar en el programa.
 - Anule la selección de **Unirse al programa de mejora de la experiencia del cliente de VMware** para no participar.

- 13 Haga clic en **Guardar configuración**.

- 14 Confirme que puede iniciar sesión en la consola de vRealize Automation.

- a Abra un explorador y vaya a `https://vcac-hostname.domain.name/vcac/`.

Si usa un equilibrador de carga, el nombre de host debe ser el nombre del dominio completo del equilibrador de carga.

- b Si recibe una solicitud, continúe aunque aparezcan advertencias de certificado.

- c Inicie sesión con **administrator@vsphere.local** y la contraseña que especificó durante la configuración de SSO.

Se abre la consola en la pestaña **Administración** de la página Tenants. La lista contiene un solo tenant denominado `vsphere.local`.

- 15 Si usa un equilibrador de carga y se han configurado todos los nodos de dicho equilibrador, configure y habilite todas las comprobaciones de estado aplicables.

Configurar más instancias del dispositivo vRealize Automation

El administrador del sistema puede implementar varias instancias del dispositivo de vRealize Automation para garantizar la redundancia en un entorno de alta disponibilidad.

Por cada el dispositivo de vRealize Automation hay que habilitar una sincronización de tiempo y añadir el dispositivo a un clúster. La información de configuración basada en los valores del dispositivo de vRealize Automation inicial (principal) se incorpora automáticamente cuando el dispositivo se añade al clúster.

Si realiza una instalación distribuida con equilibradores de carga para alta disponibilidad y conmutación por error, notifique al equipo responsable de configurar su entorno de vRealize Automation. Sus administradores de tenants deben configurar la administración de directorios para alta disponibilidad cuando configuren el vínculo a Active Directory.

Habilitar la sincronización de hora en el dispositivo de vRealize Automation

Los relojes en el servidor de el dispositivo de vRealize Automation y en los servidores de Windows deben estar sincronizados para que la instalación se realice correctamente.

Si aparecen advertencias de certificado durante este proceso, continúe sin problemas hasta finalizar la instalación.

Prerequisitos

“Configurar el dispositivo de vRealize Automation principal,” página 67.

Procedimiento

- 1 Vaya a la consola de administración de el dispositivo de vRealize Automation utilizando su nombre de dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 2 Inicie sesión con el nombre de usuario **root** y la contraseña que especificó cuando se implementó el dispositivo.
- 3 Seleccione **Administración > Configuración de hora**.
- 4 Seleccione una opción del menú **Modo de sincronización de hora**.

Opción	Acción
Usar servidor horario	Seleccione Usar servidor horario del menú Modo de sincronización de hora para usar el protocolo de tiempo de redes. Por cada servidor horario que utilice, especifique la dirección IP o el nombre de host correspondiente en el cuadro de texto Servidor horario .
Usar hora de host	Seleccione Usar hora de host del menú Modo de sincronización de hora para usar la sincronización de hora de VMware Tools. Para poder usar la sincronización de hora de VMware Tools, deberá configurar las conexiones con los servidores del protocolo de tiempo de redes.

- 5 Haga clic en **Guardar configuración**.
- 6 Compruebe que el valor reflejado en **Hora actual** es correcto.
Puede cambiar la zona horaria cuando lo desee en la página Configuración de zona horaria de la pestaña **Sistema**.

Unir un el dispositivo de vRealize Automation a un clúster

Las instalaciones distribuidas en las que se usan equilibradores de carga permiten usar más de un el dispositivo de vRealize Automation en una implementación. Cada dispositivo en la implementación debe pertenecer a un clúster.

Un el dispositivo de vRealize Automation se une a un clúster en la consola de administración. La operación de unión copia la información de configuración de dispositivo del clúster (como el certificado, SSO, licencia, base de datos y mensajes) en el dispositivo que se va a añadir al clúster.

Realice esta tarea en la consola de administración de cada servidor que quiera unir al clúster, salvo el nodo de clúster de encabezado.

La operación de unión no es necesaria en el caso del nodo de clúster de encabezado porque dicha operación vincula el nodo de clúster de encabezado con el nodo de la consola de administración con la que esté trabajando, lo que hace que ambos nodos formen parte del mismo clúster. Una vez que un dispositivo forma parte de un clúster, se puede especificar su FQDN como el nodo de clúster de encabezado.

NOTA: Cuando se añade el primer nodo a un clúster, es posible que sea necesario volver a importar o crear el certificado. De igual forma, los nodos deben añadirse a un clúster de uno en uno, no en paralelo.

Prerequisitos

- [“Configurar el dispositivo de vRealize Automation principal,”](#) página 67.
- Si su sitio usa un equilibrador de carga, compruebe que está configurado para usarse con su el dispositivo de vRealize Automation.
- [“Habilitar la sincronización de hora en el dispositivo de vRealize Automation,”](#) página 71. La sincronización de hora debe estar habilitada en cada dispositivo.
- Compruebe que el tráfico puede atravesar el equilibrador de carga hacia los nodos instalados y el nodo que se está configurando. El nodo principal también debe estar disponible.

Procedimiento

- 1 Vaya a la consola de administración de el dispositivo de vRealize Automation utilizando su nombre de dominio completo, <https://vra-va-hostname.domain.name:5480/>.
- 2 Continúe aunque aparezcan advertencias de certificado.
- 3 Inicie sesión con el nombre de usuario raíz y la contraseña que especificó al implementar el dispositivo de vRealize Automation.
- 4 Seleccione **Configuración de vRA > Clúster**.
- 5 En el cuadro de texto **Nodo de clúster de encabezado**, escriba el FQDN de un el dispositivo de vRealize Automation que se haya configurado anteriormente.
Puede usar el FQDN del el dispositivo de vRealize Automation principal o de cualquier el dispositivo de vRealize Automation que ya se haya unido al clúster.
- 6 Escriba la contraseña raíz en el cuadro de texto **Contraseña**.
- 7 Haga clic en **Unirse a clúster**.
- 8 Continúe aunque aparezcan advertencias de certificado.
Los servicios del clúster se reinician.
- 9 Confirme que los servicios se estén ejecutando.
 - a Haga clic en la pestaña **Servicios**.
 - b Haga clic en la pestaña **Actualizar** para ver el progreso del inicio de los servicios.

Deshabilitar los servicios sin usar

Un administrador del sistema puede deshabilitar los servicios de vRealize Orchestrator integrados. Estos servicios no se utilizan en una implementación distribuida, de modo que deben deshabilitarse para no consumir recursos innecesariamente.

Prerequisitos

[“Unir un el dispositivo de vRealize Automation a un clúster,”](#) página 72

Procedimiento

- 1 Inicie sesión en el dispositivo de vRealize Automation mediante SSH.
- 2 Detenga el servicio de vRealize Orchestrator integrado.


```
service vco-server stop
chkconfig vco-server off
```
- 3 Cierre sesión en el dispositivo de vRealize Automation.

Validar la implementación distribuida

Después de implementar instancias adicionales de el dispositivo de vRealize Automation, debería validar el acceso a los dispositivos agrupados en clúster.

Procedimiento

- 1 En la interfaz de administración del equilibrador de carga o en el archivo de configuración, deshabilite temporalmente todos los nodos excepto el que esté probando.
- 2 Para confirmar que puede iniciar sesión en la consola de vRealize Automation, vaya a `https://vcac-hostname.domain.name/vcac`, donde `vcac-hostname.domain.name` es la dirección del equilibrador de carga.
- 3 Después de utilizar el equilibrador de carga para comprobar que el nuevo el dispositivo de vRealize Automation es accesible, vuelva a habilitar los demás nodos.

Instalar los componentes de IaaS en una configuración distribuida

El administrador del sistema instala los componentes de IaaS después de que los dispositivos se hayan implementado y configurado por completo. Los componentes de IaaS proporcionan acceso a las características de infraestructura de vRealize Automation.

Todos los componentes se deben ejecutar en la misma cuenta de servicio.

Prerequisitos

- [“Configurar el dispositivo de vRealize Automation principal,”](#) página 67.
- Si el sitio contiene varias instancias de el dispositivo de vRealize Automation, [“Unir un el dispositivo de vRealize Automation a un clúster,”](#) página 72.
- Compruebe que los servidores de instalación cumplen los requisitos descritos en [“Requisitos del servidor de Model Management y el servicio web de IaaS,”](#) página 21.
- Obtenga un certificado de una entidad de certificación de confianza para importarlo en el almacén de certificados raíz de confianza de las máquinas en las que pretende instalar los datos del sitio web de componentes y de Model Manager.
- Si usa equilibradores de carga en su entorno, asegúrese de que reúnen los requisitos de configuración.

Procedimiento

- 1 [Instalar certificados de IaaS](#) página 75
 En los entornos de producción, obtenga un certificado de dominio de una entidad de certificación de confianza. Importe el certificado al almacén de certificados raíz de confianza de todas las máquinas en las que tenga intención de instalar el componente de sitio web y Manager Service (máquinas de IIS) durante la instalación de IaaS.
- 2 [Descargar el instalador de IaaS](#) página 75
 Un administrador del sistema descarga el instalador de IaaS de el dispositivo de vRealize Automation en una máquina física o virtual con Windows 2008 o Windows 2012.
- 3 [Elegir un escenario de base de datos de IaaS](#) página 76
 IaaS de vRealize Automation utiliza una base de datos de Microsoft SQL Server para conservar la información sobre las máquinas que administra, así como sobre sus propios elementos y políticas.
- 4 [Instalar un componente de sitio web de IaaS con Model Manager Data](#) página 81
 El administrador del sistema instala el componente de sitio web para dar acceso a las funciones de infraestructura en la consola web de vRealize Automation. Se pueden instalar una o varias instancias del componente de sitio web, pero Model Manager Data se debe configurar en la máquina donde se aloje el primer componente de sitio web. Model Manager Data solamente se instala una vez.
- 5 [Instalar más componentes de sitio web de IaaS](#) página 85
 El componente de sitio web ofrece acceso a las funciones de infraestructura en la consola web de vRealize Automation. El administrador del sistema puede instalar una o varias instancias del componente de sitio web.
- 6 [Instalar el Manager Service activo](#) página 87
 El componente Manager Service coordina la comunicación entre los agentes y los agentes de proxy, la base de datos y SMTP. Debe haber instalada una instancia del componente Manager Service como mínimo. Se puede instalar una instancia activa y otra de copia de seguridad del componente Manager Service para proporcionar redundancia en una implementación de alta disponibilidad.
- 7 [Instalar un componente de copia de seguridad de Manager Service](#) página 89
 Se puede instalar una instancia de copia de seguridad pasiva del componente Manager Service que se puede iniciar manualmente con el fin de proporcionar redundancia en una implementación de alta disponibilidad.
- 8 [Instalar Distributed Execution Managers](#) página 92
 Los Distributed Execution Managers se instalan como una de estas dos funciones: DEM orquestador o DEM de trabajo. Debe haber instalada como mínimo una instancia de DEM por cada función, del mismo modo que se pueden instalar más instancias de DEM para disponer de conmutación por error y alta disponibilidad.
- 9 [Configurar el servicio de Windows para acceder a la base de datos de IaaS](#) página 95
 Un administrador del sistema puede cambiar el método de autenticación que se usa para acceder a la base de datos SQL en el tiempo de ejecución (una vez que la instalación se ha completado). La identidad de Windows de la cuenta que ha iniciado sesión actualmente es la que se usa de forma predeterminada para establecer la conexión con la base de datos después haberse instalado.
- 10 [Comprobar los servicios de IaaS](#) página 96
 Tras la instalación, el administrador del sistema comprueba que los servicios de IaaS se estén ejecutando. La ejecución de los servicios indica que la instalación se ha realizado correctamente.

Qué hacer a continuación

Instale un orquestador de DEM y, al menos, una instancia de trabajo de DEM. Consulte [“Instalar Distributed Execution Managers,”](#) página 92.

Instalar certificados de IaaS

En los entornos de producción, obtenga un certificado de dominio de una entidad de certificación de confianza. Importe el certificado al almacén de certificados raíz de confianza de todas las máquinas en las que tenga intención de instalar el componente de sitio web y Manager Service (máquinas de IIS) durante la instalación de IaaS.

Prerequisitos

Debe deshabilitar TLS1.2 en los certificados que usan SHA512 en máquinas con Windows 2012. Para obtener más información sobre cómo deshabilitar TLS1.2, consulte el artículo de Microsoft Knowledge Base en <http://support.microsoft.com/kb/245030>.

Procedimiento

- 1 Obtenga un certificado de dominio de una entidad de certificación de confianza.
- 2 Abra el Administrador de Internet Information Services (IIS).
- 3 Haga doble clic en **Certificados de servidor** en la vista Características.
- 4 Haga clic en **Importar** en el panel Acciones.
 - a Escriba un nombre de archivo en el cuadro de texto **Archivo de certificado** o haga clic en el botón Examinar (...) para ir al nombre de un archivo donde esté almacenado el certificado exportado.
 - b Si el certificado se exportó con una contraseña, escríbala en el cuadro de texto **Contraseña**.
 - c Seleccione **Marcar esta clave como exportable**.
- 5 Haga clic en **Aceptar**.
- 6 Haga clic en el certificado importado y seleccione **Ver**.
- 7 Confirme que el certificado y su cadena son de confianza.

Si el certificado no es de confianza, verá el mensaje **No se confía en este certificado de raíz de CA**.

NOTA: Deberá resolver este problema de confianza para poder continuar con la instalación. De lo contrario, la implementación no podrá realizarse.

- 8 Reinicie IIS o abra una ventana de símbolo del sistema con privilegios elevados y escriba `iisreset`.

Qué hacer a continuación

[“Descargar el instalador de IaaS,”](#) página 75.

Descargar el instalador de IaaS

Un administrador del sistema descarga el instalador de IaaS de el dispositivo de vRealize Automation en una máquina física o virtual con Windows 2008 o Windows 2012.

Si aparecen advertencias de certificado durante este proceso, continúe sin problemas hasta finalizar la instalación.

Prerequisitos

- [“Configurar el dispositivo de vRealize Automation principal,”](#) página 67 y, opcionalmente, [“Unir un el dispositivo de vRealize Automation a un clúster,”](#) página 72.
- Compruebe que los servidores de instalación cumplen los requisitos descritos en [“Requisitos del servidor de Model Management y el servicio web de IaaS,”](#) página 21.
- Confirme que ha importado un certificado a IIS y que la raíz del certificado o la entidad de certificación están en la raíz de confianza en la máquina de instalación.

- Si usa equilibradores de carga en su entorno, asegúrese de que reúnen los requisitos de configuración.

Procedimiento

- 1 (Opcional) Active HTTP si realiza la instalación en una máquina con Windows 2012.
 - a Seleccione **Características > Agregar características** en el Administrador del servidor.
 - b Expanda **Servicios WCF** en las características de .NET Framework.
 - c Seleccione **Activación HTTP**.
- 2 Inicie sesión en la máquina de Windows donde vaya a realizar la instalación.
- 3 Abra un explorador web.
- 4 Escriba la URL de la página de descarga del instalador de IaaS de VMware vRealize Automation.
Por ejemplo, **https://vra-va-hostname.domain.name:5480/installer**, donde *vra-va-hostname.domain.name* es el nombre de host de el dispositivo de vRealize Automation.
- 5 Descargue el instalador haciendo clic en el vínculo **Instalador de IaaS**.
- 6 Cuando se le pida, guarde el archivo del instalador (`setup__vra-va-hostname.domain.name@5480.exe`) en el escritorio.
No modifique el nombre de archivo, ya que sirve para conectar la instalación a el dispositivo de vRealize Automation.
- 7 Descargue el archivo del instalador en todas las máquinas en las que esté instalando componentes.

Qué hacer a continuación

Instale una base de datos de IaaS (consulte [“Elegir un escenario de base de datos de IaaS,”](#) página 76).

Elegir un escenario de base de datos de IaaS

IaaS de vRealize Automation utiliza una base de datos de Microsoft SQL Server para conservar la información sobre las máquinas que administra, así como sobre sus propios elementos y políticas.

Según cuáles sean sus preferencias y privilegios, puede elegir entre varios procedimientos para crear la base de datos de IaaS.

NOTA: Puede habilitar un SSL seguro al crear o actualizar la base de datos SQL. Así, cuando se disponga a crear o actualizar la base de datos SQL, puede usar la opción de SSL seguro para especificar que, cuando se realice la conexión con la base de datos SQL, se aplique la configuración de SSL que ya está establecida en el servidor SQL. SSL ofrece una conexión mucho más segura entre el servidor de IaaS y la base de datos SQL. Esta opción, disponible en el asistente de instalación personalizada, requiere que SSL ya está configurado en el servidor SQL. Para obtener información relacionada sobre cómo configurar SSL en el servidor SQL, consulte el artículo de la base de conocimientos 316898 sobre *cómo habilitar el cifrado SSL para una instancia de SQL Server mediante Microsoft Management Console* en el sitio de soporte de Microsoft.

Tabla 4-13. Elegir un escenario de base de datos de IaaS

Escenario	Procedimiento
Crear la base de datos de IaaS manualmente usando los scripts de base de datos provistos. Con esta opción, un administrador de base de datos puede revisar los cambios detenidamente antes de crear la base de datos.	“Crear la base de datos de IaaS manualmente,” página 77.
Preparar una base de datos vacía y usar el instalador para rellenar el esquema de base de datos. Con esta opción, el instalador puede utilizar un usuario de base de datos con privilegios dbo para rellenar la base de datos, en vez de necesitar privilegios sysadmin .	“Preparar una base de datos vacía,” página 78.
Usar el instalador para crear la base de datos. Se trata de la opción más sencilla, pero requiere privilegios sysadmin en el instalador.	“Crear la base de datos de IaaS con el asistente de instalación,” página 79.

Crear la base de datos de IaaS manualmente

El administrador del sistema de vRealize Automation puede crear la base de datos manualmente con scripts proporcionados por VMware.

Prerequisitos

- .NET 4.5.1 o una versión posterior debe estar instalado en el host de SQL Server.
- Use la autenticación de Windows (no la autenticación de SQL) para conectarse a la base de datos.
- Confirme los requisitos previos de instalación de base de datos. Consulte [“Requisitos del servidor de la base de datos de IaaS,”](#) página 21.
- Descargue los scripts del programa de instalación de la base de datos de IaaS en el dispositivo de vRealize Automation, a través de <https://vra-va-hostname.domain.name:5480/installer/>.

Procedimiento

- 1 Vaya al subdirectorio Database en el directorio donde haya descomprimido el archivo ZIP de instalación.
- 2 Descomprima el archivo DBInstall.zip en un directorio local.
- 3 Inicie sesión en el host de base de datos de Windows con derechos suficientes para crear y quitar bases de datos y privilegios **sysadmin** en la instancia de SQL Server.
- 4 Revise los scripts de implementación de base de datos según corresponda. En particular, revise los valores en la sección DBSettings del archivo CreateDatabase.sql y modifíquelos si así lo precisa.

Los valores en el script son los valores recomendados. Solamente ALLOW_SNAPSHOT_ISOLATION ON y READ_COMMITTED_SNAPSHOT ON son obligatorios.

- 5 Ejecute el siguiente comando con los argumentos descritos en la tabla.

```
BuildDB.bat /p:DBServer=db_server;
DBName=db_name;DBDir=db_dir;
LogDir=[log_dir];ServiceUser=service_user;
ReportLogin=web_user;
VersionString=version_string
```

Tabla 4-14. Valores de base de datos

Variable	Valor
<i>db_server</i>	Especifica la instancia de SQL Server con el formato <code>dbhostname[,port number]\SQL instance</code> . Indique un número de puerto solamente si utiliza un puerto distinto al predeterminado. El número de puerto predeterminado de Microsoft SQL es 1433. El valor predeterminado de <i>db_server</i> es <code>localhost</code> .
<i>db_name</i>	Nombre de la base de datos. El valor predeterminado es <code>vra</code> . Los nombres de base de datos no deben tener más de 128 caracteres ASCII.
<i>db_dir</i>	Ruta al directorio de datos de la base de datos (quitando la barra diagonal final).
<i>log_dir</i>	Ruta al directorio de log de la base de datos (quitando la barra diagonal final).
<i>service_user</i>	Nombre de usuario con el que se ejecuta Manager Service.
<i>Web_user</i>	Nombre de usuario con el que se ejecutan los servicios web.
<i>version_string</i>	Especifica la versión de vRealize Automation. Por ejemplo, la cadena de versión de la versión 6.1 sería <code>6.1.0.1200</code> .

La base de datos se ha creado.

Qué hacer a continuación

[“Instalar los componentes de IaaS en una configuración distribuida,”](#) página 73.

Preparar una base de datos vacía

Un administrador del sistema de vRealize Automation puede instalar el esquema de IaaS en una base de datos vacía. Este método de instalación proporciona el máximo control sobre la seguridad de la base de datos.

Prerequisitos

- Confirme los requisitos previos de instalación de base de datos. Consulte [“Requisitos del servidor de la base de datos de IaaS,”](#) página 21.
- Descargue los scripts del programa de instalación de la base de datos de IaaS en el dispositivo de vRealize Automation, a través de <https://vra-va-hostname.domain.name:5480/installer/>.

Procedimiento

- 1 Vaya al directorio Database que se encuentra dentro del directorio en el que extrajo el archivo ZIP de instalación.
- 2 Descomprima el archivo DBInstall.zip en un directorio local.
- 3 Inicie sesión en el host de la base de datos de Windows con privilegios **sysadmin** en la instancia de SQL Server.

- 4 Edite `CreateDatabase.sql` y sustituya todas las instancias de las variables de la tabla por los valores correctos de su entorno.

Tabla 4-15. Valores de base de datos

Variable	Valor
<code>\$(DBName)</code>	Nombre de la base de datos, por ejemplo <code>vra</code> . Los nombres de base de datos no deben tener más de 128 caracteres ASCII.
<code>\$(DBDir)</code>	Ruta al directorio de datos de la base de datos (quitando la barra diagonal final).
<code>\$(LogDir)</code>	Ruta al directorio de log de la base de datos (quitando la barra diagonal final).

- 5 Revise la configuración de la sección `DB Settings` de `CreateDatabase.sql` y edítela si es necesario.
La configuración del script es la recomendada para la base de datos de IaaS. Solo son obligatorios `ALLOW_SNAPSHOT_ISOLATION ON` y `READ_COMMITTED_SNAPSHOT ON`.
- 6 Abra SQL Server Management Studio.
- 7 Haga clic en **Nueva consulta**.
Se abrirá una ventana de consulta SQL.
- 8 En el menú **Consulta**, asegúrese de que **Modo SQLCMD** está activado.
- 9 Pegue el contenido modificado completo de `CreateDatabase.sql` en el panel de consulta.
- 10 Haga clic en **Ejecutar**.
El script se ejecutará y se creará la base de datos.

Qué hacer a continuación

[“Instalar los componentes de IaaS en una configuración distribuida,”](#) página 73.

Crear la base de datos de IaaS con el asistente de instalación

vRealize Automation utiliza una base de datos de Microsoft SQL Server para conservar la información sobre las máquinas que administra, así como sobre sus propios elementos y políticas.

Los siguientes pasos describen cómo crear la base de datos de IaaS usando el instalador o rellenar una base de datos vacía ya existente. La base de datos también se puede crear manualmente. Consulte [“Crear la base de datos de IaaS manualmente,”](#) página 77.

Prerequisitos

- Si va a crear la base de datos con autenticación de Windows y en lugar de con autenticación de SQL, confirme que el usuario que ejecuta el instalador tiene derechos de **sysadmin** en el servidor SQL.
- [“Descargar el instalador de IaaS,”](#) página 75.

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 2 Haga clic en **Siguiente**.
- 3 Acepte el acuerdo de licencia y haga clic en **Siguiente**.

- 4 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 5 Haga clic en **Siguiente**.
- 6 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 7 Seleccione **Servidor de IaaS** en Selección de componentes, en la página Tipo de instalación.
- 8 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 9 Haga clic en **Siguiente**.
- 10 En la página de instalación personalizada del servidor de IaaS, seleccione **Base de datos**.
- 11 En el cuadro de texto **Instancia de base de datos**, indique la instancia de base de datos o haga clic en **Examinar** para seleccionarla de la lista de instancias. Si la instancia de base de datos está en un puerto que no es predeterminado, indique el número de puerto en la especificación de la instancia con la forma *dbhost,SQL_port_number\SQLinstance*. El número de puerto predeterminado de Microsoft SQL es 1443.
- 12 (Opcional) Active la casilla **Usar SSL para la conexión de base de datos**.
Esta casilla está activada de forma predeterminada. SSL ofrece una conexión mucho más segura entre el servidor de IaaS y la base de datos SQL. Sin embargo, debe configurar SSL en el servidor SQL para poder usar esta opción. Para obtener información relacionada sobre cómo configurar SSL en el servidor SQL, consulte el artículo de la base de conocimientos 316898 sobre *cómo habilitar el cifrado SSL para una instancia de SQL Server mediante Microsoft Management Console* en el sitio de soporte de Microsoft.
- 13 Elija el tipo de instalación de base de datos en el panel **Nombre de base de datos**.
 - Seleccione **Usar esquema vacío existente** para crear el esquema en una base de datos existente.
 - Escriba un nombre de base de datos nuevo o utilice el nombre predeterminado **vra** para crear una base de datos nueva. Los nombres de base de datos no deben tener más de 128 caracteres ASCII.
- 14 Anule la selección de la opción **Usar directorios de datos y log predeterminados** para especificar otras ubicaciones o déjela seleccionada para usar los directorios predeterminados (recomendado).
- 15 Seleccione un método de autenticación para instalar la base de datos de la lista **Autenticación**.
 - Seleccione **Usar identidad de Windows...** para utilizar las credenciales con las que se va a ejecutar el instalador para crear la base de datos.
 - Si va a usar la autenticación de SQL, anule la selección de **Usar identidad de Windows...** Escriba las credenciales de SQL en los cuadros de texto de usuario y contraseña.
De manera predeterminada, la cuenta de usuario del servicio de Windows se usa durante el acceso en tiempo de ejecución a la base de datos, y debe tener derechos sysadmin en la instancia de SQL Server. Las credenciales utilizadas para acceder a la base de datos en tiempo de ejecución se pueden configurar para usar credenciales de SQL.
- 16 Haga clic en **Siguiente**.

- 17 Complete la comprobación de requisitos previos.

Opción	Descripción
Sin errores	Haga clic en Siguiente .
Sin errores críticos	Haga clic en Omitir .
Errores críticos	Si se omiten errores críticos, la instalación no se llevará a cabo. Si aparecen advertencias, seleccione la advertencia en el panel izquierdo y siga las instrucciones que se muestran a la derecha. Aborde todos los errores críticos y haga clic en Comprobar de nuevo para confirmar que se han solucionado.

- 18 Haga clic en **Instalar**.
- 19 Cuando aparezca el mensaje que indica que todo está correcto, anule la selección de **Guiarme por la configuración inicial** y haga clic en **Siguiente**.
- 20 Haga clic en **Finalizar**.

La base de datos estará lista para usarse.

Instalar un componente de sitio web de IaaS con Model Manager Data

El administrador del sistema instala el componente de sitio web para dar acceso a las funciones de infraestructura en la consola web de vRealize Automation. Se pueden instalar una o varias instancias del componente de sitio web, pero Model Manager Data se debe configurar en la máquina donde se aloje el primer componente de sitio web. Model Manager Data solamente se instala una vez.

Prerequisitos

- Instale la base de datos de IaaS (consulte [“Elegir un escenario de base de datos de IaaS,”](#) página 76).
- Si ya tiene otros componentes instalados en este entorno, asegúrese de que conoce la frase de contraseña que se creó. Consulte [“Frase de contraseña de seguridad,”](#) página 29.
- Si usa equilibradores de carga en su entorno, asegúrese de que reúnen los requisitos de configuración.

Procedimiento

- 1 [Instalar el primer componente de sitio web de IaaS](#) página 81
El administrador del sistema instala el componente de sitio web para ofrecer acceso a las funciones de infraestructura en la consola web de vRealize Automation.
- 2 [Configurar Model Manager Data](#) página 83
El componente Model Manager se instala en la misma máquina que aloja el primer componente de sitio web. Model Manager Data se puede instalar solamente una vez.

Se puede instalar más componentes de sitio web o instalar Manager Service. Consulte [“Instalar más componentes de sitio web de IaaS,”](#) página 85 o [“Instalar el Manager Service activo,”](#) página 87.

Instalar el primer componente de sitio web de IaaS

El administrador del sistema instala el componente de sitio web para ofrecer acceso a las funciones de infraestructura en la consola web de vRealize Automation.

Puede instalar varios componentes de sitio web, pero solo uno podrá contener los datos de Model Manager. Los datos de Model Manager deben instalarse en el primer componente de sitio web que cree.

Prerequisitos

- [“Crear la base de datos de IaaS con el asistente de instalación,”](#) página 79.

- Compruebe que el entorno reúne los requisitos descritos en “Requisitos del servidor de Model Management y el servicio web de IaaS,” página 21.
- Si ya tiene otros componentes instalados en este entorno, asegúrese de que conoce la frase de contraseña que se creó. Consulte “Frase de contraseña de seguridad,” página 29.
- Si usa equilibradores de carga en su entorno, asegúrese de que reúnen los requisitos de configuración.

Procedimiento

- 1 Deshabilite las comprobaciones de estado del equilibrador de carga y procure que el tráfico se dirija al nodo.
- 2 Deshabilite los otros nodos que haya en el equilibrador de carga.
- 3 Haga clic con el botón derecho en el archivo de instalación `setup__vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 4 Haga clic en **Siguiente**.
- 5 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 6 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 7 Haga clic en **Siguiente**.
- 8 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 9 Seleccione **Servidor de IaaS** en Selección de componentes, en la página Tipo de instalación.
- 10 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 11 Haga clic en **Siguiente**.
- 12 Seleccione **Sitio web** y **ModelManagerData** en la página Instalación personalizada de servidor de IaaS.
- 13 Seleccione un sitio web de los sitios web disponibles o acepte el sitio web predeterminado en la pestaña **Sitio web de Model Manager y administración**.
- 14 Escriba un número de puerto disponible en el cuadro de texto **Número de puerto** o acepte el puerto predeterminado 443.
- 15 Haga clic en **Probar enlace** para confirmar que el número de puerto puede utilizarse.

- 16 Seleccione el certificado de este componente.
 - a Si importó un certificado después de iniciar la instalación, haga clic en **Actualizar** para actualizar la lista.
 - b Seleccione el certificado que quiera usar en **Certificados disponibles**.
 - c Si importó un certificado que no tiene un nombre descriptivo y que no figura en la lista, anule la selección de **Mostrar certificados con nombres descriptivos** y haga clic en **Actualizar**.

Si está realizando la instalación en un entorno en el que no se usan equilibradores de carga, puede seleccionar **Generar un certificado autofirmado** en lugar de seleccionar un certificado. Si está instalando más componentes de sitio web detrás de un equilibrador de carga, no genere certificados autofirmados. Importe el certificado desde el servidor web de IaaS principal para garantizar que se usa el mismo certificado en todos los servidores tras el equilibrador de carga.

- 17 (Opcional) Haga clic en **Ver certificado**, vea el certificado y haga clic en **Aceptar** para cerrar la ventana de información.
- 18 (Opcional) Seleccione **Suprimir discrepancia de certificado** para eliminar los errores de certificado. La instalación omite los errores de discrepancia de nombre de certificado, así como cualquier otro error de discrepancia de revocación de certificado.

Esta opción es menos segura.

Configurar Model Manager Data

El componente Model Manager se instala en la misma máquina que aloja el primer componente de sitio web. Model Manager Data se puede instalar solamente una vez.

Prerequisitos

[“Instalar el primer componente de sitio web de IaaS,”](#) página 81.

Procedimiento

- 1 Haga clic en la pestaña **Model Manager Data**.
- 2 Escriba el nombre de dominio completo del dispositivo de vRealize Automation en el cuadro de texto **Servidor**.
Las direcciones IP no se reconocen.
Por ejemplo, **vra.mycompany.com**.
- 3 Haga clic en **Cargar** para mostrar el **Tenant predeterminado de SSO**.
El tenant predeterminado **vsphere.local** se crea automáticamente cuando se configura el inicio de sesión único. No lo modifique.
- 4 Haga clic en **Descargar** para importar el certificado desde el dispositivo virtual.
La descarga del certificado puede tardar varios minutos.
- 5 (Opcional) Haga clic en **Ver certificado**, vea el certificado y haga clic en **Aceptar** para cerrar la ventana de información.
- 6 Haga clic en **Aceptar certificado**.
- 7 Escriba **administrator@vsphere.local** en el cuadro de texto **Nombre de usuario** y la contraseña que creó al configurar el SSO en los cuadros de texto **Contraseña** y **Confirmar**.
- 8 (Opcional) Haga clic en **Probar** para comprobar las credenciales.

- 9 Escriba el nombre completo del servidor de sitio web de IaaS en el cuadro de texto **Servidor de IaaS**.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo del equilibrador de carga del servidor de sitio web de IaaS. Por ejemplo, IaaS-load-balancer.eng.mycompany.com . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo del servidor de sitio web de IaaS. Por ejemplo, IaaS.eng.mycompany.com . Las direcciones IP no se reconocen.

- 10 Haga clic en **Probar** para comprobar la conexión del servidor.
- 11 Haga clic en **Siguiente**.
- 12 Complete la comprobación de requisitos previos.

Opción	Descripción
Sin errores	Haga clic en Siguiente .
Sin errores críticos	Haga clic en Omitir .
Errores críticos	Si se omiten errores críticos, la instalación no se llevará a cabo. Si aparecen advertencias, seleccione la advertencia en el panel izquierdo y siga las instrucciones que se muestran a la derecha. Aborde todos los errores críticos y haga clic en Comprobar de nuevo para confirmar que se han solucionado.

- 13 En los cuadros de texto **Información de instalación de servidor** de la página Configuración de cuenta y servidor, escriba el nombre de usuario y la contraseña de la cuenta de usuario que tenga privilegios administrativos en el servidor de instalación actual.
- 14 Proporcione la frase de contraseña que se usó para generar la clave de cifrado con la que se protege la base de datos.

Opción	Descripción
Si ya tiene componentes instalados en este entorno	Escriba la frase de contraseña que creó anteriormente en los cuadros de texto Frase de contraseña y Confirmar .
Si es la primera instalación	Escriba una frase de contraseña en los cuadros de texto Frase de contraseña y Confirmar . Deberá usar esta frase de contraseña cada vez que quiera instalar un componente nuevo.

Guárdela en un lugar seguro para poder usarla en ocasiones posteriores.

- 15 Especifique el servidor de base de datos de IaaS, el nombre de base de datos y el método de autenticación del servidor de base de datos en el cuadro de texto **Información de instalación de base de datos de Microsoft SQL**.

Esta es la información de autenticación, nombre y servidor de la base de datos IaaS que creó anteriormente.

- 16 Haga clic en **Siguiente**.
- 17 Haga clic en **Instalar**.
- 18 Cuando la instalación finalice, anule la selección de **Guiarme por la configuración inicial** y haga clic en **Siguiente**.

Qué hacer a continuación

Se puede instalar más componentes de sitio web o instalar Manager Service. Consulte [“Instalar más componentes de sitio web de IaaS,”](#) página 85 o [“Instalar el Manager Service activo,”](#) página 87. Si no tiene previsto añadir más nodos al equilibrador de carga, habilite las comprobaciones de estado que correspondan.

Instalar más componentes de sitio web de IaaS

El componente de sitio web ofrece acceso a las funciones de infraestructura en la consola web de vRealize Automation. El administrador del sistema puede instalar una o varias instancias del componente de sitio web.

No instale datos de Model Manager con el componente de sitio web. Solamente el primer componente de sitio web que instale podrá contener los datos de Model Manager.

Prerequisitos

- [“Instalar un componente de sitio web de IaaS con Model Manager Data,”](#) página 81.
- Compruebe que el entorno reúne los requisitos descritos en [“Requisitos del servidor de Model Management y el servicio web de IaaS,”](#) página 21.
- Si ya tiene otros componentes instalados en este entorno, asegúrese de que conoce la frase de contraseña que se creó. Consulte [“Frase de contraseña de seguridad,”](#) página 29.
- Si usa equilibradores de carga en su entorno, asegúrese de que reúnen los requisitos de configuración.

Procedimiento

- 1 Deshabilite las comprobaciones de estado del equilibrador de carga y procure que el tráfico se dirija al nodo.
- 2 Haga clic con el botón derecho en el archivo de instalación `setup_vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 3 Haga clic en **Siguiente**.
- 4 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 5 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 6 Haga clic en **Siguiente**.
- 7 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 8 Seleccione **Servidor de IaaS** en Selección de componentes, en la página Tipo de instalación.
- 9 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 10 Haga clic en **Siguiente**.
- 11 Seleccione **Sitio web** en la página Instalación personalizada de servidor de IaaS.

- 12 Seleccione un sitio web de los sitios web disponibles o acepte el sitio web predeterminado en la pestaña **Sitio web de Model Manager y administración**.
- 13 Escriba un número de puerto disponible en el cuadro de texto **Número de puerto** o acepte el puerto predeterminado 443.
- 14 Haga clic en **Probar enlace** para confirmar que el número de puerto puede utilizarse.
- 15 Seleccione el certificado de este componente.

- a Si importó un certificado después de iniciar la instalación, haga clic en **Actualizar** para actualizar la lista.
- b Seleccione el certificado que quiera usar en **Certificados disponibles**.
- c Si importó un certificado que no tiene un nombre descriptivo y que no figura en la lista, anule la selección de **Mostrar certificados con nombres descriptivos** y haga clic en **Actualizar**.

Si está realizando la instalación en un entorno en el que no se usan equilibradores de carga, puede seleccionar **Generar un certificado autofirmado** en lugar de seleccionar un certificado. Si está instalando más componentes de sitio web detrás de un equilibrador de carga, no genere certificados autofirmados. Importe el certificado desde el servidor web de IaaS principal para garantizar que se usa el mismo certificado en todos los servidores tras el equilibrador de carga.

- 16 (Opcional) Haga clic en **Ver certificado**, vea el certificado y haga clic en **Aceptar** para cerrar la ventana de información.
- 17 (Opcional) Seleccione **Suprimir discrepancia de certificado** para eliminar los errores de certificado. La instalación omite los errores de discrepancia de nombre de certificado, así como cualquier otro error de discrepancia de revocación de certificado.

Esta opción es menos segura.

- 18 Escriba la información de servidor de IaaS en el cuadro de texto **Servidor de IaaS**.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo del equilibrador de carga del servidor de sitio web de IaaS. Por ejemplo, IaaS-load-balancer.eng.mycompany.com .
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo del servidor de sitio web de IaaS. Por ejemplo, IaaS.eng.mycompany.com .

- 19 Haga clic en **Probar** para comprobar la conexión del servidor.
- 20 Haga clic en **Siguiente**.
- 21 Complete la comprobación de requisitos previos.

Opción	Descripción
Sin errores	Haga clic en Siguiente .
Sin errores críticos	Haga clic en Omitir .
Errores críticos	Si se omiten errores críticos, la instalación no se llevará a cabo. Si aparecen advertencias, seleccione la advertencia en el panel izquierdo y siga las instrucciones que se muestran a la derecha. Aborde todos los errores críticos y haga clic en Comprobar de nuevo para confirmar que se han solucionado.

- 22 En los cuadros de texto **Información de instalación de servidor** de la página Configuración de cuenta y servidor, escriba el nombre de usuario y la contraseña de la cuenta de usuario que tenga privilegios administrativos en el servidor de instalación actual.

- 23 Proporcione la frase de contraseña que se usó para generar la clave de cifrado con la que se protege la base de datos.

Opción	Descripción
Si ya tiene componentes instalados en este entorno	Escriba la frase de contraseña que creó anteriormente en los cuadros de texto Frase de contraseña y Confirmar .
Si es la primera instalación	Escriba una frase de contraseña en los cuadros de texto Frase de contraseña y Confirmar . Deberá usar esta frase de contraseña cada vez que quiera instalar un componente nuevo.

Guárdela en un lugar seguro para poder usarla en ocasiones posteriores.

- 24 Especifique el servidor de base de datos de IaaS, el nombre de base de datos y el método de autenticación del servidor de base de datos en el cuadro de texto **Información de instalación de base de datos de Microsoft SQL**.

Esta es la información de autenticación, nombre y servidor de la base de datos IaaS que creó anteriormente.

- 25 Haga clic en **Siguiente**.
- 26 Haga clic en **Instalar**.
- 27 Cuando la instalación finalice, anule la selección de **Guiarme por la configuración inicial** y haga clic en **Siguiente**.

Qué hacer a continuación

[“Instalar el Manager Service activo,”](#) página 87. Si no tiene previsto añadir más nodos al equilibrador de carga, habilite las comprobaciones de estado que correspondan.

Instalar el Manager Service activo

El componente Manager Service coordina la comunicación entre los agentes y los agentes de proxy, la base de datos y SMTP. Debe haber instalada una instancia del componente Manager Service como mínimo. Se puede instalar una instancia activa y otra de copia de seguridad del componente Manager Service para proporcionar redundancia en una implementación de alta disponibilidad.

Prerequisitos

- Si ya tiene otros componentes instalados en este entorno, asegúrese de que conoce la frase de contraseña que se creó. Consulte [“Frase de contraseña de seguridad,”](#) página 29.
- (Opcional) Si desea instalar Manager Service en un sitio web que no sea el predeterminado, cree antes un sitio web en Internet Information Services.
- Microsoft .NET Framework 4.5.2 está instalado.
- Asegúrese de que ha importado a IIS un certificado de una entidad de certificación y, asimismo, de que el certificado raíz o la entidad de certificación son de confianza. Todos los componentes bajo el equilibrador de carga deben tener el mismo certificado.
- Compruebe que el equilibrador de carga de sitio web esté configurado y que su valor de tiempo de espera esté establecido en un mínimo de 180 segundos.
- [“Instalar un componente de sitio web de IaaS con Model Manager Data,”](#) página 81.

Procedimiento

- 1 Deshabilite las comprobaciones de estado del equilibrador de carga y procure que el tráfico se dirija al nodo.
- 2 Haga clic con el botón derecho en el archivo de instalación `setup_vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.

- 3 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 4 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.

Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 5 Haga clic en **Siguiente**.
- 6 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 7 Seleccione **Servidor de IaaS** en Selección de componentes, en la página Tipo de instalación.
- 8 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 9 Haga clic en **Siguiente**.
- 10 Seleccione **Manager Service** en la página Instalación personalizada de servidor de IaaS.
- 11 Escriba la información de servidor de IaaS en el cuadro de texto **Servidor de IaaS**.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo del equilibrador de carga del servidor de sitio web de IaaS. Por ejemplo, IaaS-load-balancer.eng.mycompany.com .
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo del servidor de sitio web de IaaS. Por ejemplo, IaaS.eng.mycompany.com .

- 12 Seleccione **Nodo activo con tipo de inicio establecido en automático**.
- 13 Seleccione un sitio web de los sitios web disponibles o acepte el sitio web predeterminado en la pestaña **Sitio web de Model Manager y administración**.
- 14 Escriba un número de puerto disponible en el cuadro de texto **Número de puerto** o acepte el puerto predeterminado 443.
- 15 Haga clic en **Probar enlace** para confirmar que el número de puerto puede utilizarse.
- 16 Seleccione el certificado de este componente.
 - a Si importó un certificado después de iniciar la instalación, haga clic en **Actualizar** para actualizar la lista.
 - b Seleccione el certificado que quiera usar en **Certificados disponibles**.
 - c Si importó un certificado que no tiene un nombre descriptivo y que no figura en la lista, anule la selección de **Mostrar certificados con nombres descriptivos** y haga clic en **Actualizar**.

Si está realizando la instalación en un entorno en el que no se usan equilibradores de carga, puede seleccionar **Generar un certificado autofirmado** en lugar de seleccionar un certificado. Si está instalando más componentes de sitio web detrás de un equilibrador de carga, no genere certificados autofirmados. Importe el certificado desde el servidor web de IaaS principal para garantizar que se usa el mismo certificado en todos los servidores tras el equilibrador de carga.
- 17 (Opcional) Haga clic en **Ver certificado**, vea el certificado y haga clic en **Aceptar** para cerrar la ventana de información.

- 18 Haga clic en **Siguiente**.
- 19 Compruebe los requisitos previos y haga clic en **Siguiente**.
- 20 En los cuadros de texto **Información de instalación de servidor** de la página Configuración de cuenta y servidor, escriba el nombre de usuario y la contraseña de la cuenta de usuario que tenga privilegios administrativos en el servidor de instalación actual.
- 21 Proporcione la frase de contraseña que se usó para generar la clave de cifrado con la que se protege la base de datos.

Opción	Descripción
Si ya tiene componentes instalados en este entorno	Escriba la frase de contraseña que creó anteriormente en los cuadros de texto Frase de contraseña y Confirmar .
Si es la primera instalación	Escriba una frase de contraseña en los cuadros de texto Frase de contraseña y Confirmar . Deberá usar esta frase de contraseña cada vez que quiera instalar un componente nuevo.

Guárdela en un lugar seguro para poder usarla en ocasiones posteriores.

- 22 Especifique el servidor de base de datos de IaaS, el nombre de base de datos y el método de autenticación del servidor de base de datos en el cuadro de texto **Información de instalación de base de datos de Microsoft SQL**.

Esta es la información de autenticación, nombre y servidor de la base de datos IaaS que creó anteriormente.
- 23 Haga clic en **Siguiente**.
- 24 Haga clic en **Instalar**.
- 25 Cuando la instalación finalice, anule la selección de **Guiarme por la configuración inicial** y haga clic en **Siguiente**.
- 26 Haga clic en **Finalizar**.

Qué hacer a continuación

Para garantizar que el Manager Service que ha instalado sea la instancia activa, compruebe que el servicio de vCloud Automation Center se esté ejecutando y establézcalo como el tipo de inicio "Automático".

Puede instalar otra instancia del componente Manager Service como copia de seguridad pasiva, que podrá iniciar manualmente si se produce un error en la instancia activa. Consulte ["Instalar un componente de copia de seguridad de Manager Service,"](#) página 89.

Un administrador del sistema puede cambiar el método de autenticación que se usa para acceder a la base de datos SQL en el tiempo de ejecución (una vez que la instalación se ha completado). Consulte ["Configurar el servicio de Windows para acceder a la base de datos de IaaS,"](#) página 95.

Instalar un componente de copia de seguridad de Manager Service

Se puede instalar una instancia de copia de seguridad pasiva del componente Manager Service que se puede iniciar manualmente con el fin de proporcionar redundancia en una implementación de alta disponibilidad.

Prerequisitos

- Si ya tiene otros componentes instalados en este entorno, asegúrese de que conoce la frase de contraseña que se creó. Consulte ["Frase de contraseña de seguridad,"](#) página 29.
- (Opcional) Si desea instalar Manager Service en un sitio web que no sea el predeterminado, cree antes un sitio web en Internet Information Services.
- Microsoft .NET Framework 4.5.2 está instalado.

- Asegúrese de que ha importado a IIS un certificado de una entidad de certificación y, asimismo, de que el certificado raíz o la entidad de certificación son de confianza. Todos los componentes bajo el equilibrador de carga deben tener el mismo certificado.
- Compruebe que el equilibrador de carga del sitio web está configurado.
- [“Instalar un componente de sitio web de IaaS con Model Manager Data,”](#) página 81.

Procedimiento

- 1 Deshabilite las comprobaciones de estado del equilibrador de carga y procure que el tráfico se dirija al nodo.
- 2 Haga clic con el botón derecho en el archivo de instalación `setup__vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 3 Haga clic en **Siguiente**.
- 4 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 5 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 6 Haga clic en **Siguiente**.
- 7 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 8 Seleccione **Servidor de IaaS** en Selección de componentes, en la página Tipo de instalación.
- 9 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 10 Haga clic en **Siguiente**.
- 11 Seleccione **Manager Service** en la página Instalación personalizada de servidor de IaaS.
- 12 Escriba la información de servidor de IaaS en el cuadro de texto **Servidor de IaaS**.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo del equilibrador de carga del servidor de sitio web de IaaS. Por ejemplo, IaaS-Load-balancer.eng.mycompany.com .
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo del servidor de sitio web de IaaS. Por ejemplo, IaaS.eng.mycompany.com .

- 13 Seleccione **Nodo de espera pasiva de recuperación ante desastres**.
- 14 Seleccione un sitio web de los sitios web disponibles o acepte el sitio web predeterminado en la pestaña **Sitio web de Model Manager y administración**.
- 15 Escriba un número de puerto disponible en el cuadro de texto **Número de puerto** o acepte el puerto predeterminado 443.
- 16 Haga clic en **Probar enlace** para confirmar que el número de puerto puede utilizarse.

- 17 Seleccione el certificado de este componente.
 - a Si importó un certificado después de iniciar la instalación, haga clic en **Actualizar** para actualizar la lista.
 - b Seleccione el certificado que quiera usar en **Certificados disponibles**.
 - c Si importó un certificado que no tiene un nombre descriptivo y que no figura en la lista, anule la selección de **Mostrar certificados con nombres descriptivos** y haga clic en **Actualizar**.

Si está realizando la instalación en un entorno en el que no se usan equilibradores de carga, puede seleccionar **Generar un certificado autofirmado** en lugar de seleccionar un certificado. Si está instalando más componentes de sitio web detrás de un equilibrador de carga, no genere certificados autofirmados. Importe el certificado desde el servidor web de IaaS principal para garantizar que se usa el mismo certificado en todos los servidores tras el equilibrador de carga.
- 18 (Opcional) Haga clic en **Ver certificado**, vea el certificado y haga clic en **Aceptar** para cerrar la ventana de información.
- 19 Haga clic en **Siguiente**.
- 20 Compruebe los requisitos previos y haga clic en **Siguiente**.
- 21 En los cuadros de texto **Información de instalación de servidor** de la página Configuración de cuenta y servidor, escriba el nombre de usuario y la contraseña de la cuenta de usuario que tenga privilegios administrativos en el servidor de instalación actual.
- 22 Proporcione la frase de contraseña que se usó para generar la clave de cifrado con la que se protege la base de datos.

Opción	Descripción
Si ya tiene componentes instalados en este entorno	Escriba la frase de contraseña que creó anteriormente en los cuadros de texto Frase de contraseña y Confirmar .
Si es la primera instalación	Escriba una frase de contraseña en los cuadros de texto Frase de contraseña y Confirmar . Deberá usar esta frase de contraseña cada vez que quiera instalar un componente nuevo.

Guárdela en un lugar seguro para poder usarla en ocasiones posteriores.

- 23 Especifique el servidor de base de datos de IaaS, el nombre de base de datos y el método de autenticación del servidor de base de datos en el cuadro de texto **Información de instalación de base de datos de Microsoft SQL**.

Esta es la información de autenticación, nombre y servidor de la base de datos IaaS que creó anteriormente.
- 24 Haga clic en **Siguiente**.
- 25 Haga clic en **Instalar**.
- 26 Cuando la instalación finalice, anule la selección de **Guiarme por la configuración inicial** y haga clic en **Siguiente**.
- 27 Haga clic en **Finalizar**.

Qué hacer a continuación

Si no va a añadir más nodos al equilibrador de carga WEB, habilite las comprobaciones de estado que correspondan.

Para garantizar que el Manager Service que ha instalado es una instancia de copia de seguridad pasiva, compruebe que el servicio vRealize Automation no se está ejecutando y establézcalo en el tipo de inicio "Manual".

Un administrador del sistema puede cambiar el método de autenticación que se usa para acceder a la base de datos SQL en el tiempo de ejecución (una vez que la instalación se ha completado). Consulte [“Configurar el servicio de Windows para acceder a la base de datos de IaaS,”](#) página 95.

Instalar Distributed Execution Managers

Los Distributed Execution Managers se instalan como una de estas dos funciones: DEM orquestador o DEM de trabajo. Debe haber instalada como mínimo una instancia de DEM por cada función, del mismo modo que se pueden instalar más instancias de DEM para disponer de conmutación por error y alta disponibilidad.

El administrador del sistema debe elegir máquinas de instalación que reúnan los requisitos de sistema predefinidos. El DEM orquestador y el DEM de trabajo pueden estar en la misma máquina.

Tenga en cuenta los siguientes aspectos cuando vaya a instalar Distributed Execution Managers:

- Los DEM orquestadores admiten la alta disponibilidad activa-activa. Por lo general, se instala un DEM orquestador en cada máquina de Manager Service.
- Instale el DEM orquestador en una máquina que posea una conectividad de red segura con el host de Model Manager.
- Instale un segundo DEM orquestador en otra máquina para disponer de conmutación por error.
- Los DEM de trabajo se suelen instalar en el servidor de IaaS Manager Service o en un servidor aparte. Este servidor debe tener conectividad de red con el host de Model Manager.
- Se pueden instalar más instancias de DEM para disponer de redundancia y escalabilidad, incluso se pueden instalar varias en la misma máquina.

Existen requisitos específicos de la instalación de DEM que dependen de los endpoints que use. Consulte [“Requisitos de Distributed Execution Manager,”](#) página 23.

Instalar Distributed Execution Managers

Un administrador del sistema instala al menos un DEM de trabajo y un DEM orquestador. El procedimiento de instalación es el mismo para ambas funciones.

Los DEM orquestadores admiten la alta disponibilidad activa-activa. Por lo general, se instala un solo DEM orquestador en cada máquina de Manager Service. Los DEM orquestadores y los DEM de trabajo se pueden instalar en la misma máquina.

Prerequisitos

[“Descargar el instalador de IaaS,”](#) página 75.

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 2 Haga clic en **Siguiente**.
- 3 Acepte el acuerdo de licencia y haga clic en **Siguiente**.

- 4 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 5 Haga clic en **Siguiente**.
- 6 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 7 Seleccione **Distributed Execution Managers** en Selección de componentes de la página Tipo de instalación.
- 8 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 9 Haga clic en **Siguiente**.
- 10 Compruebe los requisitos previos y haga clic en **Siguiente**.
- 11 Escriba las credenciales de inicio de sesión con las que se va a ejecutar el servicio. Debe ser una cuenta de administrador local.
- 12 Haga clic en **Siguiente**.
- 13 Seleccione el tipo de instalación del menú desplegable **Función de DEM**.

Opción	Descripción
Trabajo	El trabajo ejecuta los flujos de trabajo.
Orquestador	El orquestador controla las actividades del DEM de trabajo (programación y preprocesamiento de flujos de trabajo incluidos) y supervisa el estado conectado del DEM de trabajo.

- 14 Escriba un nombre único con el que se identificará este DEM en el cuadro de texto **Nombre de DEM**.
Si tiene previsto usar la herramienta de migración, este nombre debe ser exactamente igual al que utilizó en la instalación de vCloud Automation Center 5.2.3. Dicho nombre no puede contener espacios ni superar los 128 caracteres. Si escribe un nombre que ya se ha usado antes, aparecerá el mensaje: "El nombre de DEM ya existe. Para especificar otro nombre de DEM, haga clic en Sí. Si está restaurando o reinstalando un DEM con el mismo nombre, haga clic en No."
- 15 (Opcional) Escriba una descripción de esta instancia en **Descripción de DEM**.
- 16 Escriba los nombres de host y los puertos en los cuadros de texto **Nombre de host de Manager Service** y **Nombre de host de servicio web de Model Manager**.

Opción	Descripción
Si usa un equilibrador de carga	Escriba los nombres de dominio completos de los equilibradores de carga de Manager Service y del servicio web de Model Manager. Por ejemplo, manager-load-balancer.eng.mycompany.com:443 y web-load-balancer.eng.mycompany.com:443 .
Si no usa un equilibrador de carga	Escriba los nombres de dominio completos de Manager Service y del servicio web de Model Manager. Por ejemplo, manager-service.eng.mycompany.com:443 y model-manager.eng.mycompany.com:443 .

- 17 (Opcional) Haga clic en **Probar** para probar las conexiones con Manager Service y con el servicio web de Model Manager.
- 18 Haga clic en **Agregar**.
- 19 Haga clic en **Siguiente**.
- 20 Haga clic en **Instalar**.
- 21 Cuando la instalación finalice, anule la selección de **Guiarme por la configuración inicial** y haga clic en **Siguiente**.
- 22 Haga clic en **Finalizar**.

Qué hacer a continuación

Confirme que el servicio se está ejecutando y que el log no contiene errores. El nombre de servicio es *DEM Role - Name* de VMware, donde Función es trabajo u orquestador. La ubicación del log es *Install Location*\Distributed Execution Manager\Name\Logs.

Repita este procedimiento para instalar más instancias de DEM.

Configurar el DEM de conexión a SCVMM en una ruta de instalación no estándar

El archivo de configuración de trabajo de DEM (*DynamicOps.DEM.exe.config*) apunta de forma predeterminada a la ruta de instalación estándar de la consola de Microsoft System Center Virtual Machine Manager (SCVMM): *{ProgramFiles}\Microsoft System Center 2012\Virtual Machine Manager\bin*. El administrador del sistema deberá cambiar la ruta si la consola está instalada en otra ubicación.

Este procedimiento es necesario únicamente cuando existen agentes y endpoints de SCVMM.

Prerequisitos

- Si la consola de SCVMM se ha instalado en otra ubicación, el archivo de configuración del trabajo de DEM (que está en *Program Files (x86)\VMware\VCAC\Distributed Execution Manager\<InstanceName>\DynamicOps.DEM.exe.config*) se deberá actualizar para cambiar la ruta predeterminada en la sección *assemblyLoadConfiguration* de forma que apunte a la nueva carpeta.

```
<assemblyLoadConfiguration>
    <assemblies>
      <!-- List of required assemblies for Scvmm -->
      <add name="Errors" path="{ProgramFiles}\Microsoft System Center 2012\Virtual
        Machine Manager\bin" />
      [...]
    </assemblies>
</assemblyLoadConfiguration>
```

Procedimiento

- 1 Detenga el trabajo de DEM.
- 2 Averigüe la ruta de instalación.
- 3 Actualice el archivo *DynamicOps.DEM.exe.config*.
- 4 Reinicie el trabajo de DEM.

La ruta predeterminada del trabajo de DEM se actualizará para reflejar la nueva carpeta.

Configurar el servicio de Windows para acceder a la base de datos de IaaS

Un administrador del sistema puede cambiar el método de autenticación que se usa para acceder a la base de datos SQL en el tiempo de ejecución (una vez que la instalación se ha completado). La identidad de Windows de la cuenta que ha iniciado sesión actualmente es la que se usa de forma predeterminada para establecer la conexión con la base de datos después haberse instalado.

Habilitar el acceso a la base de datos de IaaS desde el usuario del servicio

Si la base de datos SQL se instala en un host independiente de Manager Service, el acceso a la base de datos se debe habilitar desde Manager Service. Si el nombre de usuario con el que se ejecutará Manager Service es el propietario de la base de datos, no es necesario llevar a cabo ninguna acción. Si el usuario no es el propietario de la base de datos, el administrador del sistema debe conceder el acceso.

Prerequisitos

- [“Elegir un escenario de base de datos de IaaS,”](#) página 76.
- Compruebe que el nombre de usuario con el que se ejecutará Manager Service no es el propietario de la base de datos.

Procedimiento

- 1 Vaya al subdirectorio `Database` que se encuentra dentro del directorio en el que extrajo el archivo ZIP de instalación.
- 2 Descomprima el archivo `DBInstall.zip` en un directorio local.
- 3 Inicie sesión en el host de base de datos como un usuario con la función **sysadmin** en la instancia de SQL Server.
- 4 Edite `VMPSOpsUser.sql` y sustituya todas las instancias de `$(Service User)` por el usuario (del Paso 3) con el que se ejecutará Manager Service.
No sustituya `ServiceUser` en la línea que acaba por `WHERE name = N'ServiceUser'`.
- 5 Abra SQL Server Management Studio.
- 6 Seleccione la base de datos (vCAC de forma predeterminada) en **Bases de datos** en el panel de la izquierda.
- 7 Haga clic en **Nueva consulta**.
Se abrirá la ventana Consulta SQL en el panel de la derecha.
- 8 Pegue el contenido modificado de `VMPSOpsUser.sql` en el panel de consulta.
- 9 Haga clic en **Ejecutar**.

El acceso a la base de datos se ha habilitado desde Manager Service.

Configurar la cuenta de servicios de Windows para usar autenticación de SQL

De forma predeterminada, la cuenta de servicios de Windows accede a la base de datos en tiempo de ejecución, incluso si la base de datos se creó con autenticación de SQL. Un administrador del sistema puede cambiar el método de autenticación en tiempo de ejecución de Windows a SQL, por ejemplo, si la base de datos está en un dominio que no es de confianza.

Prerequisitos

[“Elegir un escenario de base de datos de IaaS,”](#) página 76.

Procedimiento

- 1 Inicie sesión en el host de Manager Service como usuario local con privilegios de **administrador**.
- 2 Detenga el servicio de vCloud Automation Center.
- 3 Vaya al directorio Server.
`C:\Archivos de programa (x86) \VMware\VCAC\Server\`
- 4 Abra el archivo `ManagerService.exe.config` en un editor de texto.
- 5 En la sección `connectionStrings` y en la sección `serviceConfiguration serviceURI`, sustituya **Integrated Security=True** por **User Id=DATABASE_USER;Password=DATABASE_PASSWORD**.
- 6 Guarde y cierre el archivo.
- 7 Vaya a `C:\Archivos de programa (x86)\VMware\VCAC\Server\Model Manager Web\`.
- 8 Abra el archivo `Web.config` en un editor de texto.
- 9 Busque la sección `repository server`.
`<repository server="localhost" database="VCAC" store="https://vcac.example.com/" />`
- 10 Añada el comando de usuario de base de datos.
user=DATABASE_USER password=DATABASE_PASSWORD. Por ejemplo:
`<repository server="localhost" database="VCAC" user="sqlUser" password="sqlPassword" store="https://vcac.example.com/" />`
- 11 Guarde y cierre el archivo.
- 12 Inicie el servicio de vCloud Automation Center.

La autenticación de SQL Server ya puede usarse en tiempo de ejecución.

Qué hacer a continuación

Reinicie Internet Information Services.

Comprobar los servicios de IaaS

Tras la instalación, el administrador del sistema comprueba que los servicios de IaaS se estén ejecutando. La ejecución de los servicios indica que la instalación se ha realizado correctamente.

Procedimiento

- 1 En el escritorio de Windows de la máquina de IaaS, seleccione **Herramientas administrativas > Servicios**.
- 2 Busque los siguientes servicios y compruebe que su estado sea **Iniciado** y que Tipo de inicio esté establecido en **Automático**.
 - VMware DEM – Orchestrator – *Nombre* donde *Name* es la cadena proporcionada en el cuadro **Nombre de DEM** durante la instalación.
 - VMware DEM – Trabajo – *Nombre* donde *Name* es la cadena proporcionada en el cuadro **Nombre de DEM** durante la instalación.
 - VMware vCloud Automation Center Agent *Nombre de agente*
 - VMware vCloud Automation Center Service
- 3 Cierre la ventana **Servicios**.

Instalación de agentes

vRealize Automation utiliza agentes para la integración con sistemas externos. Un administrador del sistema puede seleccionar los agentes que se van a instalar para que se comuniquen con otras plataformas de virtualización.

vRealize Automation utiliza los siguientes tipos de agentes para administrar sistemas externos:

- Agentes de proxy de hipervisor (vSphere, servidores de Citrix Xen y servidores de Microsoft Hyper-V)
- Agentes de integración de infraestructura de aprovisionamiento externo (EPI)
- Agentes de infraestructura de escritorio virtual (VDI)
- Agentes de Instrumental de administración de Windows (WMI)

Para ofrecer alta disponibilidad, se pueden instalar varios agentes para un solo endpoint. Instale cada agente redundante en un servidor distinto, pero asígneles el mismo nombre y configúrelos exactamente igual. Los agentes redundantes proporcionan cierta capacidad de tolerancia a fallos, pero no conmutación por error. Así, por ejemplo, si instala dos agentes de vSphere (uno en el servidor A y otro en el servidor B) y el servidor A deja de estar disponible, el agente instalado en el servidor B continuará procesando los elementos de trabajo, pero no podrá finalizar el procesamiento del elemento de trabajo que el agente del servidor A inició.

Puede optar por instalar un agente de vSphere como parte de la instalación mínima, pero después de la instalación también podrá añadir más agentes, incluido un agente de vSphere extra. En una implementación distribuida, todos los agentes se instalan después de finalizar la instalación distribuida base. Los agentes que se instalen dependerán de los recursos de la infraestructura.

Para obtener información sobre cómo usar los agentes de vSphere, consulte [“Requisitos del agente de vSphere,”](#) página 99.

Establecer la política de ejecución de PowerShell en RemoteSigned

Debe establecer la política de ejecución de PowerShell de Restricted a RemoteSigned o Unrestricted para permitir la ejecución de scripts de PowerShell locales.

Prerequisitos

- Inicie sesión como administrador de Windows.
- Antes de instalar el agente, confirme que Microsoft PowerShell está instalado en el host de instalación. La versión que sea necesaria dependerá del sistema operativo del host de instalación. Consulte la ayuda y soporte técnico de Microsoft.
- Para obtener más información sobre la política de ejecución de PowerShell, ejecute `help about_signing` o `help Set-ExecutionPolicy` en un símbolo del sistema de PowerShell.

Procedimiento

- 1 Seleccione **Inicio > Todos los programas > Versión de Windows PowerShell > Windows PowerShell**.
- 2 Para RemoteSigned, ejecute `Set-ExecutionPolicy RemoteSigned`.
- 3 Para Unrestricted, ejecute `Set-ExecutionPolicy Unrestricted`.
- 4 Compruebe que el comando no produce ningún error.
- 5 Escriba **Exit** en el símbolo del sistema de PowerShell.

Elegir un escenario de instalación de agentes

Los agentes que es necesario instalar dependen de los sistemas externos en los que tenga previsto integrarse.

Tabla 4-16. Elegir un escenario de agentes

Escenario de integración	Procedimientos y requisitos de agente
Aprovisionar máquinas en la nube integrándose en un entorno de nube como Amazon Web Services o Red Hat Enterprise Linux OpenStack Platform.	No hay que instalar ningún agente.
Aprovisionar máquinas virtuales integrándose con un entorno de vSphere.	“Instalar y configurar el agente de proxy de vSphere,” página 98
Aprovisionar máquinas virtuales integrándose con un entorno de Microsoft Hyper-V Server.	“Instalar el agente de proxy de Hyper-V o XenServer,” página 103
Aprovisionar máquinas virtuales integrándose con un entorno de XenServer.	<ul style="list-style-type: none"> ■ “Instalar el agente de proxy de Hyper-V o XenServer,” página 103 ■ “Instalar el agente de EPI de Citrix,” página 111
Aprovisionar máquinas virtuales integrándose con un entorno de XenDesktop.	<ul style="list-style-type: none"> ■ “Instalar el agente de VDI de XenDesktop,” página 107 ■ “Instalar el agente de EPI de Citrix,” página 111
Ejecutar scripts de Visual Basic como un paso extra dentro del proceso de aprovisionamiento antes o después de aprovisionar una máquina, o bien al desaprovisionarla.	“Instalar el agente de EPI de Visual Basic Scripting,” página 114
Recopilar datos de las máquinas de Windows aprovisionadas, por ejemplo, el estado de Active Directory del propietario de una máquina.	“Instalar el agente de WMI para solicitudes de WMI remotas,” página 117
Aprovisionar máquinas virtuales integrándose con otra plataforma virtual compatible.	No hay que instalar ningún agente.

Ubicación y requisitos de instalación de agentes

Los administradores del sistema suelen instalar los agentes en el servidor de vRealize Automation que aloja el componente de Manager Service activo.

Si se instala un agente en otro host, la configuración de red debe permitir la comunicación entre el agente y la máquina donde esté instalado Manager Service.

Cada agente se instala con un nombre único en su propio directorio, *Agents\agentname*, en el directorio de instalación de vRealize Automation (normalmente *Archivos de programa(x86)\VMware\VCAC*), y su configuración se almacena en el archivo *VRMAgent.exe.config* de dicho directorio.

Instalar y configurar el agente de proxy de vSphere

Un administrador del sistema instala agentes de proxy para que se comuniquen con las instancias de servidor de vSphere. Los agentes detectan el trabajo disponible, recuperan información sobre el host e informan de los elementos de trabajo completados y de otros cambios de estado del host.

Requisitos del agente de vSphere

Las credenciales de endpoint de vSphere, o las credenciales con las que se ejecuta el servicio de agente, deben tener acceso administrativo al host de instalación. Varios agentes de vSphere deben cumplir los requisitos de configuración de vRealize Automation.

Credenciales

Cuando se crea un endpoint que representa la instancia de vCenter Server que debe administrarse mediante un agente de vSphere, el agente puede usar las credenciales con las que se ejecuta el servicio para interactuar con vCenter Server o especificar credenciales de endpoint independientes.

En esta tabla se muestran los permisos detallados que deben tener las credenciales de endpoint de vSphere para administrar una instancia de vCenter Server.

Tabla 4-17. Permisos necesarios para que el agente de vSphere administre una instancia de vCenter Server

Valor de atributo	Permiso	
Almacén de datos	Asignar espacio	
	Examinar almacén de datos	
Carpeta	Crear carpeta	
	Eliminar carpeta	
Global	Administrar atributos personalizados	
	Establecer atributo personalizado	
Red	Asignar red	
Permisos	Modificar permiso	
Recurso	Asignar máquina virtual a grupo de recursos	
	Migrar máquina virtual apagada	
	Migrar máquina virtual encendida	
Máquina virtual	Inventario	Crear a partir de existente
		Crear nueva
		Migrar máquina virtual encendida
	Interacción	Mover
		Quitar
		Configurar CD
		Interacción de consola
		Conexión de dispositivos
		Apagar
		Encender
		Restablecer
		Suspender
		Instalación de herramientas
Configuración	Añadir disco existente	
	Añadir disco nuevo	
	Añadir o quitar	

Tabla 4-17. Permisos necesarios para que el agente de vSphere administre una instancia de vCenter Server (Continúa)

Valor de atributo	Permiso
	Quitar disco
	Avanzado
	Cambiar recuento de CPU
	Cambiar recurso
	Configuración de disco virtual de ampliación de dispositivo
	Seguimiento de cambios de disco
	Memoria
	Modificar configuración de dispositivo
	Cambiar nombre
	Establecer anotación (versión 5.0 y posterior)
	Configuración
	Colocación de archivo de intercambio
Aprovisionar	Personalizar
	Clonar plantilla
	Clonar máquina virtual
	Implementar plantilla
	Leer especificaciones de personalización
Estado	Crear snapshot
	Quitar snapshot
	Restaurar el snapshot

Deshabilite o vuelva a configurar el software de terceros que pueda cambiar el estado de energía de las máquinas virtuales fuera de vRealize Automation. Dichos cambios pueden interferir en la administración del ciclo de vida de la máquina por parte de vRealize Automation.

Instalar el agente de vSphere

Instale un agente de vSphere para administrar las instancias de vCenter Server. Para ofrecer alta disponibilidad, puede instalar un segundo agente redundante de vSphere para la misma instancia de vCenter Server. Ambos agentes de vSphere deben tener exactamente el mismo nombre y la misma configuración, pero estar instalados en máquinas distintas.

Prerequisitos

- Los componentes de IaaS (Manager Service y sitio web incluidos) están instalados.
- Confirme que ha completado todos los [“Requisitos del agente de vSphere,”](#) página 99.
- Si ya ha creado un endpoint de vSphere para utilizarlo con este agente, anote el nombre del endpoint.
- [“Descargar el instalador de IaaS,”](#) página 75.

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 2 Haga clic en **Siguiente**.
- 3 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 4 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 5 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 6 Seleccione **Selección de componentes** en la página Tipo de instalación.
- 7 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 8 Haga clic en **Siguiente**.
- 9 Inicie sesión con los privilegios de **administrador** de los servicios de Windows en la máquina de instalación.
El servicio debe ejecutarse en la misma máquina de instalación.
- 10 Haga clic en **Siguiente**.
- 11 Seleccione vSphere de la lista **Tipo de agente**.
- 12 Escriba un identificador de este agente en el cuadro de texto **Nombre de agente**.
Mantenga un registro del nombre de agente, las credenciales, el nombre de endpoint y la instancia de plataforma de cada agente. Esta información es necesaria para configurar endpoints y para añadir hosts más adelante.

IMPORTANTE: No duplique nombres de agente a menos que instale agentes redundantes configurados de forma idéntica para disponer de alta disponibilidad.

Opción	Descripción
Instalación de agentes redundantes	Instale agentes redundantes en servidores distintos, pero asígneles el mismo nombre y configúrelos exactamente igual para proporcionar alta disponibilidad.
Instalación de un solo agente	Seleccione un nombre único para este agente.

- Configure una conexión con el componente Manager Service.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service. Por ejemplo, manager-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service. Por ejemplo, manager_service.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- Configure una conexión con el componente Manager Website.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Website. Por ejemplo, website-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Website. Por ejemplo, website_component.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- Haga clic en **Probar** para comprobar la conectividad con cada host.

- Escriba el nombre del endpoint.

El nombre de endpoint que configure en vRealize Automation debe coincidir con el que se proporcionó al agente de proxy de vSphere durante la instalación o, de lo contrario, el endpoint no funcionará.

- Haga clic en **Agregar**.

- Haga clic en **Siguiente**.

- Haga clic en **Instalar** para comenzar la instalación.

Transcurridos unos minutos, se mostrará un mensaje de operación correcta.

- Haga clic en **Siguiente**.

- Haga clic en **Finalizar**.

- Confirme que la instalación se ha realizado correctamente.

- (Opcional) Añada varios agentes con configuraciones diferentes y un endpoint en el mismo sistema.

Qué hacer a continuación

[“Configurar el agente de vSphere,”](#) página 102.

Configurar el agente de vSphere

Se puede usar la utilidad de agente de proxy para modificar las configuraciones iniciales cifradas en el archivo de configuración del agente o para cambiar la política de eliminación de máquinas en las plataformas de virtualización.

Prerequisitos

Inicie sesión como **administrador del sistema** en la máquina en la que está instalado el agente.

Procedimiento

- 1 Abra una consola de comandos de Windows como administrador.
- 2 Vaya al directorio de instalación de agentes.
Por ejemplo, `cd Program Files (x86)\VMware\VCAC\CD Agents\agent_name.`
- 3 (Opcional) Escriba `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get` para ver la configuración actual.

Este es un ejemplo de resultado del comando:

```
managementEndpointName: VCEndpoint doDeletes: True
```

- 4 (Opcional) Introduzca el comando `set managementEndpointName` para cambiar el nombre del endpoint genérico que configuró durante la instalación.

Por ejemplo, `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName MyEndpoint.`

Cambia esta propiedad para cambiar el nombre del endpoint genérico en vRealize Automation en lugar de cambiar los endpoints.

- 5 (Opcional) Introduzca el comando `set doDeletes` para configurar la política de eliminación de máquinas virtuales.

Por ejemplo, `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes false.`

Opción	Descripción
true	(Predeterminado) Elimine de vCenter Server las máquinas virtuales destruidas en vRealize Automation.
false	Mueva las máquinas virtuales destruidas en vRealize Automation al directorio VRMDelated de vCenter Server.

- 6 Vaya a **Inicio > Herramientas administrativas > Servicios** y reinicie el servicio Agente de vRealize Automation – *agentname*.

Qué hacer a continuación

Para ofrecer alta disponibilidad, puede instalar y configurar un agente redundante para su endpoint. Instale cada agente redundante en un servidor distinto, pero asígñeles el mismo nombre y configúrelos exactamente igual.

Instalar el agente de proxy de Hyper-V o XenServer

Un administrador del sistema instala agentes de proxy para que se comuniquen con las instancias de servidor de Hyper-V y XenServer. Los agentes detectan el trabajo disponible, recuperan información sobre el host e informan de los elementos de trabajo completados y de otros cambios de estado del host.

Requisitos de Hyper-V y XenServer

Los agentes de proxy de hipervisor de Hyper-V requieren credenciales de administrador en la instalación.

Las credenciales con las que hay que ejecutar el servicio de agente deben tener acceso administrativo al host de instalación.

Se necesitan credenciales de nivel de administrador en todas las instancias de XenServer o Hyper-V en los hosts que el agente vaya a administrar.

Si usa grupos de Xen, todos los nodos dentro de ese grupo de Xen deben poder identificarse por sus nombres de dominio completo.

NOTA: Hyper-V no está configurado de forma predeterminada para la administración remota. Un agente de proxy de Hyper-V en vRealize Automation no se puede comunicar con un servidor de Hyper-V a menos que la administración remota esté habilitada.

Consulte la documentación de Microsoft Windows Server para obtener más información sobre cómo configurar Hyper-V para la administración remota.

Instalar el agente de Hyper-V o XenServer

El agente de Hyper-V administra las instancias de servidor de Hyper-V, mientras que el agente de XenServer hace lo propio con las instancias de servidor de XenServer.

Prerequisitos

- Los componentes de IaaS (Manager Service y sitio web incluidos) están instalados.
- [“Descargar el instalador de IaaS,”](#) página 75.
- Compruebe que los agentes de proxy de hipervisor de Hyper-V tienen credenciales de administrador del sistema.
- Compruebe que las credenciales con las que hay que ejecutar el servicio de agente tienen acceso administrativo al host de instalación.
- Compruebe que todas las instancias de XenServer o Hyper-V en los hosts que el agente va a administrar tienen credenciales de nivel de administrador.
- Si usa grupos de Xen, tenga en cuenta que todos los nodos dentro de ese grupo de Xen deben poder identificarse por sus nombres de dominio completo.

vRealize Automation no se puede comunicar con un nodo (ni tampoco administrarlo) que no se pueda identificar por su nombre de dominio completo en el grupo de Xen.

- Configure Hyper-V para la administración remota a fin de permitir la comunicación de servidor de Hyper-V con los agentes de proxy de Hyper-V de vRealize Automation.

Consulte la documentación de Microsoft Windows Server para obtener más información sobre cómo configurar Hyper-V para la administración remota.

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 2 Haga clic en **Siguiente**.
- 3 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 4 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.

Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.

- 5 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 6 Seleccione **Selección de componentes** en la página Tipo de instalación.
- 7 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 8 Haga clic en **Siguiente**.
- 9 Inicie sesión con los privilegios de **administrador** de los servicios de Windows en la máquina de instalación.

El servicio debe ejecutarse en la misma máquina de instalación.

- 10 Haga clic en **Siguiente**.
- 11 Seleccione el agente de la lista **Tipo de agente**.
 - Xen
 - Hyper-V
- 12 Escriba un identificador de este agente en el cuadro de texto **Nombre de agente**.

Mantenga un registro del nombre de agente, las credenciales, el nombre de endpoint y la instancia de plataforma de cada agente. Esta información es necesaria para configurar endpoints y para añadir hosts más adelante.

IMPORTANTE: No duplique nombres de agente a menos que instale agentes redundantes configurados de forma idéntica para disponer de alta disponibilidad.

Opción	Descripción
Instalación de agentes redundantes	Instale agentes redundantes en servidores distintos, pero asígneles el mismo nombre y configúrelos exactamente igual para proporcionar alta disponibilidad.
Instalación de un solo agente	Seleccione un nombre único para este agente.

- 13 Indique el **Nombre de agente** al administrador de IaaS que configure los endpoints.
Para permitir el acceso y la recopilación de datos, el endpoint debe estar vinculado al agente que lo haya configurado.
- 14 Configure una conexión con el componente Manager Service.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service. Por ejemplo, manager-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service. Por ejemplo, manager_service.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- 15 Configure una conexión con el componente Manager Website.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Website. Por ejemplo, website-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Website. Por ejemplo, website_component.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- 16 Haga clic en **Probar** para comprobar la conectividad con cada host.
- 17 Escriba las credenciales de un usuario con permisos de nivel administrativo en la instancia del servidor administrado.
- 18 Haga clic en **Agregar**.
- 19 Haga clic en **Siguiente**.
- 20 (Opcional) Añada otro agente.
Por ejemplo, puede añadir un agente de XEN si antes ha añadido uno de Hyper-V.
- 21 Haga clic en **Instalar** para comenzar la instalación.
Transcurridos unos minutos, se mostrará un mensaje de operación correcta.
- 22 Haga clic en **Siguiente**.
- 23 Haga clic en **Finalizar**.
- 24 Confirme que la instalación se ha realizado correctamente.

Qué hacer a continuación

Para ofrecer alta disponibilidad, puede instalar y configurar un agente redundante para su endpoint. Instale cada agente redundante en un servidor distinto, pero asígñeles el mismo nombre y configúrelos exactamente igual.

[“Configurar el agente de Hyper-V o XenServer,”](#) página 106.

Configurar el agente de Hyper-V o XenServer

Un administrador del sistema puede modificar los valores de configuración de los agentes de proxy, por ejemplo, la política de eliminación de las plataformas de virtualización. Se puede usar la utilidad de agente de proxy para cambiar las configuraciones iniciales cifradas en el archivo de configuración del agente.

Prerequisitos

Inicie sesión como **administrador del sistema** en la máquina en la que está instalado el agente.

Procedimiento

- 1 Vaya al directorio de instalación de agentes, donde *agent_name* es el directorio que contiene el agente de proxy, que es asimismo el nombre por el cual el agente está instalado.

```
cd Program Files (x86)\VMware\VCAC Agents\agent_name
```

- 2 Consulte los valores de configuración actuales.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

Este es un ejemplo de resultado del comando:

```
Username: XSadmin
```

- 3 Escriba el comando set para cambiar una propiedad, donde *property* es una de las opciones recogidas en la tabla.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set property value
```

Si omite el *value*, la utilidad le pedirá que especifique un valor nuevo.

Propiedad	Descripción
username	Nombre de usuario que representa las credenciales de nivel de administrador del servidor de XenServer o de Hyper-V con el que el agente se comunica.
password	Contraseña del nombre de usuario de nivel de administrador.

- 4 Haga clic en **Inicio > Herramientas administrativas > Servicios** y reinicie el servicio Agente de vRealize Automation – *agentname*.

Ejemplo: cambiar las credenciales de nivel de administrador

Escriba el siguiente comando para cambiar las credenciales de nivel de administrador de la plataforma de virtualización especificada durante la instalación del agente.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith
```

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password
```

Qué hacer a continuación

Para ofrecer alta disponibilidad, puede instalar y configurar un agente redundante para su endpoint. Instale cada agente redundante en un servidor distinto, pero asígneles el mismo nombre y configúrelos exactamente igual.

Instalar el agente de VDI de XenDesktop

vRealize Automation emplea agentes de PowerShell de integración de escritorio virtual (VDI) para registrar las máquinas de XenDesktop que aprovisiona con sistemas de administración de escritorio externos.

El agente de integración de VDI provee a los propietarios de máquinas registradas de una conexión directa con la Interfaz Web de XenDesktop. Puede instalar un agente de VDI como un agente dedicado que interactúe con un único Desktop Delivery Controller (DDC), o bien como un agente general que interactúe con varios DDC.

Requisitos de XenDesktop

Un administrador del sistema instala un agente de infraestructura de escritorio virtual (VDI) para integrar servidores de XenDesktop en vRealize Automation.

Puede instalar un agente de VDI para interactuar con varios servidores. Si instala un agente dedicado en cada servidor por razones de equilibrio de carga o autorización, debe proporcionar el nombre del servidor DDC de XenDesktop cuando instale el agente. Un agente dedicado solo puede controlar las solicitudes de registro dirigidas al servidor especificado en su configuración.

Consulte *Matriz de soporte de vRealize Automation* en el sitio web de VMware para obtener información sobre las versiones de XenDesktop compatibles con servidores DDC de XenDesktop.

Host de instalación y credenciales

Las credenciales con las que se ejecuta el agente deben tener acceso administrativo a todos los servidores DDC de XenDesktop con los que interactúa.

Requisitos de XenDesktop

El nombre asignado al host de XenServer en el servidor de XenDesktop debe coincidir con el UUID del grupo de Xen en XenCenter. Consulte [“Definir el nombre de host de XenServer,”](#) página 108 para obtener más información.

Todos los servidores DDC de XenDesktop con los que tenga previsto registrar máquinas deben estar configurados del siguiente modo:

- El tipo de grupo/catálogo debe estar establecido en **Existente** para poder utilizarse con vRealize Automation.
- El nombre de un host de vCenter Server en un servidor de DDC debe coincidir con el nombre de la instancia de vCenter Server tal y como se especifica en el endpoint de vSphere de vRealize Automation, pero sin el dominio. El endpoint debe estar configurado con un nombre de dominio completo (FQDN) y no con una dirección IP. Por ejemplo, si la dirección en el endpoint es `https://virtual-center27.domain/sdk`, el nombre del host en el servidor DDC debe establecerse en `virtual-center27`.

Si su endpoint de vSphere de vRealize Automation se ha configurado con una dirección IP, debe cambiarlo para que use un nombre de dominio completo. Consulte *Configuración de IaaS* para obtener más información sobre la configuración de endpoints.

Requisitos del host del agente de XenDesktop

Debe instalarse el SDK de Citrix XenDesktop. El SDK para XenDesktop se incluye en el disco de instalación de XenDesktop.

Antes de instalar el agente, confirme que Microsoft PowerShell está instalado en el host de instalación. La versión que sea necesaria dependerá del sistema operativo del host de instalación. Consulte la ayuda y soporte técnico de Microsoft.

La política de ejecución de MS PowerShell está establecida en RemoteSigned o en Unrestricted. Consulte [“Establecer la política de ejecución de PowerShell en RemoteSigned,”](#) página 97.

Para obtener más información sobre la política de ejecución de PowerShell, ejecute `help about_signing` o `help Set-ExecutionPolicy` en un símbolo del sistema de PowerShell.

Definir el nombre de host de XenServer

En XenDesktop, el nombre asignado al host de XenServer en el servidor de XenDesktop debe coincidir con el UUID del grupo de Xen en XenCenter. Si no se configura XenPool, el nombre debe coincidir con el UUID del propio XenServer.

Procedimiento

- 1 En Citrix XenCenter, seleccione su XenPool o XenServer independiente y haga clic en la pestaña **General**. Registre el UUID.
- 2 Cuando añada el grupo de XenServer o host independiente a XenDesktop, escriba el UUID que se registró en el paso anterior como el nombre de **Conexión**.

Instalar el agente de XenDesktop

Los agentes de PowerShell de integración de escritorio virtual (VDI) se integran con sistemas de escritorio virtual externos como XenDesktop y Citrix. Utilice un agente de PowerShell de VDI para administrar la máquina de XenDesktop.

Prerequisitos

- Los componentes de IaaS (Manager Service y sitio web incluidos) están instalados.
- Compruebe que el entorno reúne los [“Requisitos de XenDesktop,”](#) página 107.
- [“Descargar el instalador de IaaS,”](#) página 75.

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 2 Haga clic en **Siguiente**.
- 3 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 4 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 5 Haga clic en **Siguiente**.
- 6 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 7 Seleccione **Agentes de proxy** en el panel Selección de componentes.
- 8 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 9 Haga clic en **Siguiente**.
- 10 Inicie sesión con los privilegios de **administrador** de los servicios de Windows en la máquina de instalación.
El servicio debe ejecutarse en la misma máquina de instalación.
- 11 Haga clic en **Siguiente**.
- 12 Seleccione **VdiPowerShell** en el menú desplegable **Tipo de agente**.

- 13 Escriba un identificador de este agente en el cuadro de texto **Nombre de agente**.

Mantenga un registro del nombre de agente, las credenciales, el nombre de endpoint y la instancia de plataforma de cada agente. Esta información es necesaria para configurar endpoints y para añadir hosts más adelante.

IMPORTANTE: No duplique nombres de agente a menos que instale agentes redundantes configurados de forma idéntica para disponer de alta disponibilidad.

Opción	Descripción
Instalación de agentes redundantes	Instale agentes redundantes en servidores distintos, pero asígneles el mismo nombre y configúrelos exactamente igual para proporcionar alta disponibilidad.
Instalación de un solo agente	Seleccione un nombre único para este agente.

- 14 Configure una conexión con el componente Manager Service.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service. Por ejemplo, manager-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service. Por ejemplo, manager_service.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- 15 Configure una conexión con el componente Manager Website.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Website. Por ejemplo, website-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Website. Por ejemplo, website_component.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- 16 Haga clic en **Probar** para comprobar la conectividad con cada host.
- 17 Seleccione la **Versión de VDI**.
- 18 Escriba el nombre de dominio completo del servidor administrado en el cuadro de texto **Servidor de VDI**.
- 19 Haga clic en **Agregar**.
- 20 Haga clic en **Siguiente**.
- 21 Haga clic en **Instalar** para comenzar la instalación.
- Transcurridos unos minutos, se mostrará un mensaje de operación correcta.
- 22 Haga clic en **Siguiente**.
- 23 Haga clic en **Finalizar**.

- 24 Confirme que la instalación se ha realizado correctamente.
- 25 (Opcional) Añada varios agentes con configuraciones diferentes y un endpoint en el mismo sistema.

Qué hacer a continuación

Para ofrecer alta disponibilidad, puede instalar y configurar un agente redundante para su endpoint. Instale cada agente redundante en un servidor distinto, pero asígneles el mismo nombre y configúrelos exactamente igual.

Instalar el agente de EPI de Citrix

Los agentes de PowerShell de integración de aprovisionamiento externo (EPI) integran máquinas externas de Citrix en el proceso de aprovisionamiento. El agente de EPI proporciona transmisión mediante secuencias a petición de las imágenes de disco de Citrix desde las que las máquinas se inician y ejecutan.

El agente de EPI dedicado interactúa con un solo servidor de aprovisionamiento externo. Por lo tanto, debe instalar un agente de EPI por cada instancia de servidor de aprovisionamiento de Citrix existente.

Servidor de aprovisionamiento de Citrix

Un administrador del sistema usa agentes de EPI (infraestructura de aprovisionamiento externa) para integrar servidores de aprovisionamiento de Citrix y permitir el uso de scripts de Visual Basic durante el aprovisionamiento.

Credenciales y ubicación de la instalación

Instale el agente en el host de PVS de las instancias de los servicios de aprovisionamiento de Citrix. Confirme que el host de instalación reúne los [“Requisitos de host del agente de Citrix,”](#) página 111 antes de instalar el agente.

Los agentes de EPI suelen interactuar con varios servidores, pero el servidor de aprovisionamiento de Citrix requiere un agente de EPI dedicado. Por lo tanto, debe instalar un agente de EPI por cada instancia de servidor de aprovisionamiento de Citrix existente, así como indicar el nombre del servidor donde se aloja. Las credenciales con las que el agente se ejecuta deben tener acceso administrativo a la instancia del servidor de aprovisionamiento de Citrix.

Consulte la *Matriz de soporte de vRealize Automation* para obtener más información sobre las versiones compatibles de PVS de Citrix.

Requisitos de host del agente de Citrix

Para poder instalar un agente, el host de instalación debe tener instalados PowerShell y el SDK de los servicios de aprovisionamiento de Citrix. Consulte la *Matriz de soporte de vRealize Automation* en el sitio web de VMware para obtener información detallada.

Antes de instalar el agente, confirme que Microsoft PowerShell está instalado en el host de instalación. La versión que sea necesaria dependerá del sistema operativo del host de instalación. Consulte la ayuda y soporte técnico de Microsoft.

Debe procurar que esté instalado también el complemento de PowerShell. Para obtener más información, consulte la *guía para programadores de PowerShell de los servicios de aprovisionamiento de Citrix* en el sitio web de Citrix.

La política de ejecución de MS PowerShell está establecida en RemoteSigned o en Unrestricted. Consulte [“Establecer la política de ejecución de PowerShell en RemoteSigned,”](#) página 97.

Para obtener más información sobre la política de ejecución de PowerShell, ejecute `help about_signing` o `help Set-ExecutionPolicy` en un símbolo del sistema de PowerShell.

Instalar el agente de Citrix

Los agentes de PowerShell de integración de aprovisionamiento externo (EPI) integran sistemas externos en el proceso de aprovisionamiento de máquinas. Utilice el agente de PowerShell de EPI para integrarse con el servidor de aprovisionamiento de Citrix con objeto de permitir el aprovisionamiento de máquinas mediante secuencia de discos a petición.

Prerequisitos

- Los componentes de IaaS (Manager Service y sitio web incluidos) están instalados.
- Confirme que reúne todos los [“Servidor de aprovisionamiento de Citrix,”](#) página 111.
- [“Descargar el instalador de IaaS,”](#) página 75.

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 2 Haga clic en **Siguiente**.
- 3 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 4 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 5 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 6 Seleccione **Selección de componentes** en la página Tipo de instalación.
- 7 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 8 Haga clic en **Siguiente**.
- 9 Inicie sesión con los privilegios de **administrador** de los servicios de Windows en la máquina de instalación.
El servicio debe ejecutarse en la misma máquina de instalación.
- 10 Haga clic en **Siguiente**.
- 11 Seleccione **EPIPowerShell** en el menú desplegable Tipo de agente.

- 12 Escriba un identificador de este agente en el cuadro de texto **Nombre de agente**.

Mantenga un registro del nombre de agente, las credenciales, el nombre de endpoint y la instancia de plataforma de cada agente. Esta información es necesaria para configurar endpoints y para añadir hosts más adelante.

IMPORTANTE: No duplique nombres de agente a menos que instale agentes redundantes configurados de forma idéntica para disponer de alta disponibilidad.

Opción	Descripción
Instalación de agentes redundantes	Instale agentes redundantes en servidores distintos, pero asígneles el mismo nombre y configúrelos exactamente igual para proporcionar alta disponibilidad.
Instalación de un solo agente	Seleccione un nombre único para este agente.

- 13 Configure una conexión con el componente Manager Service.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service. Por ejemplo, manager-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service. Por ejemplo, manager_service.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- 14 Configure una conexión con el componente Manager Website.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Website. Por ejemplo, website-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Website. Por ejemplo, website_component.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- 15 Haga clic en **Probar** para comprobar la conectividad con cada host.
- 16 Seleccione el tipo de EPI.
- 17 Escriba el nombre de dominio completo del servidor administrado en el cuadro de texto **Servidor de EPI**.
- 18 Haga clic en **Agregar**.
- 19 Haga clic en **Siguiente**.
- 20 Haga clic en **Instalar** para comenzar la instalación.
- Transcurridos unos minutos, se mostrará un mensaje de operación correcta.
- 21 Haga clic en **Siguiente**.
- 22 Haga clic en **Finalizar**.

- 23 Confirme que la instalación se ha realizado correctamente.
- 24 (Opcional) Añada varios agentes con configuraciones diferentes y un endpoint en el mismo sistema.

Qué hacer a continuación

Para ofrecer alta disponibilidad, puede instalar y configurar un agente redundante para su endpoint. Instale cada agente redundante en un servidor distinto, pero asígneles el mismo nombre y configúrelos exactamente igual.

Instalar el agente de EPI de Visual Basic Scripting

Un administrador del sistema puede especificar scripts de Visual Basic como pasos extra dentro del proceso de aprovisionamiento antes o después de aprovisionar una máquina, o bien al desaproveionarla. Para poder ejecutar scripts de Visual Basic es necesario instalar un agente de PowerShell de integración de aprovisionamiento externo (EPI).

Los scripts de Visual Basic se especifican en el blueprint desde el que se aprovisionan las máquinas. Estos scripts tienen acceso a todas las propiedades personalizadas asociadas a la máquina y pueden actualizar sus valores. Así, el siguiente paso en el flujo de trabajo tendrá acceso a estos nuevos valores.

Por ejemplo, podría usar un script para generar certificados o tokens de seguridad antes de realizar el aprovisionamiento y usar esos certificados y tokens en el aprovisionamiento de máquinas.

Para permitir el uso de scripts en el aprovisionamiento, debe instalar un tipo específico de agente de EPI y colocar los scripts que quiera usar en el sistema en el que el agente esté instalado.

Cuando se ejecuta un script, el agente de EPI pasa todas las propiedades personalizadas de máquina como argumentos a ese script. Para devolver las propiedades personalizadas actualizadas, debe colocar esas propiedades en un diccionario y llamar a una función de vRealize Automation. En el subdirectorio de scripts del directorio de instalación del agente de EPI encontrará un script de ejemplo. Este script contiene un encabezado para cargar todos los argumentos en un diccionario, un cuerpo en el que se pueden incluir funciones y un pie de página para devolver las propiedades personalizadas actualizadas.

NOTA: Se pueden instalar varios agentes de EPI/VBScripts en distintos servidores y realizar el aprovisionamiento usando un agente concreto y los scripts de Visual Basic que hay en el host de dicho agente. Póngase en contacto con el equipo de atención al cliente de VMware si necesita llevar esto a cabo.

Requisitos de Visual Basic Scripting

Un administrador del sistema instala agentes de EPI (infraestructura de aprovisionamiento externo) para permitir el uso de scripts de Visual Basic en el proceso de aprovisionamiento.

En la siguiente tabla se describen los requisitos aplicables para instalar un agente de EPI para permitir el uso de scripts de Visual Basic en el proceso de aprovisionamiento.

Tabla 4-18. Agentes de EPI para la creación de scripts de Visual Basic

Requisito	Descripción
Credenciales	Las credenciales con las que se ejecuta el agente deben tener acceso administrativo en el host de instalación.
Microsoft PowerShell	Microsoft PowerShell debe estar instalado en el host de instalación antes de instalar el agente. La versión necesaria dependerá del sistema operativo del host de instalación y podría estar instalada con dicho sistema operativo. Visite http://support.microsoft.com para obtener más información.
Política de ejecución de MS PowerShell	La política de ejecución de MS PowerShell debe estar establecida en RemoteSigned o Unrestricted . Para obtener más información sobre la política de ejecución de PowerShell, emita uno de los siguientes comandos en el símbolo del sistema de PowerShell: <pre>help about_signing help Set-ExecutionPolicy</pre>

Instalar el agente de Visual Basic Scripting

Los agentes de PowerShell de integración de aprovisionamiento externo (EPI) permiten integrar sistemas externos en el proceso de aprovisionamiento de máquinas. Utilice un agente de EPI para ejecutar scripts de Visual Basic a modo de pasos extra durante el proceso de aprovisionamiento.

Prerequisitos

- Los componentes de IaaS (Manager Service y sitio web incluidos) están instalados.
- Confirme que reúne todos los [“Requisitos de Visual Basic Scripting,”](#) página 114.
- [“Descargar el instalador de IaaS,”](#) página 75.

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 2 Haga clic en **Siguiente**.
- 3 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 4 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.

Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 5 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 6 Seleccione **Selección de componentes** en la página Tipo de instalación.
- 7 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 8 Haga clic en **Siguiente**.

- Inicie sesión con los privilegios de **administrador** de los servicios de Windows en la máquina de instalación.

El servicio debe ejecutarse en la misma máquina de instalación.

- Haga clic en **Siguiente**.
- Seleccione **EPIPowerShell** en el menú desplegable Tipo de agente.
- Escriba un identificador de este agente en el cuadro de texto **Nombre de agente**.

Mantenga un registro del nombre de agente, las credenciales, el nombre de endpoint y la instancia de plataforma de cada agente. Esta información es necesaria para configurar endpoints y para añadir hosts más adelante.

IMPORTANTE: No duplique nombres de agente a menos que instale agentes redundantes configurados de forma idéntica para disponer de alta disponibilidad.

Opción	Descripción
Instalación de agentes redundantes	Instale agentes redundantes en servidores distintos, pero asígneles el mismo nombre y configúrelos exactamente igual para proporcionar alta disponibilidad.
Instalación de un solo agente	Seleccione un nombre único para este agente.

- Configure una conexión con el componente Manager Service.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service. Por ejemplo, manager-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service. Por ejemplo, manager_service.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- Configure una conexión con el componente Manager Website.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Website. Por ejemplo, website-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Website. Por ejemplo, website_component.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- Haga clic en **Probar** para comprobar la conectividad con cada host.
- Seleccione el tipo de EPI.
- Escriba el nombre de dominio completo del servidor administrado en el cuadro de texto **Servidor de EPI**.
- Haga clic en **Agregar**.
- Haga clic en **Siguiente**.

- 20 Haga clic en **Instalar** para comenzar la instalación.
Transcurridos unos minutos, se mostrará un mensaje de operación correcta.
- 21 Haga clic en **Siguiente**.
- 22 Haga clic en **Finalizar**.
- 23 Confirme que la instalación se ha realizado correctamente.
- 24 (Opcional) Añada varios agentes con configuraciones diferentes y un endpoint en el mismo sistema.

Instalar el agente de WMI para solicitudes de WMI remotas

Un administrador del sistema habilita el protocolo de Instrumentación de administración de Windows (WMI) e instala el agente de WMI en todas las máquinas administradas de Windows para que sus datos y operaciones puedan administrarse. El agente es necesario para recopilar datos de las máquinas de Windows, por ejemplo, el estado de Active Directory del propietario de una máquina.

Habilitar solicitudes de WMI remotas en máquinas de Windows

Para utilizar agentes de WMI, las solicitudes de WMI remotas deben estar habilitadas en los servidores de Windows administrados.

Procedimiento

- 1 En cada uno de los dominios que contengan máquinas virtuales de Windows aprovisionadas y administradas, cree un grupo de Active Directory y añádale las credenciales de servicio de los agentes de WMI que cursan solicitudes de WMI remotas en las máquinas aprovisionadas.
- 2 Habilite las solicitudes de WMI remotas relativas a los grupos de Active Directory que contienen credenciales de agente en cada máquina de Windows aprovisionada.

Instalar el agente de WMI

El agente de Instrumental de administración de Windows (WMI) permite recopilar datos de las máquinas administradas de Windows.

Prerequisitos

- Los componentes de IaaS (Manager Service y sitio web incluidos) están instalados.
- Confirme que reúne todos los requisitos (consulte [“Habilitar solicitudes de WMI remotas en máquinas de Windows,”](#) página 117).
- [“Descargar el instalador de IaaS,”](#) página 75.

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vra-va-nombre_de_host.dominio.nombre@5480.exe` y seleccione **Ejecutar como administrador**.
- 2 Haga clic en **Siguiente**.
- 3 Acepte el acuerdo de licencia y haga clic en **Siguiente**.

- 4 En la página de inicio de sesión, escriba las credenciales de administrador de el dispositivo de vRealize Automation y compruebe el certificado SSL.
 - a Escriba el nombre de usuario, que es **root**, y la contraseña.
La contraseña es aquella que especificó al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital del certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado de el dispositivo de vRealize Automation se puede ver en el explorador del cliente cuando se accede a la consola de administración a través del puerto 5480.
- 5 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 6 Seleccione **Selección de componentes** en la página Tipo de instalación.
- 7 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
- 8 Haga clic en **Siguiente**.
- 9 Inicie sesión con los privilegios de **administrador** de los servicios de Windows en la máquina de instalación.
El servicio debe ejecutarse en la misma máquina de instalación.
- 10 Haga clic en **Siguiente**.
- 11 Seleccione **WMI** de la lista **Tipo de agente**.
- 12 Escriba un identificador de este agente en el cuadro de texto **Nombre de agente**.

Mantenga un registro del nombre de agente, las credenciales, el nombre de endpoint y la instancia de plataforma de cada agente. Esta información es necesaria para configurar endpoints y para añadir hosts más adelante.

IMPORTANTE: No duplique nombres de agente a menos que instale agentes redundantes configurados de forma idéntica para disponer de alta disponibilidad.

Opción	Descripción
Instalación de agentes redundantes	Instale agentes redundantes en servidores distintos, pero asígneles el mismo nombre y configúrelos exactamente igual para proporcionar alta disponibilidad.
Instalación de un solo agente	Seleccione un nombre único para este agente.

- 13 Configure una conexión con el componente Manager Service.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service. Por ejemplo, manager-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service. Por ejemplo, manager_service.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- 14 Configure una conexión con el componente Manager Website.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Website. Por ejemplo, website-load-balancer.eng.mycompany.com:443 . Las direcciones IP no se reconocen.
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Website. Por ejemplo, website_component.mycompany.com:443 . Las direcciones IP no se reconocen.

El puerto predeterminado es 443.

- 15 Haga clic en **Probar** para comprobar la conectividad con cada host.
- 16 Haga clic en **Agregar**.
- 17 Haga clic en **Siguiente**.
- 18 Haga clic en **Instalar** para comenzar la instalación.
- Transcurridos unos minutos, se mostrará un mensaje de operación correcta.
- 19 Haga clic en **Siguiente**.
- 20 Haga clic en **Finalizar**.
- 21 Confirme que la instalación se ha realizado correctamente.
- 22 (Opcional) Añada varios agentes con configuraciones diferentes y un endpoint en el mismo sistema.

Configurar el acceso al tenant predeterminado

5

Debe conceder a su equipo derechos de acceso al tenant predeterminado para que puedan empezar a configurar vRealize Automation.

El tenant predeterminado se crea automáticamente cuando se configura el inicio de sesión único en el asistente de instalación. No es posible editar los detalles del tenant como, por ejemplo, el nombre o token de URL, aunque puede crear nuevos usuarios locales y asignar administradores de tenant o de IaaS adicionales en cualquier momento.

Procedimiento

- 1 Inicie sesión en la consola de vRealize Automation como administrador del sistema del tenant predeterminado.
 - a Vaya a la consola de vRealize Automation.

Opción	Descripción
Si no usa un equilibrador de carga	<code>https://vrealize-appliance-hostname.domain.name/vcac</code>

- b Inicie sesión con el nombre de usuario **administrator** y la contraseña que haya definido para este usuario al configurar SSO.
- 2 Seleccione **Administración > Tenants**.
 - 3 Haga clic en el nombre del tenant predeterminado, **vsphere.local**.
 - 4 Haga clic en la pestaña **Usuarios locales**.
 - 5 Cree cuentas de usuario local para el tenant predeterminado de vRealize Automation.

Los usuarios locales son específicos del tenant y solo pueden acceder al tenant en el que se hayan creado.

 - a Haga clic en el icono **Añadir (+)**.
 - b Especifique los detalles del usuario responsable de administrar la infraestructura.
 - c Haga clic en **Agregar**.
 - d Repita este paso para añadir uno o varios usuarios adicionales que sean responsables de configurar el tenant predeterminado.
 - 6 Haga clic en la pestaña **Administradores**.

- 7 Asigne sus usuarios locales a las funciones de administrador de tenants y administrador de IaaS.
 - a Introduzca un nombre de usuario en el cuadro de búsqueda **Administradores de tenants** y presione Entrar.
 - b Introduzca un nombre de usuario en el cuadro de búsqueda **Administradores de IaaS** y presione Entrar.

El administrador de IaaS es responsable de crear y administrar los endpoints de infraestructura en vRealize Automation. Solo el administrador del sistema puede conceder esta función.
- 8 Haga clic en **Actualizar**.

Qué hacer a continuación

Proporcione a su equipo la URL de acceso y los datos de inicio de sesión para las cuentas de usuario que haya creado, para que así puedan empezar a configurar vRealize Automation.

- Los administradores de tenants configuran valores como la autenticación de usuarios, incluida la configuración de Administración de directorios para una mayor disponibilidad. Consulte *Configuración de vRealize Automation*.
- Los administradores de IaaS preparan los recursos externos para el aprovisionamiento. Consulte *Configuración de vRealize Automation*.
- Si configuró Crear contenido inicial durante la instalación, el administrador de la configuración puede solicitar el elemento del catálogo Contenido inicial para rellenar en poco tiempo una prueba del concepto. Para ver un ejemplo de cómo solicitar el elemento y completar la acción de usuario manual, consulte *Instalación y configuración de vRealize Automation para el escenario de Rainpole*.

Reemplazar los certificados autofirmados por certificados proporcionados por una entidad

6

Si ha instalado vRealize Automation con certificados autofirmados, puede que desee cambiarlos por certificados proporcionados por una entidad de certificación antes de implementarlo en producción.

Para obtener más información sobre cómo actualizar certificados, consulte *Administración de vRealize Automation*.

Solucionar problemas

En la resolución de problemas de vRealize Automation se ofrecen procedimientos para solucionar los problemas que podría encontrar durante la instalación o configuración de vRealize Automation.

Este capítulo cubre los siguientes temas:

- [“Ubicaciones de logs predeterminadas,”](#) página 125
- [“Revertir una instalación fallida,”](#) página 126
- [“Crear un paquete de soporte para vRealize Automation,”](#) página 128
- [“Solucionar problemas de instalación general,”](#) página 128
- [“Solucionar problemas de dispositivos de vRealize Automation,”](#) página 132
- [“Solucionar problemas con componentes de IaaS,”](#) página 133
- [“Solucionar problemas de errores de inicio de sesión,”](#) página 140

Ubicaciones de logs predeterminadas

Consulte los archivos log del producto y del sistema para obtener información acerca de los errores de instalación.

Las rutas de archivo que se muestran a continuación son las rutas predeterminadas. Si instaló IaaS en otro directorio, vaya a su directorio de instalación personalizado.

NOTA: VMware vRealize™ Automation (vRA) Content Pack for vRealize Log Insight ofrece un resumen de los eventos de log de todos los componentes de vRealize Automation. Para obtener más información, consulte la descripción de vRA 6.1+ Log Insight Content Pack sobre VMware Solution Exchange en https://solutionexchange.vmware.com/store/products/vra-6-1-log-insight-content-pack#.VU0r3_PD-Ht.

Logs de Windows

Busque los archivos log de los eventos de Windows en la siguiente ubicación.

Log	Ubicación
Logs del Visor de eventos de Windows	Inicio > Panel de control > Herramientas administrativas > Visor de eventos

Logs de instalación

Los logs de instalación se encuentran en las siguientes ubicaciones.

Log	Ubicación predeterminada
Logs de instalación	C:\Archivos de programa (x86)\vCAC\InstallLogs C:\Archivos de programa (x86)\VMware\vCAC\Server\ConfigTool\Log
Logs de instalación de WAPI	C:\Archivos de programa (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX>

Logs de IaaS

Los logs de IaaS se encuentran en las siguientes ubicaciones.

Log	Ubicación predeterminada
Logs de sitio web	C:\Archivos de programa (x86)\VMware\vCAC\Server\Website\Logs
Logs de repositorio	C:\Archivos de programa (x86)\VMware\vCAC\Server\Model Manager Web\Logs
Logs de Manager Service	C:\Archivos de programa (x86)\VMware\vCAC\Server\Logs
Logs de orquestaciones DEM	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<system-name> DEO \Logs
Logs de agente	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Agents\<agent-name>\logs

Logs de marco de vRealize Automation

Las entradas de logs para los marcos vRealize Automation se encuentran en la siguiente ubicación.

Log	Ubicación predeterminada
Logs de marco	/var/log/vmware

Logs de aprovisionamiento de componentes de software

Los logs de aprovisionamiento de componentes de software se encuentran en la siguiente ubicación.

Log	Ubicación predeterminada
Log de arranque de agente de software	/opt/vmware-appdirector (para Linux) o \opt\vmware-appdirector (para Windows)
Logs del script de ciclo de vida del software	/tmp/taskId (para Linux) \Users\darwin\AppData\Local\Temp\taskId (para Windows)

Recopilación de logs en implementaciones distribuidas

Puede crear un archivo ZIP que empaquete todos los logs de los componentes en una implementación distribuida. .

Revertir una instalación fallida

Cuando se produce un error de instalación y esta se revierte, el administrador del sistema debe comprobar que se han desinstalado todos los archivos necesarios antes de iniciar una nueva instalación. Algunos archivos se deben desinstalar de forma manual.

Revertir una instalación mínima

Un administrador del sistema debe eliminar de forma manual algunos archivos y revertir la base de datos para desinstalar por completo una instalación de IaaS de vRealize Automation con errores.

Procedimiento

- 1 Si los siguientes componentes están presentes, desinstálelos mediante el programa de desinstalación de Windows.
 - Agentes de vRealize Automation
 - DEM de trabajo de vRealize Automation
 - DEM orquestador de vRealize Automation
 - Servidor de vRealize Automation
 - WAPI de vRealize Automation

NOTA: Si ve el siguiente mensaje, reinicie la máquina y, a continuación, siga los pasos de este procedimiento: Error al abrir el archivo de log de la instalación. Compruebe que la ubicación del archivo de log especificada existe y que se puede escribir en ella.

NOTA: Si el sistema Windows se ha revertido, o si ha desinstalado IaaS, debe ejecutar el comando `iisreset` antes de reinstalar el IaaS de vRealize Automation.

- 2 Reverta la base de datos al estado en el que estaba antes de iniciar la instalación. El método que utilice dependerá del modo de instalación de la base de datos original.
- 3 En IIS (Administrador de Internet Information Services) seleccione Sitio web predeterminado (o su sitio personalizado) y haga clic en **Enlaces**. Quite el enlace HTTPS (el valor predeterminado es 443).
- 4 Compruebe que se han eliminado el repositorio de aplicaciones, vRealize Automation y WAPI, y que los grupos de aplicaciones `RepositoryAppPool`, `vCACAppPool` y `WapiAppPool` también se han eliminado.

La instalación se ha eliminado por completo.

Revertir una instalación distribuida

Un administrador del sistema debe eliminar de forma manual algunos archivos y revertir la base de datos para desinstalar por completo una instalación de IaaS con errores.

Procedimiento

- 1 Si los siguientes componentes están presentes, desinstálelos mediante el programa de desinstalación de Windows.
 - Servidor de vRealize Automation
 - WAPI de vRealize Automation

NOTA: Si ve el siguiente mensaje, reinicie la máquina y, a continuación, siga este procedimiento: Error al abrir el archivo de log de la instalación. Compruebe que la ubicación del archivo de log especificada existe y que se puede escribir en ella.

NOTA: Si el sistema Windows se ha revertido, o si ha desinstalado IaaS, debe ejecutar el comando `iisreset` antes de reinstalar el IaaS de vRealize Automation.

- 2 Reverta la base de datos al estado en el que estaba antes de iniciar la instalación. El método que utilice dependerá del modo de instalación de la base de datos original.
- 3 En IIS (Administrador de Internet Information Services) seleccione el sitio web predeterminado (o su sitio personalizado) y haga clic en **Enlaces**. Quite el enlace HTTPS (el valor predeterminado es 443).
- 4 Compruebe que se han eliminado el repositorio de aplicaciones, vCAC y WAPI, y que los grupos de aplicaciones RepositoryAppPool, vCACAppPool y WapiAppPool también se han eliminado.

Tabla 7-1. Puntos de error de reversión

Punto de error	Acción
Instalar Manager Service	Si está presente, desinstale el servidor de vCloud Automation Center.
Instalar el DEM orquestador	Si está presente, desinstale el DEM orquestador.
Instalar el DEM de trabajo	Si están presentes, desinstale los DEM de trabajo.
Instalar un agente	Si están presentes, desinstale todos los agentes de vRealize Automation.

Crear un paquete de soporte para vRealize Automation

Un usuario raíz puede usar un paquete de soporte en la consola de administración de el dispositivo de vRealize Automation o en componentes de IaaS. Estos paquetes sirven para que el equipo de soporte de VMware identifique el origen de los problemas que puedan surgir.

Para obtener información sobre cómo crear un paquete de soporte para un componente de IaaS, consulte el artículo de la base de conocimientos de VMware sobre cómo *recopilar logs de VMware vRealize Automation con la utilidad de recopilación de logs (2078179)* en <http://kb.vmware.com/kb/2078179>.

Realice el siguiente procedimiento para crear un paquete de soporte para el dispositivo de vRealize Automation.

Procedimiento

- 1 Vaya a la consola de administración de el dispositivo de vRealize Automation utilizando su nombre de dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 2 Inicie sesión y vaya a **Administración > Logs**.
- 3 Haga clic en **Crear paquete de soporte**.
- 4 Haga clic en **Descargar** y guarde el archivo en el sistema.

Puede usar el paquete de soporte para solucionar problemas por sí mismo o para enviarlos al representante de soporte de VMware.

Solucionar problemas de instalación general

Los temas de la solución de problemas de dispositivos de vRealize Automation proporcionan soluciones para problemas relacionados con la instalación que puede encontrarse cuando utilice vRealize Automation.

Error de tiempo de espera agotado de un equilibrador de carga al instalar o actualizar

Se ha producido un error en la instalación o actualización de vRealize Automation en una implementación distribuida con un equilibrador de carga y se ha recibido el error de servicio no disponible 503.

Problema

Se ha producido un error en la instalación o actualización porque la configuración de tiempo de espera del equilibrador de carga no permite que haya tiempo suficiente para finalizar la tarea.

Origen

Es posible que el error se deba a que la configuración de tiempo de espera del equilibrador de carga sea insuficiente. Para corregir el problema, puede aumentar la configuración del tiempo de espera del equilibrador de carga en 100 segundos como mínimo y volver a ejecutar la tarea.

Solución

- 1 Aumente el valor de tiempo de espera del equilibrador de carga en al menos 100 segundos. Por ejemplo, y en función del equilibrador de carga que esté usando, edite la configuración del tiempo de espera del equilibrador de carga en el archivo `ssl.conf`, `httpd.conf` o en otro archivo de configuración web.
- 2 Vuelva a ejecutar la instalación o la actualización.

Horas de servidor no sincronizadas

Es posible que una instalación no se complete correctamente si los servidores horarios de IaaS no están sincronizados con el dispositivo de vRealize Automation.

Problema

No puede iniciar sesión tras la instalación, o se produce un error durante la instalación.

Origen

Es posible que los servidores horarios no estén sincronizados en todos los servidores.

Solución

En cada servidor de el dispositivo de vRealize Automation y en todos los servidores de Windows donde se vayan a instalar componentes de IaaS, habilite la sincronización de hora tal y como se describe en los temas siguientes:

- [“Habilitar la sincronización de hora en el dispositivo de vRealize Automation,”](#) página 51
- [“Habilitar la sincronización de hora en el servidor de Windows,”](#) página 55

Para ver una descripción general del cronometraje en vRealize Automation, consulte [“Sincronización de hora,”](#) página 29.

Pueden aparecer páginas en blanco al utilizar Internet Explorer 9 o 10 en Windows 7

Si utiliza Internet Explorer 9 o 10 en Windows 7 y tiene habilitado el modo de compatibilidad, algunas páginas aparecen sin contenido.

Problema

Cuando se utiliza Internet Explorer 9 o 10 en Windows 7, las siguientes páginas aparecen sin contenido:

- Infraestructura
- Carpeta de tenant predeterminada en la página Orchestrator
- Configuración de servidor en la página Orchestrator

Origen

El problema puede deberse al hecho de que el modo de compatibilidad esté habilitado. Siga estos pasos para deshabilitar el modo de compatibilidad en Internet Explorer.

Solución

Prerequisitos

Asegúrese de que la barra de menús esté visible. Si utiliza Internet Explorer 9 o 10, presione Alt para mostrar la barra de menús (o haga clic con el botón derecho en la barra de direcciones y seleccione **Barra de menús**).

Procedimiento

- 1 Seleccione **Herramientas > Configuración de Vista de compatibilidad**.
- 2 Desactive la opción **Mostrar sitios de la intranet en Vista de compatibilidad**.
- 3 Haga clic en **Cerrar**.

No se puede establecer una relación de confianza para el canal seguro SSL/TLS

Es posible que reciba el mensaje "No se puede establecer una relación de confianza para el canal seguro SSL/TLS al actualizar certificados de seguridad para vCloud Automation Center".

Problema

Si surge un problema de certificado con vcac-config.exe al actualizar un certificado de seguridad, puede ser que vea el siguiente mensaje:

Se ha terminado la conexión: No se puede establecer una relación de confianza para el canal seguro SSL/TLS

Si desea obtener más información sobre la causa del problema, siga el procedimiento que se describe a continuación.

Solución

- 1 Abra el archivo `vcac-config.exe.config` y busque la dirección de repositorio: `<add key="repositoryAddress" value="https://[IaaS address]:443/repository/" />`
- 2 Navegue a esa dirección con Internet Explorer.
- 3 Recorra los mensajes de error relativos a problemas de confianza de certificados.
- 4 Obtenga un informe de seguridad de Internet Explorer y úselo para solucionar el problema de confianza de este certificado.

Si el problema persiste, repita el procedimiento y esta vez navegue a la dirección que necesita registrarse, es decir, la dirección de Endpoint que usó en el registro con vcac-config.exe.

Conectarse a la red mediante un servidor proxy

Algunos sitios pueden conectarse a Internet mediante un servidor proxy.

Problema

Su implementación no puede conectarse a la Internet abierta. Por ejemplo, no puede acceder a sitios web, a las nubes públicas que administra ni a las direcciones de proveedores desde donde descarga software o actualizaciones.

Origen

Su sitio se conecta a Internet mediante un servidor proxy.

Solución

Prerequisitos

Solicítele al administrador de su sitio los nombres, números de puerto y credenciales del servidor proxy.

Procedimiento

- 1 Abra en un navegador web la consola de administración de el dispositivo de vRealize Automation:
`https://appliance-FQDN-or-IP-address:5480`
- 2 Inicie sesión con el nombre de usuario **root** y la contraseña que utilizó para implementar el dispositivo.
- 3 Haga clic en la pestaña **Red**.
- 4 Escriba el FQDN, o dirección IP, y el número de puerto del servidor proxy de su sitio.
- 5 Si el servidor proxy requiere credenciales, introduzca el nombre de usuario y la contraseña.
- 6 Haga clic en **Guardar configuración**.

Qué hacer a continuación

Si configura el uso de un proxy, puede que el usuario tenga problemas a la hora de acceder a VMware Identity Manager. Para corregir el problema, consulte [“El servidor proxy impide el inicio de sesión de usuario de VMware Identity Manager,”](#) página 131.

El servidor proxy impide el inicio de sesión de usuario de VMware Identity Manager

Configurar el uso de un proxy puede impedir el inicio de sesión de los usuarios de VMware Identity Manager.

Problema

Si configura vRealize Automation para acceder a la red a través de un servidor proxy, los usuarios de VMware Identity Manager ven el siguiente error cuando intentan iniciar sesión.

Error Unable to get metadata

Solución

Prerequisitos

Configure vRealize Automation para acceder a la red a través de un servidor proxy. Consulte [“Conectarse a la red mediante un servidor proxy,”](#) página 130.

Procedimiento

- 1 Inicie sesión en la consola del el dispositivo de vRealize Automation como raíz.
- 2 Abra el siguiente archivo en un editor de texto.
`/etc/sysconfig/proxy`
- 3 Actualice la línea `NO_PROXY` para que omita el servidor proxy en los inicios de sesión de VMware Identity Manager.
`NO_PROXY=vra-hostname`
Por ejemplo, `NO_PROXY=localhost, 127.0.0.1, vra.system.mycompany.com`.
- 4 Guarde y cierre el proxy.

- 5 Escriba el siguiente comando para reiniciar el servicio del área de trabajo de Horizon.
`service horizon-workspace restart`

Solucionar problemas de dispositivos de vRealize Automation

Los temas de resolución de problemas para dispositivos de vRealize Automation proporcionan soluciones a posibles problemas relacionados con la instalación con los que se puede encontrar cuando utiliza sus dispositivos de vRealize Automation.

Error de descarga de los instaladores

Los instaladores no se pueden descargar de el dispositivo de vRealize Automation.

Problema

Los instaladores no se descargan cuando se ejecuta `setup__vra-va-hostname.domain.name.exe`.

Origen

- Problemas de conectividad de red al conectarse a la máquina de el dispositivo de vRealize Automation.
- No se puede conectar a la máquina de el dispositivo de vRealize Automation porque la máquina no está accesible o no responde antes de que el tiempo de conexión se agote.

Solución

- 1 Compruebe que puede conectarse a el dispositivo de vRealize Automation; para ello, escriba la siguiente URL en un explorador web.
`https://vra-va-hostname.domain.name`
- 2 Consulte el resto de temas de solución de problemas de el dispositivo de vRealize Automation.
- 3 Descargue el archivo de instalación y vuelva a conectarse a el dispositivo de vRealize Automation.

El archivo Encryption.key tiene permisos incorrectos

Se puede producir un error del sistema cuando se asignan permisos incorrectos al archivo Encryption.key de un dispositivo virtual.

Problema

Inicia sesión en el dispositivo de vRealize Automation y se abre la página Tenants. Una vez que la página empieza a cargarse, aparece el mensaje Error del sistema.

Origen

El archivo Encryption.key tiene permisos incorrectos o el nivel de usuario de propietario o grupo está mal asignado.

Solución

Prerequisitos

Inicie sesión en el dispositivo virtual donde se muestra el error.

NOTA: Si los dispositivos virtuales funcionan con un equilibrador de carga, deberá comprobar cada uno de ellos.

Procedimiento

- 1 Consulte el archivo de log `/var/log/vcac/catalina.out` y busque el mensaje `Cannot write to /etc/vcac/Encryption.key`.

- 2 Vaya al directorio `/etc/vcac/` y compruebe los permisos y propiedad del archivo `Encryption.key`. Debería ver una línea parecida a esta:


```
-rw----- 1 vcac vcac 48 Dec 4 06:48 encryption.key
```

 Se necesitan permisos de lectura y escritura y el propietario y grupo del archivo debe ser `vcac`.
- 3 Si ve otra cosa, cambie los permisos o la propiedad del archivo según corresponda.

Qué hacer a continuación

Iniciar sesión en la página Tenants para constatar que puede hacerlo sin errores.

Identity Manager no puede iniciarse después del reinicio de Horizon-Workspace

En un entorno de alta disponibilidad de vRealize Automation, puede producirse un error de inicio de Identity Manager después de reiniciar el servicio de Horizon-Workspace.

Problema

El servicio de Horizon-Workspace no se puede iniciar debido a un error similar al siguiente:

```
Error al crear haz con el nombre 'liquibase' definido en el recurso de ruta de clase [spring/datastore-wireup.xml]: Error de invocación del método init; la excepción anidada es liquibase.exception.LockException: No se pudo adquirir el bloqueo del log de cambio. Bloqueado actualmente por fe80:0:0:0:250:56ff:fea8:7d0c%eth0 (fe80:0:0:0:250:56ff:fea8:7d0c%eth0) desde 29/10/15
```

Origen

Es posible que se produzca un error al iniciar Identity Manager en un entorno de alta disponibilidad debido a problemas con la utilidad de administración de datos liquibase usada por vRealize Automation.

Solución

- 1 Inicie sesión como raíz en el dispositivo de vRealize Automation usando `ssh`.
- 2 Ejecute el comando `service horizon-workspace` para detener el servicio de Horizon-Workspace.
- 3 Ejecute el comando `su postgres` para convertirse en un usuario postgres.
- 4 Ejecute el comando `psql vcac`.
- 5 Ejecute la siguiente consulta SQL: `"update "databasechangelock" set locked=FALSE, lockgranted=NULL, lockedby=NULL where id=1;"`
- 6 Ejecute la consulta SQL `select *` desde `databasechangelock`.
La salida debe mostrar un valor `"f"` de bloqueo.
- 7 Inicie el servicio de Horizon-Workspace mediante el comando `service horizon-workspace start`.

Solucionar problemas con componentes de IaaS

Los temas de resolución de problemas para componentes de IaaS de vRealize Automation proporcionan soluciones a posibles problemas relacionados con la instalación con los que se puede encontrar cuando utiliza vRealize Automation,

Validar certificados de servidor para IaaS

Puede utilizar el comando `vcac-Config.exe` para comprobar que un servidor de IaaS acepta certificados de el dispositivo de vRealize Automation y de dispositivos SSO.

Problema

Aparecen errores de autorización al utilizar las funciones de IaaS.

Origen

Los errores de autorización se pueden producir cuando IaaS no reconoce los certificados de seguridad de otros componentes.

Solución

- 1 Abra un símbolo del sistema como administrador y vaya al directorio Cafe de `<vra-installation-dir>\Server\Model Manager Data\Cafe`, que suele estar ubicado en `C:\Archivos de programa (x86)\VMware\VCAC\Server\Model Manager Data\Cafe`.
- 2 Escriba un comando con el formato `Vcac-Config.exe CheckServerCertificates -d [vra-database] -s [vRA SQL server] -v`. Los parámetros opcionales son `-su [SQL user name]` y `-sp [password]`.

Si el comando se ejecuta correctamente, aparece el siguiente mensaje:

```
Certificates validated successfully.
Command succeeded."
```

Si el comando no se ejecuta correctamente, aparece un mensaje de error detallado.

NOTA: Este comando solo está disponible en el nodo del componente Model Manager Data.

Error de credenciales al ejecutar el instalador de IaaS

Al instalar componentes de IaaS, aparece un error cuando escribe las credenciales del dispositivo virtual.

Problema

Tras proporcionar las credenciales en el instalador de IaaS, aparece un error de `org.xml.sax.SAXParseException`.

Origen

Ha usado credenciales incorrectas o un formato de credencial incorrecto.

Solución

- ◆ Procure usar los valores de nombre de usuario y tenant adecuados.

Por ejemplo, el tenant predeterminado de SSO utiliza un nombre de dominio del tipo `vsphere.local`, no `administrador@vsphere.local`.

Se muestra una advertencia de configuración no guardada durante la instalación de IaaS

Aparece un mensaje durante la instalación de IaaS. Advertencia: no se pudo guardar la configuración en el dispositivo virtual durante la instalación de IaaS.

Problema

Durante la instalación de IaaS se muestra un mensaje de error poco específico donde se indica que la configuración de usuario no se ha guardado.

Origen

Este mensaje puede aparecer por error cuando hay problemas de comunicación o de red.

Solución

Ignórela y continúe con la instalación. Este mensaje no debería provocar errores en la instalación.

Error al instalar el servidor de sitios web y Distributed Execution Managers

La instalación de Distributed Execution Managers y del servidor de sitios web de la infraestructura de el dispositivo de vRealize Automation no puede continuar si la contraseña de su cuenta de servicio de IaaS contiene comillas dobles.

Problema

Verá un mensaje que le indica que se ha producido un error en la instalación de Distributed Execution Managers (DEM) y el servidor de sitios web de el dispositivo de vRealize Automation porque los parámetros de msiexec no son válidos.

Origen

Se ha usado un carácter de comillas dobles en la contraseña de la cuenta de servicio de IaaS.

Solución

- 1 Compruebe que su contraseña de la cuenta de servicio de IaaS no contenga comillas dobles.
- 2 Si su contraseña contiene comillas dobles, cree una nueva.
- 3 Reinicie la instalación.

La autenticación de IaaS genera un error durante la instalación de administración de modelo y web de IaaS

Al ejecutar el Comprobador de requisitos previos, aparece un mensaje que indica que la comprobación de la autenticación de IIS no se ha podido realizar.

Problema

En el mensaje se señala que la autenticación no está habilitada, pero la casilla de autenticación de IIS sí está activada.

Solución

- 1 Desactive la casilla de autenticación de Windows.
- 2 Haga clic en **Guardar**.
- 3 Active la casilla de autenticación de Windows.
- 4 Haga clic en **Guardar**.
- 5 Vuelva a ejecutar el Comprobador de requisitos previos.

Error al instalar los componentes web y Model Manager Data

Si el instalador de IaaS no puede guardar el componente de Model Manager Data ni el componente web, se producirá un error en la instalación de vRealize Automation.

Problema

Se produce un error en la instalación con el siguiente mensaje:

El instalador de IaaS no ha podido guardar los componentes web y de Model Manager Data.

Origen

El error tiene varias causas posibles.

- Problemas de conectividad con el dispositivo de vRealize Automation o problemas de conectividad entre los dispositivos. Se produce un error al intentar conectarse debido a que no se ha obtenido respuesta o a que no se ha podido establecer la conexión.
- Problemas con el certificado de confianza en IaaS cuando se usa una configuración distribuida.
- Discrepancia del nombre de certificado en una configuración distribuida.
- Puede que el certificado no sea válido o que se haya producido un error en la cadena de certificados.
- Error de inicio del servicio de repositorio.
- Configuración incorrecta del equilibrador de carga en un entorno distribuido.

Solución

■ Conectividad

Compruebe que puede conectarse a el dispositivo de vRealize Automation; para ello, escriba la siguiente URL en un navegador web: `https://vra-va-hostname.domain.name`.

■ Problemas con el certificado de confianza

- En IaaS, abra Microsoft Management Console con el comando `mmc.exe` y compruebe que el certificado usado en la instalación se ha añadido al almacén de certificados raíz de confianza de la máquina.
- Desde un navegador, compruebe `https://<ip-web>/repository/data/MetaModel.svc` y confirme que no hay errores de certificado en el navegador.

■ Discrepancia del nombre de certificado

Este error se puede producir cuando el certificado se emite para un nombre concreto, pero se utiliza un nombre o una dirección IP diferente. Puede suprimir el error de discrepancia de nombre de certificado durante la instalación si selecciona **Suprimir discrepancia de certificado**.

También puede usar esa opción para omitir los errores de discrepancia de revocación de certificado remotos.

■ Certificado no válido

Abra la Microsoft Management Console con el comando `mmc.exe`. Compruebe que el certificado no ha caducado y que su estado es correcto. Realice esta acción para todos los certificados de la cadena de certificados. Puede que deba importar otros certificados de la cadena en el almacén de certificados raíz de confianza cuando utilice una jerarquía de certificados.

■ Servicio del repositorio

Use las siguientes acciones para comprobar el estado del servicio de repositorio.

- Desde un navegador, compruebe el estado del servicio MetaModel en `https://<ip-web>/repository/data/MetaModel.svc`.
- Compruebe el archivo `Repository.log` para determinar si contiene errores.
- Restablezca IIS (`iisreset`) si tiene problemas con las aplicaciones alojadas en el sitio web (repositorio, vRealize Automation o WAPI).
- Compruebe los logs del sitio web en `%SystemDrive%\inetpub\logs\LogFiles` para obtener información de registro adicional.
- Compruebe que el resultado del Comprobador de requisitos previos fue correcto cuando se comprobaron los requisitos.

- En Windows 2012, compruebe que se han instalado los servicios WCF de .NET Framework y la activación HTTP.

Error interno al añadir un endpoint de XaaS

Al intentar crear un endpoint de XaaS, aparece un mensaje de error interno.

Problema

Al crear un endpoint, aparece el siguiente mensaje de error interno: Se ha producido un error interno. Si el problema continúa, póngase en contacto con el administrador del sistema. Cuando se ponga en contacto con el administrador del sistema, use esta referencia: *c0DD0C01*. Los códigos de referencia se generan aleatoriamente y no están vinculados a un mensaje de error concreto.

Solución

- 1 Abra el archivo log del dispositivo vRealize Automation.
`/var/log/vcac/catalina.out`
- 2 Busque el código de referencia en el mensaje de error.
Por ejemplo, *c0DD0C01*.
- 3 Busque el código de referencia en el archivo log para ubicar la entrada asociada.
- 4 Para solucionar el problema, revise las entradas que aparecen por encima y por debajo de la entrada asociada.

La entrada de log asociada no señala específicamente el origen del problema.

Error al desinstalar un agente de proxy

Pueden producirse errores al quitar un agente de proxy si está habilitado el registro del programa de instalación de Windows.

Problema

Al intentar desinstalar un agente de proxy del Panel de control de Windows, la desinstalación no se realiza correctamente y aparece el siguiente error:

```
Error opening installation log file. Verify that the
specified log file location exists and is writable
```

Origen

Esto puede ocurrir si está habilitado el registro del programa de instalación de Windows y el motor del programa de instalación de Windows no puede escribir correctamente el archivo de log de desinstalación. Para obtener más información, consulte el artículo de Microsoft Knowledge Base en <http://support.microsoft.com/kb/2564571>.

Solución

- 1 Reinicie la máquina o reinicie explorer.exe desde el Administrador de tareas.
- 2 Desinstale el agente.

Error de solicitudes de máquinas cuando las transacciones remotas están deshabilitadas

Se producen errores en las solicitudes de máquina cuando las transacciones remotas del Coordinador de transacciones distribuidas (DTC) de Microsoft están deshabilitadas en las máquinas servidor de Windows.

Problema

Si se aprovisiona una máquina cuando las transacciones remotas están deshabilitadas en el portal de Model Manager o SQL Server, la solicitud no se realizará. Se produce un error en la recopilación de datos y la solicitud de máquina se mantiene en el estado CloneWorkflow.

Origen

Las transacciones remotas de DTC están deshabilitadas en la instancia de SQL de IaaS que el sistema vRealize Automation utiliza.

Solución

- 1 Inicie Windows Server Manager para habilitar DTC en todos los servidores de vRealize y servidores SQL relacionados.

En Windows 7, vaya a **Inicio > Herramientas administrativas > Servicios de componentes**.

NOTA: Asegúrese de que todos los servidores de Windows tienen SID únicos en la configuración de MSDTC.

- 2 Abra todos los nodos para encontrar el DTC local (o el DTC en clúster, si usa un sistema en clúster).
Vaya a **Servicios de componentes > Equipos > Mi PC > Coordinador de transacciones distribuidas**.
- 3 Haga clic con el botón derecho en el DTC local o en clúster y seleccione **Propiedades**.
- 4 Haga clic en la pestaña Seguridad.
- 5 Seleccione la opción **Acceso a DTC desde la red**.
- 6 Seleccione las opciones **Permitir cliente remoto** y **Permitir administración remota**.
- 7 Seleccione las opciones **Permitir entrantes** y **Permitir salientes**.
- 8 Escriba o seleccione NT AUTHORITY\Network Service en el campo **Cuenta** de la cuenta de inicio de sesión en DTC.
- 9 Haga clic en **Aceptar**.
- 10 Quite las máquinas que estén en estado CloneWorkflow.
 - a Inicie sesión en el dispositivo de vRealize Automation.
`https://virtualappliancename/vcac/tenantname`
 - b Vaya a **Infraestructura > Máquinas administradas**.
 - c Haga clic con el botón derecho en la máquina de destino.
 - d Seleccione **Eliminar** para quitar la máquina.

Error en la comunicación de Manager Service

Los nodos de IaaS que se clonan a partir de una plantilla donde está instalado MS DTC contienen identificadores duplicados para MS DTC, lo que impide la comunicación entre los nodos.

Problema

Se produce un error en IaaS Manager Service y se muestra el siguiente mensaje de error en el log de Manager Service.

Error de comunicación con el administrador de transacciones subyacente. --->
System.Runtime.InteropServices.COMException: el administrador de transacciones de MS DTC no pudo obtener la transacción del administrador de transacciones de origen debido a problemas de comunicación. Posibles causas: hay un firewall que no incluye una excepción para el proceso de MS DTC, las dos máquinas no pueden encontrarse la una a la otra por sus nombres de NetBIOS o la compatibilidad con transacciones de red no está habilitada para uno de los dos administradores de transacciones.

Origen

Cuando se clona un nodo de IaaS que tiene instalado MS DTC, ambos clones usan el mismo identificador único para MS DTC. Se produce un error de comunicación entre los nodos.

Solución

- 1 Abra un símbolo del sistema de administrador.
- 2 Ejecute el siguiente comando: `msdtc -uninstall`
- 3 Reinicie la máquina virtual.
- 4 Abra un símbolo del sistema distinto y ejecute el siguiente comando:
`msdtc -install <manager-service-host>`.

El comportamiento de personalización de correo electrónico ha cambiado

En vRealize Automation 6.0 o posterior, solo las notificaciones generadas con el componente IaaS se pueden personalizar mediante la funcionalidad de plantillas de correo electrónico de versiones anteriores.

Solución

Puede usar las siguientes plantillas XSLT:

- ArchivePeriodExpired
- EpiRegister
- EpiUnregister
- LeaseAboutToExpire
- LeaseExpired
- LeaseExpiredPowerOff
- ManagerLeaseAboutToExpire
- ManagerLeaseExpired
- ManagerReclamationExpiredLeaseModified
- ManagerReclamationForcedLeaseModified
- ReclamationExpiredLeaseModified
- ReclamationForcedLeaseModified

- VdiRegister
- VdiUnregister

Las plantillas de correo electrónico se encuentran en el directorio `\Templates` del directorio de instalación del servidor, que suele ser `%SystemDrive%\Program Files x86\VMware\vCAC\Server`. El directorio `\Templates` también incluye plantillas XSLT que ya no son compatibles y no se pueden modificar.

Solucionar problemas de errores de inicio de sesión

Los temas de resolución de problemas por errores de inicio de sesión de vRealize Automation proporcionan soluciones para posibles problemas relacionados con la instalación que pueden surgir al utilizar vRealize Automation.

Error sin explicación al intentar iniciar sesión como administrador de IaaS con credenciales con formato de UPN incorrecto

Al intentar iniciar sesión en vRealize Automation como administrador de IaaS, se le redirige a la página de inicio de sesión sin motivo aparente.

Problema

Si se intenta iniciar sesión en vRealize Automation como un administrador de IaaS con credenciales con formato de UPN que no incluyen la parte `@@yourdomain` del nombre de usuario, se cerrará la sesión de SSO de forma inmediata y se le redirigirá a la página de inicio de sesión sin ninguna explicación.

Origen

El UPN introducido debe tener el formato `yourname.admin@yourdomain`; por ejemplo, si inicia sesión con el nombre de usuario `jsmith.admin@sqa.local`, pero el UPN en Active Directory está establecido como `jsmith.admin`, se producirá un error al iniciar sesión.

Solución

Para subsanar el problema, cambie el valor `userPrincipalName` para que incluya el contenido `@yourdomain` necesario y, a continuación, intente iniciar sesión de nuevo. En este ejemplo el nombre de UPN debería ser `jsmith.admin@sqa.local`. Esta información se encuentra en el archivo de log ubicado en la carpeta `log/vcac`.

No se puede iniciar sesión en un tenant o los almacenes de identidades de tenants desaparecen

Noventa días después de la implementación, no puede iniciar sesión en un tenant o el almacén de identidades de un tenant desaparece.

Problema

- Cuando inicia sesión en un tenant, aparece una página en blanco con un botón Enviar en la esquina superior izquierda.
- Recibe un error de excepción del sistema al acceder a la página de configuración del almacén de identidades del tenant.
- La configuración del almacén de identidades desaparece.
- No puede iniciar sesión en un tenant con una cuenta LDAP.
- El log `catalina.out` ubicado en `/var/log/vmware/vcac/` muestra un error similar al siguiente:

```
12:40:49,190 [tomcat-http--34] [authentication] INFO
com.vmware.vim.sso.client.impl.SecurityTokenServiceImpl
$RequestResponseProcessor.handleFaultCondition:922 - Failed trying to retrieve token:
ns0:RequestFailed: Error occurred looking for solution user :: Insufficient access YYYY-03-18
12:40:49,201 [tomcat-http--34] [authentication] ERROR
com.vmware.vcac.platform.service.rest.resolver.ApplicationExceptionHandler.handleUnexpectedEx
ception:820 - Failed trying to retrieve token: ns0:RequestFailed: Error occurred looking for
solution user :: Insufficient access com.vmware.vim.sso.client.exception.InternalError:
Failed trying to retrieve token: ns0:RequestFailed: Error occurred looking for solution
user :: Insufficient access
```

Origen

La contraseña de administrador de tenants interna de SSO caduca a los 90 días de forma predeterminada. Este problema es interno de vRealize Automation y no afecta a los almacenes de identidades de Active Directory externos.

La falta de aviso en la interfaz de usuario de vRealize Automation de que la contraseña de administrador de tenants va a caducar es un problema conocido. Para solucionar este problema, deshabilite la caducidad de la contraseña para la cuenta de administrador de tenants.

Si desea ver instrucciones paso a paso para solucionar este problema, consulte el artículo de la base de conocimientos de VMware en <http://kb.vmware.com/kb/2075011>.

Índice

A

- acceso a la base de datos de IaaS, habilitar desde el usuario del servicio **95**
- administradores de IaaS, crear **121**
- Agente de administración
 - desinstalar **35, 42**
 - instalar **34, 35, 42**
- agente de proxy, error de desinstalación **137**
- agente de VDI de XenDesktop, instalar **107**
- agente de vSphere
 - configuración de simultaneidad admitida **99**
 - permisos necesarios **99**
- agentes
 - agentes de integración **16**
 - agentes de WMI **16**
 - configurar agentes de vSphere **102**
 - configurar Hyper-V **106**
 - configurar XenServer **106**
 - elegir un escenario de instalación **98**
 - EPI PowerShell **16**
 - habilitar solicitudes de WMI remotas **117**
 - Hyper-V **103, 104**
 - instalar **97**
 - instalar agente de EPI para Citrix **111**
 - instalar agentes de Citrix **112**
 - instalar agentes de vSphere **100**
 - instalar el agente de EPI para Visual Basic Scripting **114**
 - instalar para Visual Basic Scripting **115**
 - instalar WMI **117**
 - instalar XenDesktop **109**
 - requisitos de creación de scripts de Visual Basic **114**
 - ubicación y requisitos de instalación **98**
 - VDI PowerShell **16**
 - XenServer **103, 104**
- agentes de Citrix, instalar **112**
- agentes de EPI, instalar para Visual Basic Scripting **114, 115**
- agentes de Hyper-V, instalar **104**
- agentes de proxy, instalar y configurar para vSphere **98**
- agentes de proxy de virtualización **16**
- agentes de proxy de vSphere, instalar y configurar **98**

- agentes de vSphere
 - configurar **102**
 - instalar **100**
- agentes de WMI
 - habilitar solicitudes remotas **117**
 - instalar **117**
- agentes de XenServer, instalar **104**
- almacén de identidades, requisitos de dominio **26**
- almacenes de identidades, resolución de problemas **140**
- archivo Encryption.key, establecer permisos **132**
- archivos PEM, comando para extraer **29**
- asistente de instalación, implementación empresarial **41**
- Asistente de instalación, descripción general **31**
- autenticación de IaaS, error **135**

B

- base de datos
 - crear con el asistente **79**
 - preparar base de datos de IaaS **76**
 - requisitos **21**
- base de datos de IaaS
 - configurar la cuenta de servicios de Windows para usar autenticación de SQL **95**
 - configurar para SSL seguro **58, 76–79**
 - configurar servicio de Windows para acceder **95**
 - creación de la base de datos **78**
 - crear la base de datos con el asistente **79**
 - crear la base de datos manualmente **77**
 - especificar la base de datos de SQL **58**

C

- cadenas de certificados, orden **28**
- certificados
 - cambiar de autofirmados **123**
 - relaciones de confianza **63**
- certificados en cadena, orden **28**
- certificados SSL, extraer **29**
- Citrix, instalar el agente de EPI **111**
- claves privadas RSA, comando para extraer **29**
- clústeres de vRealize Appliance, unir **72**
- clústeres;unir **72**
- componente de sitio web, instalar **81, 83, 85**
- componentes de IaaS
 - instalar **55**

- instalar en una configuración distribuida **73**
- registrar **60**
- solucionar problemas **133**
- componentes de IaaS, definiciones **62**
- componentes de infraestructura, instalar **56**
- componentes de instalación
 - comprobar requisitos previos **58**
 - dispositivo de VMware vRealize Automation **15**
 - elegir una ruta de implementación **11**
 - Infraestructura como servicio (IaaS) de VMware **15**
 - SSO **14**
- Comprobador de requisitos previos, ejecutar en el asistente de instalación **37, 44**
- configuración de contenido inicial, crear contraseña **40, 47**
- configuración de cuenta, especificar **58**
- configuración de hora de los dispositivos virtuales, con el Asistente de instalación **37, 44**
- configuración de servidor, especificar **58**
- configurar, dispositivo de vRealize Automation **68**
- contraseña, restricciones **20**
- Coordinador de transacciones distribuidas (DTC) **21**
- cuenta de servicios de Windows, configurar para usar autenticación de SQL **95**

D

- dem
 - requisitos de Amazon Web Services EC2 **23**
 - requisitos de Red Hat **23**
 - requisitos de SCVMM **24**
- DEM
 - acerca de la instalación **92**
 - error de instalación **135**
 - instalar **92**
 - requisitos **23**
- descarga de instalación, resolución de problemas **132**
- desinstalar, instalación con errores **127**
- discrepancia del nombre de certificado **135**
- dispositivo de vRealize Automation, implementar **65**
- dispositivos, configurar más **71**
- dispositivos de vRealize Automation, solucionar problemas **132**
- Distributed Execution Manager, Véase DEM
- Distributed Execution Managers, Véase también DEM
- DTC (Coordinador de transacciones distribuidas) **21**

E

- equilibradores de carga, configurar **66**
- error de inicio de sesión, servidores desincronizados **129**
- error de instalación, servidores desincronizados **129**
- error de solicitud de máquina **138**
- error interno, añadir endpoint de XaaS **137**
- errores de inicio de sesión, solucionar problemas **140**
- escenario de implementación
 - implementación distribuida **61**
 - implementación mínima **49**
 - instalación mínima **11**
- escenarios, elegir una instalación de agentes **98**

H

- hipervisor, requisitos **103**
- Huella digital SSL del agente de administración, buscar **34, 42**
- Hyper-V
 - agente **103**
 - agente de proxy **103**
 - requisitos **103**

I

- IaaS
 - agentes **16**
 - descargar instalador **75**
- IaaS de VMware
 - Distributed Execution Manager **16**
 - Manager Service **15**
- IaaS de VMware, base de datos **16**
- IaaS de VMware, Model Manager **15**
- IaaS Manager Service, requisitos **22**
- Identity Manager, error al iniciarse **133**
- implementación distribuida
 - descripción de instalación **13**
 - deshabilitar servicios sin usar **73**
 - instalar con asistente **41**
 - validar **73**
- implementación empresarial, instalar con asistente **41**
- implementación mínima, descripción de instalación **12**
- implementaciones mínimas, instalar con el asistente de instalación **33**
- información actualizada **9**
- inicio de sesión de administrador de IaaS erróneo **140**
- instalación
 - completar **60**
 - configurar **125**
 - descripción de implementación distribuida **13**

- descripción de una implementación mínima **12**
- descripción general **11**
- descripción general de una instalación mínima **49**
- dispositivo de vRealize Automation **50, 67**
- DNS y resolución de nombres de host **19**
- especificar agentes **59**
- especificar managers **59**
- finalizar **39, 46**
- preparación **19**
- solucionar problemas **125**
- usar la consola de administración **49**
- instalación con errores, logs **125**
- instalación distribuida
 - descripción general **61**
 - desinstalación **127**
- instalación distribuida de IaaS **62**
- instalación mínima, desinstalación **127**
- instalador de IaaS
 - descargar **57**
 - resolución de problemas **134**
- instalar
 - configurar dispositivos de vCloud Automation Center **67**
 - consideraciones sobre los navegadores **20**
 - descargar instalador de IaaS **75**
 - hoja de trabajo **63**

L

- logs
 - IaaS **125**
 - solucionar problemas **125**
 - ubicaciones **125**

M

- Manager Service
 - definición **62**
 - instalar **87, 89**
 - requisitos **22**
- mensaje de error del sistema **132**
- Model Manager
 - definición **62**
 - entorno multicliente seguro **15**
 - lógica empresarial editable **15**
 - modelo de datos unificados **15**
 - políticas de ejecución **15**
 - solucionar problemas de error de instalación **135**
- Model Manager Data, instalar **81, 83, 85**
- Model Manager Web **15**

N

- nodos de IaaS clonados **139**
- nombre de host de XenServer, configuración **108**

P

- paquete de soporte, crear **128**
- parámetro de instalación, validación **39, 46**
- parámetros de implementación, especificar **38, 45**
- personalizaciones de correo electrónico **139**
- PowerShell, establecer en RemoteSigned **97**
- preparación de la instalación, sincronización de hora **29**
- problemas con el certificado de confianza **135**
- proxy **131**

R

- requisitos
 - base de datos **21**
 - DEM **23**
 - SQL **21**
- requisitos de instalación
 - credenciales **26**
 - entornos de implementación **20**
 - hardware **20**
 - máquina virtual **20**
 - requisitos de IaaS **21**
 - requisitos de puertos **24**
 - seguridad **28**
 - servidor de Windows **21**
 - sistema operativo **20**
 - usuarios **26**
 - XenDesktop **107**
- requisitos de Java, para base de datos de MSSQL **21**
- requisitos de servidor, IaaS o servidor de Windows **21**
- requisitos previos
 - comprobar **58**
 - consideraciones sobre los navegadores **20**
- resolución de problemas
 - aparición de páginas en blanco **129**
 - instalador de IaaS **134**
 - servidores horarios desincronizados **129**
- ruta de implementación
 - elegir **11**
 - instalación distribuida **11**

S

- seguridad
 - certificados **28**
 - certificados de IaaS **56, 75**
 - frase de contraseña **29**

- relaciones de confianza **63**
- software de terceros **29**
- servicios de IaaS, comprobar **96**
- servidor de aprovisionamiento **111**
- sincronización de hora
 - habilitar en máquina de Windows **55**
 - servidores **51, 71**
- snapshots, crear **38, 45**
- solucionar problemas
 - nodos de IaaS clonados **139**
 - solicitudes de máquinas **138**
 - ubicaciones de logs **125**
- solucionar problemas de instalación **128**
- SQL, requisitos **21**

T

- tareas posteriores a la instalación, configurar
 - servicio de Windows para acceder a la base de datos de IaaS **95**
- tenants
 - configurar tenant predeterminado **121**
 - solucionar problemas de almacenes de identidades **140**
 - solucionar problemas de inicio de sesión **140**
- tiempo de espera del equilibrador de carga
 - agotado antes de finalizar, cambiar configuración de tiempo de espera de equilibrador de carga **128**
- tipo de instalación
 - inicio de sesión **57**
 - seleccionar **57**
- trabajo de DEM, conectar a SCVMM **94**

V

- validación de certificados **133**
- vCloud Suite, licencia **7**
- Visual Basic, requisitos de creación de scripts **114**
- Visual Basic Scripting
 - instalar agentes de EPI **115**
 - instalar el agente de EPI **114**
- VMware IaaS, Sitio Web de IaaS **15**
- VMware Identity Manager **131**
- vRealize Appliance
 - configurar **52**
 - implementar **31, 50**
- vRealize Orchestrator, usar externo para implementaciones de alta disponibilidad **61**

W

- WAPI, error de instalación **135**

X

- XenDesktop
 - instalar agente **109**

- instalar agente de VDI **107**
- requisitos de instalación **107**
- XenServer
 - agente **103**
 - agente de proxy **103**