

Instalación de vRealize Automation

21 de julio de 2021

vRealize Automation 7.6

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

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

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

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

Copyright © 2014-2021 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Instalación de vRealize Automation 7

Información actualizada 8

1 Descripción de la instalación 9

- Acerca de la instalación 9
- Novedad en esta instalación 10
- Componentes de instalación 10
 - El dispositivo de vRealize Automation 10
 - infraestructura como servicio 11
- Tipo de implementación 14
 - Implementaciones mínimas 14
 - Implementaciones distribuidas 15
- Elegir el método de instalación 18

2 Preparar la instalación 19

- Preparación general 19
- Cuentas y contraseñas 20
- Nombres de host y direcciones IP 22
- Latencia y ancho de banda 23
- Dispositivo de vRealize Automation 23
 - Puertos de dispositivo de vRealize Automation 24
- Servidores de Windows de IaaS 26
 - Puertos en servidores de Windows de IaaS 28
- Servidor web de IaaS 29
- Host de Manager Service de IaaS 30
- Host de SQL Server en IaaS 31
- Host de Distributed Execution Manager de IaaS 32
 - Los trabajos de DEM con Amazon Web Services 32
 - Trabajos de DEM con Openstack o PowerVC 32
 - Trabajos de DEM con Red Hat Enterprise Virtualization 33
 - Trabajos de DEM con SCVMM 33
- Certificados 35
 - Requisitos de los certificados de vRealize Automation 36
 - Extraer certificados y claves privadas 37

3 Implementar el dispositivo de vRealize Automation 39

- Acerca de la implementación del dispositivo 39

Implementar el dispositivo de vRealize Automation	39
Añadir controladores de interfaz de red antes de ejecutar el instalador	43

4 Instalación con el Asistente de instalación 45

Usar el asistente de instalación en implementaciones mínimas	45
Iniciar el asistente de instalación para una implementación mínima	45
Instalar el agente de administración	46
Completar el asistente de instalación	48
Usar el asistente de instalación en implementaciones empresariales	48
Iniciar el asistente de instalación para una implementación empresarial	49
Instalar el agente de administración	50
Completar el asistente de instalación	52

5 Las interfaces estándar de instalación 53

Usar interfaces estándar en implementaciones mínimas	53
Lista de comprobación de implementación mínima	54
Configurar el dispositivo de vRealize Automation	54
Instalar componentes de IaaS	58
Usar interfaces estándar para implementaciones distribuidas	65
Lista de comprobación de implementación distribuida	65
Deshabilitar las comprobaciones de estado del equilibrador de carga	66
Requisitos de confianza de certificados en una implementación distribuida	67
Configurar certificados de confianza para los hosts de componentes web, Manager Service y DEM	69
Hojas de trabajo de instalación	70
Configurar el equilibrador de carga	73
Configurar dispositivos para vRealize Automation	73
Instalar los componentes de IaaS en una configuración distribuida	80
Instalación de agentes	112
Establecer la política de ejecución de PowerShell en RemoteSigned	112
Elegir un escenario de instalación de agentes	113
Ubicación y requisitos de instalación de agentes	114
Instalar y configurar el agente de proxy de vSphere	114
Instalar el agente de proxy de Hyper-V o XenServer	120
Instalar el agente de VDI de XenDesktop	125
Instalar el agente de EPI de Citrix	129
Instalar el agente de EPI de Visual Basic Scripting	133
Instalar el agente de WMI para solicitudes de WMI remotas	137

6 Instalación silenciosa 141

Acerca de la instalación silenciosa	141
Realizar una instalación silenciosa	142

Realizar una instalación silenciosa del agente de administración	142
Archivo de respuesta de la instalación silenciosa	144
La línea de comando de instalación	145
Principios básicos de la línea de comandos de instalación	145
Nombres de comando de instalación	146
La API de instalación	146
Convertir entre las propiedades silenciosas y JSON	148

7 Tareas posteriores a la instalación 149

No cambiar la zona horaria	149
Configurar el cifrado compatible con FIPS	150
Habilitar la conmutación por error automática de Manager Service	151
Acerca de la conmutación por error automática de Manager Service	151
Conmutación por error automática de una base de datos de PostgreSQL	152
Reemplazar los certificados autofirmados por certificados proporcionados por una entidad	153
Cambiar nombres de host y direcciones IP	153
Cambiar el nombre de host del dispositivo	153
Cambiar la dirección IP del dispositivo	154
Ajuste de la base de datos SQL para un nombre de host modificado	156
Cambiar una dirección IP del servidor de IaaS	156
Cambiar un nombre de host del servidor de IaaS	158
Establecer la URL de inicio de sesión como un nombre personalizado	160
Eliminar un nodo de dispositivo de vRealize Automation	161
Instalar el agente de vRealize Log Insight	161
Cambiar el puerto de proxy de VMware Remote Console	161
Cambiar el FQDN de un dispositivo por el FQDN original	162
Configurar grupo de disponibilidad AlwaysOn de SQL	163
Añadir controladores de interfaz de red después de instalar vRealize Automation	163
Configurar rutas estáticas	165
Acceder a la administración de revisiones	166
Configurar el acceso al tenant predeterminado	167

8 Solucionar problemas de instalación 169

Revertir una instalación fallida	169
Revertir una instalación mínima	169
Revertir una instalación distribuida	170
Crear un paquete de soporte	171
Solucionar problemas de instalación general	172
Error de tiempo de espera agotado de un equilibrador de carga al instalar o actualizar	173
Horas de servidor no sincronizadas	173
Pueden aparecer páginas en blanco al utilizar Internet Explorer 9 o 10 en Windows 7	174

No se puede establecer una relación de confianza para el canal seguro SSL/TLS	174
Conectarse a la red mediante un servidor proxy	175
Pasos de la consola para la configuración de contenido inicial	176
No se pueden degradar licencias de vRealize Automation	177
Solucionar problemas del dispositivo vRealize Automation	177
Error de descarga de los instaladores	177
El archivo Encryption.key tiene permisos incorrectos	178
Identity Manager para la gestión de directorios no puede iniciarse tras el reinicio de Horizon-Workspace	179
Asignaciones incorrectas de la función del dispositivo tras una conmutación por error	180
Problemas después de la promoción de los nodos de réplica y principales	181
Registros de servicios de componentes incorrectos	182
Una NIC adicional provoca errores en la interfaz de administración	184
No se puede promocionar un dispositivo virtual secundario a principal	185
El tiempo de retención del log de sincronización de Active Directory es demasiado corto	185
RabbitMQ no puede resolver nombres de host	186
Solucionar problemas con componentes de IaaS	187
Se rechazan las conexiones del coordinador de transacciones distribuidas	187
Los servidores de IaaS parecen estar desconectados	188
El Comprobador de requisitos previos no puede instalar funciones .NET	189
Validar certificados de servidor para IaaS	190
Error de credenciales al ejecutar el instalador de IaaS	190
Se muestra una advertencia de configuración no guardada durante la instalación de IaaS	191
Error al instalar el servidor de sitios web y Distributed Execution Managers	191
La autenticación de IaaS genera un error durante la instalación de administración de modelo y web de IaaS	192
Error al instalar los componentes web y Model Manager Data	192
Los servidores de IaaS de Windows no admiten FIPS	194
Error interno al añadir un endpoint de XaaS	194
Error al desinstalar un agente de proxy	195
Error de solicitudes de máquinas cuando las transacciones remotas están deshabilitadas	195
Error en la comunicación de Manager Service	197
El comportamiento de personalización de correo electrónico ha cambiado	197
Solucionar problemas de errores de inicio de sesión	198
Error sin explicación al intentar iniciar sesión como administrador de IaaS con credenciales con formato de UPN incorrecto	198
Errores de inicio de sesión con alta disponibilidad	199
El proxy impide el inicio de sesión de un usuario de VMware Identity Manager	200

Instalación de vRealize Automation

Esta guía para la *Instalación de vRealize Automation* contiene instrucciones para realizar instalaciones silenciosas, manuales o con asistente de 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.

Información actualizada

En la siguiente tabla se enumeran los cambios realizados en *Instalación de vRealize Automation* de esta versión de producto.

Revisión	Descripción
XX TBD 202X	<ul style="list-style-type: none">■ Se actualizó Instalación del agente de administración de vRealize Automation.■ Se actualizó Habilitar la conmutación por error automática de Manager Service.■ Se actualizó Registros de servicios de componentes de vRealize Automation incorrectos.
12 de agosto de 2020	Se actualizó Extraer certificados y claves privadas .
14 de febrero de 2020	<ul style="list-style-type: none">■ Se actualizó Servidores de Windows de IaaS.■ Se actualizó Host de Manager Service de IaaS.■ Se actualizó Host de SQL Server en IaaS.■ Se actualizó No cambiar la zona horaria de vRealize Automation.■ Se actualizó Acceder a la administración de revisiones.■ Se ha añadido Se rechazan las conexiones del coordinador de transacciones distribuidas.■ Se actualizó Error de solicitudes de máquinas cuando las transacciones remotas están deshabilitadas.
24 de octubre de 2019	Se ha añadido el recordatorio del conector a Añadir otro dispositivo de vRealize Automation al clúster .
9 de septiembre de 2019	<ul style="list-style-type: none">■ Se actualizó Dispositivo de vRealize Automation.■ Se ha añadido No cambiar la zona horaria de vRealize Automation.
14 de junio de 2019	<ul style="list-style-type: none">■ Se ha actualizado la configuración de la directiva de grupo en Cuentas y contraseñas.■ Se ha actualizado la configuración regional en inglés en Servidores de Windows de IaaS.■ Se ha añadido Los servidores de IaaS parecen estar desconectados.
30 de mayo de 2019	<ul style="list-style-type: none">■ Se ha añadido la configuración de la directiva de grupo en Cuentas y contraseñas.■ Se eliminó PowerShell 2 y se añadió la configuración regional en inglés en Servidores de Windows de IaaS.
7 de mayo de 2019	Se han corregido algunos hipervínculos.
11 de abril de 2019	Versión del documento inicial.

Descripción general de la instalación de vRealize Automation

1

vRealize Automation se puede instalar de forma que solo admita entornos mínimos de validación técnica, o bien en configuraciones empresariales distribuidas de distintos tamaños capaces de asimilar cargas de trabajo de producción. La instalación puede ser interactiva o silenciosa.

Tras la instalación, para empezar a utilizar vRealize Automation hay que personalizar la configuración de los tenants, lo que proporciona a los usuarios acceso al aprovisionamiento de autoservicio y a la administración de ciclo de vida de los servicios de nube.

Este capítulo incluye los siguientes temas:

- [Acerca de la instalación de vRealize Automation](#)
- [Novedad en esta instalación de vRealize Automation](#)
- [Componentes de instalación de vRealize Automation](#)
- [Tipo de implementación](#)
- [Elegir el método de instalación](#)

Acerca de la instalación de vRealize Automation

Puede instalar vRealize Automation de varias maneras, cada una de ellas con diferentes niveles de interactividad.

Para instalar, implemente un dispositivo de vRealize Automation y luego complete la instalación real utilizando una de las siguientes opciones:

- Un consolidado asistente de instalación basado en un navegador
- Una configuración independiente del dispositivo basada en navegador e instalaciones de Windows independientes para los componentes del servidor de IaaS
- Un programa de instalación silencioso basado en líneas de comandos que acepta información de un archivo de propiedades de respuesta
- Una API de REST de instalación que acepta datos con formato JSON

También puede instalar vRealize Automation con Lifecycle Manager. Para obtener más información, consulte la [Guía de instalación, actualización y administración de vRealize Suite Lifecycle Manager](#).

vRealize Suite Lifecycle Manager automatiza la instalación, la configuración, la actualización, la aplicación de revisiones, la administración de la configuración, la corrección de desfases y el estado desde un único panel centralizado. Haga clic aquí para instalar [vRealize Suite Lifecycle Manager](#). Lifecycle Manager proporciona a los administradores de TI de la administración de nube los recursos necesarios para centrarse en iniciativas críticas para la empresa mientras se mejoran el tiempo de consecución del valor, la confiabilidad y la coherencia.

Novedad en esta instalación de vRealize Automation

Si instaló versiones anteriores de vRealize Automation, familiarícese con los cambios en el proceso de instalación de esta versión.

- Cuando se inicia sesión después de la instalación, se abre la interfaz de administración de dispositivos de vRealize Automation en una nueva página Resumen con información sobre el sistema, el estado y las estadísticas de uso.
- La pestaña Clúster de la interfaz de administración de dispositivos de vRealize Automation ahora puede informar sobre diversas estadísticas de estado.

Para cambiar los informes de clústeres predeterminados, edite el siguiente archivo en el dispositivo de vRealize Automation.

```
/etc/vcac/validation.properties
```

Algunas opciones de configuración del archivo también afectan el estado de la página Resumen.

- Esta versión soluciona los problemas notificados como se detalla en las notas de la versión.

Componentes de instalación de vRealize Automation

Una instalación típica de vRealize Automation consiste en un dispositivo de vRealize Automation y uno o varios servidores de Windows que, juntos, proporcionan infraestructura como servicio de vRealize Automation (IaaS).

El dispositivo de vRealize Automation

El dispositivo de vRealize Automation es un dispositivo virtual preconfigurado de Linux. El dispositivo de vRealize Automation se presenta como un archivo de virtualización de código abierto que se implementa en la infraestructura virtualizada existente como vSphere.

El dispositivo de vRealize Automation realiza varias funciones principales de vRealize Automation.

- El dispositivo contiene el servidor que aloja el portal de productos de vRealize Automation, donde los usuarios inician sesión para acceder al aprovisionamiento de autoservicio y la administración de los servicios de nube.

- El dispositivo administra Single Sign-On (SSO) para la autorización y autenticación de usuarios.
- El servidor del dispositivo aloja una interfaz de administración para la configuración del dispositivo de vRealize Automation.
- El dispositivo incluye una base de datos preconfigurada de PostgreSQL que se utiliza para fines internos del dispositivo de vRealize Automation.

En las implementaciones grandes con dispositivos redundantes, las bases de datos de los dispositivos secundarios sirven a modo de réplicas para proporcionar una alta disponibilidad.

- El dispositivo incluye una instancia preconfigurada de vRealize Orchestrator. vRealize Automation utiliza flujos de trabajo y acciones de vRealize Orchestrator para ampliar sus capacidades.

Ahora se recomienda la instancia integrada de vRealize Orchestrator. No obstante, en implementaciones más antiguas o en casos especiales, es posible que los usuarios conecten vRealize Automation a un vRealize Orchestrator externo en su lugar.

- El dispositivo contiene el programa de instalación del agente de administración que puede descargarse. Todos los servidores de Windows que conforman su vRealize AutomationIaaS deben instalar el agente de administración.

El agente de administración registra los servidores de Windows 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.

infraestructura como servicio

vRealize Automation IaaS está formado por uno o varios servidores Windows que funcionan de forma conjunta para modelar y aprovisionar sistemas en infraestructuras de nubes privadas, públicas o híbridas.

Instale los componentes de IaaS de vRealize Automation en uno o varios servidores Windows físicos o virtuales. Después de la instalación, las operaciones de IaaS aparecen bajo la pestaña Infraestructura de la interfaz del producto.

IaaS está formada por los siguientes componentes, que se pueden instalar de forma conjunta o por separado, según el tamaño de la implementación.

Servidor web

El servidor web de IaaS permite la administración de la infraestructura y la creación de servicios de la interfaz de producto de vRealize Automation. El componente del servidor web se comunica con Manager Service, que proporciona actualizaciones desde Distributed Execution Manager (DEM), la base de datos de SQL Server y los agentes.

Model Manager

vRealize Automation utiliza modelos para facilitar la integración con bases de datos y sistemas externos. Los modelos implementan la lógica empresarial utilizada por DEM.

Model Manager proporciona servicios y utilidades dirigidos a la persistencia, control de versiones, protección y distribución de los elementos de modelo. Model Manager se aloja en uno de los servidores web de IaaS y se comunica con los DEM, la base de datos de SQL Server y el sitio web de la interfaz de producto.

Manager Service

Manager Service es un servicio de Windows que coordina la comunicación entre los DEM de IaaS, la base de datos de SQL Server, los agentes y SMTP. Asimismo, Manager Service se comunica con el servidor web a través de Model Manager y se debe ejecutar en una cuenta de dominio con privilegios de administrador local en todos los servidores Windows de IaaS.

A menos que haya habilitado la conmutación por error automática de Manager Service, IaaS requiere que solo haya una máquina de Windows que ejecute activamente Manager Service. En situaciones de copia de seguridad o de alta disponibilidad, puede implementar más máquinas de Manager Service, pero el método de conmutación por error manual requiere que en las máquinas de copia de seguridad el servicio esté detenido y configurado para iniciarse manualmente.

Para obtener más información, consulte [Acerca de la conmutación por error automática de Manager Service](#).

Base de datos de SQL Server

IaaS 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. La mayoría de los usuarios permite que vRealize Automation cree la base de datos durante la instalación. También puede crear la base de datos por separado según las políticas del sitio.

Distributed Execution Manager

El componente de DEM de IaaS ejecuta la lógica empresarial de los modelos personalizados mediante la interacción con la base de datos de SQL Server de IaaS, además de con bases de datos y sistemas externos. Una forma frecuente de hacerlo es instalar los DEM en el servidor Windows de IaaS que aloja a la instancia activa de Manager Service, aunque no es necesario.

Cada instancia de DEM actúa como trabajo u orquestador. Las funciones se pueden instalar en los mismos servidores o en servidores independientes.

DEM de trabajo: tiene una función para ejecutar flujos de trabajo. Se puede aumentar la capacidad utilizando varios DEM de trabajo, que se pueden instalar en los mismos servidores o en servidores independientes.

DEM orquestador: realiza las siguientes funciones de vigilancia.

- Supervisa los DEM de trabajo. Si un trabajo se detiene o pierde su conexión con Model Manager, el DEM orquestador desplaza los flujos de trabajo a otro DEM de trabajo.
- Programa los flujos de trabajo creando instancias en el momento programado.
- Garantiza que solo una instancia de un flujo de trabajo programado se ejecute en un momento determinado.

- Preprocesa los flujos de trabajo antes de que se ejecuten. El preprocesamiento incluye la comprobación de las precondiciones para los flujos de trabajo y la creación del historial de ejecución del flujo de trabajo.

El DEM orquestador activo necesita una fuerte conectividad de red al host de Model Manager. En implementaciones grandes con varios orquestadores de DEM en servidores independientes, los orquestadores secundarios actúan como copias de seguridad. Los orquestadores de DEM secundarios supervisan el orquestador de DEM activo y proporcionan redundancia y conmutación por error cuando se produce un problema con el orquestador de DEM activo. Para este tipo de configuración de conmutación por error, puede instalar el DEM orquestador activo con el host de Manager Service activo e instalar los DEM orquestadores secundarios con los hosts de Manager Service en espera.

Agentes

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

Una forma frecuente de hacerlo es instalar los agentes de vRealize Automation en el servidor Windows de IaaS que aloja la instancia activa de Manager Service, aunque no es necesario. Se puede aumentar la capacidad utilizando varios agentes, que se pueden instalar en los mismos servidores o en servidores independientes.

Agentes de proxy de virtualización

vRealize Automation crea y administra máquinas virtuales en hosts de virtualización. Los agentes de proxy de virtualización envían comandos y recopilan datos de vSphere ESX Server, XenServer, los hosts de Hyper-V y las máquinas virtuales aprovisionadas en ellos.

Un agente de proxy de virtualización se caracteriza por lo siguiente.

- Normalmente requiere privilegios de administrador en la plataforma de virtualización que administra.
- Se comunica con la instancia de Manager Service de IaaS.
- Se instala de forma independiente con su propio archivo de configuración.

La mayoría de las implementaciones de vRealize Automation instalan el agente de proxy de vSphere. Podría instalar otros agentes de proxy dependiendo de los recursos de virtualización utilizados en su sitio.

Agentes de Virtual Desktop Integration

Los agentes de Virtual Desktop Integration (VDI) PowerShell permiten la integración de vRealize Automation con sistemas de escritorio virtual externos. Los agentes de VDI necesitan privilegios de administrador en los sistemas externos.

Puede registrar máquinas virtuales aprovisionadas por vRealize Automation con XenDesktop en un Citrix Desktop Delivery Controller (DDC), que permite al usuario acceder a la interfaz web de XenDesktop desde vRealize Automation.

Agentes de integración de aprovisionamiento externo

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 EPI necesitan privilegios de administrador sobre los sistemas externos con los que interactúan.

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 de Windows, y permite administrar servidores Windows remotos desde una ubicación centralizada. El agente de WMI también permite la recopilación de datos de los servidores Windows que vRealize Automation administra.

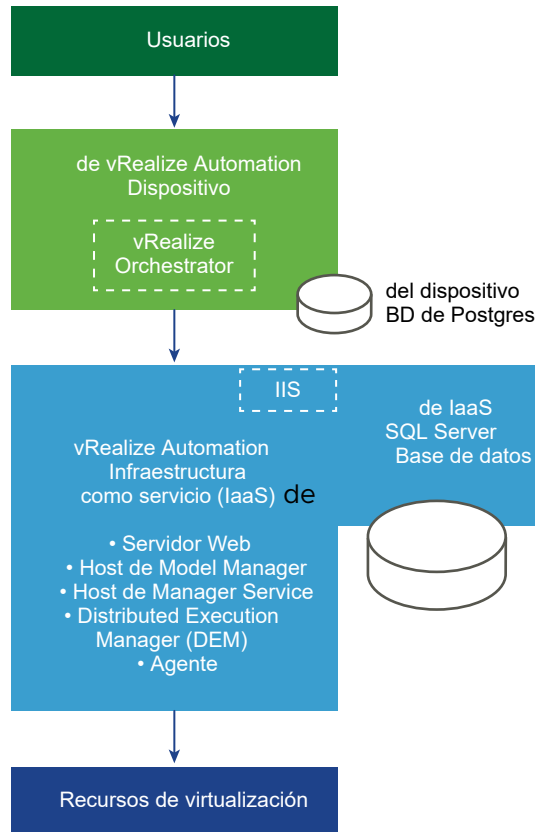
Tipo de implementación

Puede instalar vRealize Automation con una implementación mínima como prueba del concepto o como trabajo de desarrollo, o en una configuración distribuida apropiada para cargas de trabajo de producción de tamaño medio a grande.

Implementaciones mínimas de vRealize Automation

Entre las implementaciones mínimas se incluyen un dispositivo de vRealize Automation y un servidor de Windows que aloja los componentes de IaaS. En una implementación mínima, la base de datos de SQL Server de vRealize Automation puede estar en el mismo servidor de Windows de IaaS con los componentes de IaaS o en un servidor de Windows independiente.

Figura 1-1. Implementación mínima de vRealize Automation

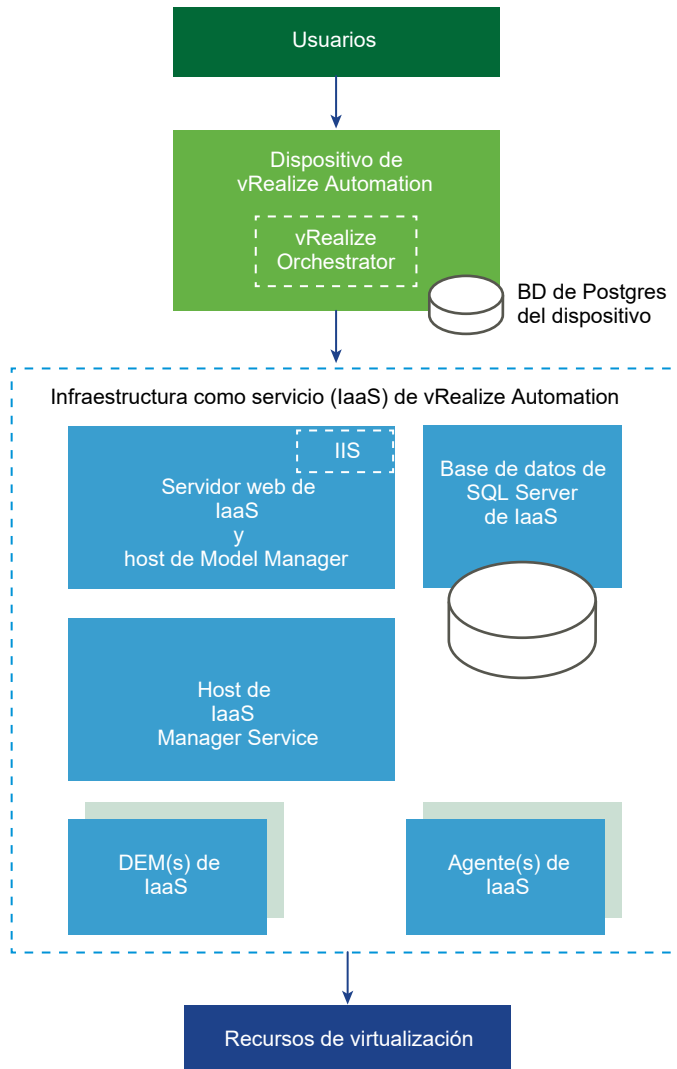


No se puede convertir una implementación mínima en una implementación empresarial. Para ampliar una implementación, comience con una implementación empresarial pequeña y añada componentes. No es posible comenzar a partir de una implementación mínima.

Implementaciones distribuidas de vRealize Automation

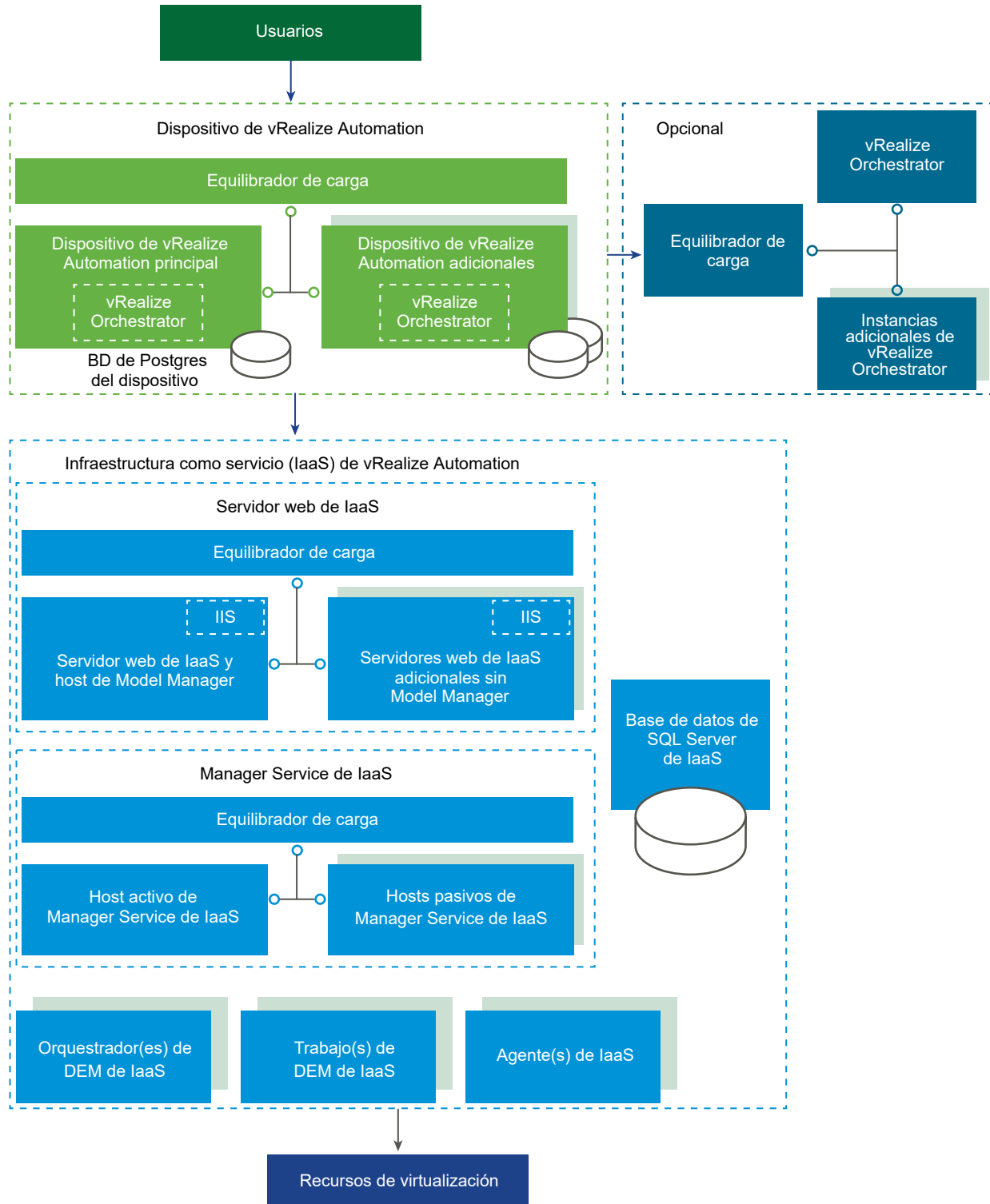
Las implementaciones empresariales distribuidas pueden tener distintos tamaños. Una implementación distribuida básica podría mejorar vRealize Automation con solo alojar los componentes de IaaS en servidores Windows independientes, como se muestra en la siguiente figura.

Figura 1-2. Implementación distribuida de vRealize Automation



Muchas implementaciones de producción van incluso más allá y hacen uso de dispositivos redundantes, servidores redundantes y equilibrio de carga para conseguir aún más capacidad. Las implementaciones grandes distribuidas proporcionan un mejor escalabilidad, alta disponibilidad y recuperación ante desastres. Observe que, aunque actualmente se recomienda integrar la instancia de vRealize Orchestrator, podría encontrar instancias de vRealize Automation conectadas a instancias de vRealize Orchestrator externas en implementaciones más antiguas.

Figura 1-3. Implementación grande distribuida y con carga equilibrada de vRealize Automation



Para obtener más información sobre escalabilidad y alta disponibilidad, consulte la guía de *arquitectura de referencia de vRealize Automation*.

Elegir el método de instalación

El asistente de instalación consolidado de vRealize Automation es su principal herramienta para las nuevas instalaciones de vRealize Automation. Como alternativa, podría realizar los procesos de instalación manual, independiente o una instalación silenciosa.

- El asistente de instalación proporciona una manera rápida y sencilla de instalar desde implementaciones mínimas hasta implementaciones empresariales distribuidas, con o sin equilibradores de carga. La mayoría de usuarios ejecutan el asistente de instalación.
- Si quiere expandir una implementación de vRealize Automation o si el asistente de instalación se ha detenido por algún motivo, necesitará los pasos manuales. Una vez que comience una instalación manual, no podrá volver y ejecutar el asistente de instalación.
- Según cuáles sean las necesidades del sitio, también podría aprovechar las ventajas de la instalación silenciosa, basada en API o en línea de comandos.

Preparar la instalación de vRealize Automation

2

vRealize Automation se instala en la infraestructura de virtualización existente. Antes de comenzar con la instalación, debe asegurarse de cumplir ciertos requisitos del sistema y del entorno.

Este capítulo incluye los siguientes temas:

- [Preparación general](#)
- [Cuentas y contraseñas](#)
- [Nombres de host y direcciones IP](#)
- [Latencia y ancho de banda](#)
- [Dispositivo de vRealize Automation](#)
- [Servidores de Windows de IaaS](#)
- [Servidor web de IaaS](#)
- [Host de Manager Service de IaaS](#)
- [Host de SQL Server en IaaS](#)
- [Host de Distributed Execution Manager de IaaS](#)
- [Certificados](#)

Preparación general

Existen varios aspectos a tener en cuenta en toda implementación antes de instalar vRealize Automation.

Para obtener más información sobre los requisitos del entorno de alto nivel, incluidos los sistemas operativos compatibles y las versiones de navegador, consulte la [matriz de compatibilidad de vRealize Automation](#).

Navegadores web del usuario

No se admite el uso de varias pestañas y ventanas del navegador. vRealize Automation admite una sesión por usuario.

VMware Remote Console incluido en vSphere solo admite un subconjunto de navegadores compatibles con vRealize Automation.

Software de terceros

Todo el software de terceros debe tener los parches más recientes del proveedor. El software de terceros incluye Microsoft Windows y SQL Server.

Sincronización de hora

Todos los dispositivos de vRealize Automation y servidores de Windows de IaaS se deben sincronizar con el mismo origen de hora. Solo puede utilizar uno de los siguientes orígenes. No combine orígenes de hora.

- El host del dispositivo de vRealize Automation
- Un servidor externo de protocolo de hora de red (NTP)

Para utilizar el host del dispositivo de vRealize Automation, debe ejecutar NTP en el host ESXi. Para obtener más información sobre el cronometraje, consulte [Artículo 1318 de la base de conocimientos de VMware](#).

Seleccione el origen de hora en la página de requisitos previos de instalación del Asistente de instalación.

Cuentas y contraseñas

Puede que deba crear o planificar una configuración para algunas cuentas de usuario y contraseñas antes de instalar vRealize Automation.

Cuenta de servicio de IaaS

IaaS instala varios servicios de Windows que se deben ejecutar en una sola cuenta de usuario.

- La cuenta debe ser un usuario de dominio.
- No es necesario que sea un administrador de dominio, pero debe contar con un permiso de administrador local, antes de la instalación, en todos los servidores de Windows de IaaS.
- La contraseña de la cuenta no puede contener un carácter de comillas dobles ("").
- El instalador del agente de administración de los servidores de Windows de IaaS solicita las credenciales de la cuenta.
- La cuenta debe tener el permiso de **inicio de sesión como servicio**, lo que permite que Manager Service se inicie y genere archivos de log.
- La cuenta debe tener un permiso de dbo en la base de datos de IaaS.

Si utiliza el instalador para crear la base de datos, agregue el inicio de sesión de la cuenta en SQL Server antes de la instalación. El instalador concede el permiso de dbo después de crear la base de datos.

- Si utiliza el instalador para crear la base de datos de SQL, agregue la función de administrador del sistema a la cuenta antes de la instalación.

La función de administrador del sistema no es necesaria si decide utilizar una base de datos vacía ya existente.

- Si el sitio usa la configuración de seguridad de la directiva de grupo, compruebe los siguientes ajustes de la cuenta. Ejecute el editor de directivas de grupo gpedit.msc y busque en **Configuración del equipo > Configuración de Windows > Configuración de seguridad > Directivas locales > Asignación de derechos de usuario**.
 - Denegar el inicio de sesión local: no añada la cuenta.
 - Permitir inicio de sesión local: añada la cuenta.
 - Denegar el acceso a este equipo desde la red: no añada la cuenta.
 - Acceder a este equipo desde la red: añada la cuenta.

Identidad del grupo de aplicaciones de IIS

La cuenta que utiliza como identidad del grupo de aplicaciones de IIS para el servicio web de Model Manager debe tener el permiso de **inicio de sesión como trabajo por lotes**.

Credenciales de la base de datos de IaaS

Puede dejar que el instalador de vRealize Automation cree la base de datos o puede crearla por separado con SQL Server. Cuando el instalador de vRealize Automation crea la base de datos, se aplican los siguientes requisitos.

- Para el instalador de vRealize Automation, si selecciona la autenticación de Windows, la cuenta que ejecuta el agente de administración en el servidor web principal de IaaS debe tener la función de administrador del sistema en SQL para crear y modificar el tamaño de la base de datos.
- Para el instalador de vRealize Automation, incluso si no selecciona la autenticación de Windows, la cuenta que ejecuta el agente de administración en el servidor web de IaaS principal debe tener la función de administrador del sistema en SQL porque las credenciales se usan en tiempo de ejecución.
- Si crea la base de datos por separado, las credenciales del usuario de Windows o del usuario de SQL que proporcione solo necesitan el permiso de dbo en la base de datos.

Frase de contraseña de seguridad de la base de datos de IaaS

La frase de contraseña de seguridad de la base de datos genera una clave de cifrado que protege los datos en la base de datos SQL de IaaS. Especifique la frase de contraseña de seguridad en la página Host de IaaS del Asistente de instalación.

- Prevea utilizar la misma frase de contraseña de seguridad de la base de datos en toda la instalación para que cada componente tenga la misma clave de cifrado.

- Registre la frase de contraseña, ya que la necesitará para restaurar la base de datos si se produce un error o se agregan componentes tras la instalación inicial.
- La frase de contraseña de seguridad de la base de datos no puede contener un carácter de comillas dobles ("). La frase de contraseña se aceptaría al crearla, pero provocaría un error en la instalación.

Endpoints de vSphere

Si prevé aprovisionar un endpoint de vSphere, necesita un dominio o una cuenta local con suficientes permisos para realizar operaciones en el destino. La cuenta también necesita el nivel de permiso apropiado configurado en vRealize Orchestrator.

Contraseña de administrador de vRealize Automation

Tras la instalación, la contraseña del administrador de vRealize Automation le permite iniciar sesión en el tenant predeterminado. Especifique la contraseña del administrador en la página Single Sign-On del Asistente de instalación.

La contraseña de administrador de vRealize Automation no puede contener el carácter de igual (=). La contraseña se acepta cuando la crea, pero más tarde produce errores cuando realiza determinadas operaciones, como guardar endpoints.

Nombres de host y direcciones IP

vRealize Automation requiere que denomine a los hosts de su instalación según determinados requisitos.

- Todas las máquinas de vRealize Automation de su instalación deben poder resolver el nombre de dominio completo (FQDN) de cada una.

Cuando realice la instalación, introduzca siempre el FQDN completo al identificar o seleccionar una máquina con vRealize Automation. No escriba direcciones IP o nombres de máquina cortos.

- Además del requisito de FQDN, las máquinas de Windows que alojan el servicio web de Model Manager, Manager Service y la base de datos de Microsoft SQL Server deben poder resolver el nombre del nombre del Servicio WINS de cada una de ellas.

Configure su sistema de nombre de dominio (DNS) para resolver estos nombres breves de host WINS.

- Planifique la nomenclatura de dominios y máquinas de forma tal que los nombres de las máquinas de vRealize Automation comiencen con letras (a-z, A-Z), terminen con letras o números (0-9) y tengan solo letras, dígitos o guiones (-) en el centro. El guion bajo (_) no debe aparecer en el nombre del host ni debe formar parte del FQDN.

Para obtener más información sobre los nombres que se permiten, revise las especificaciones para los nombres de host del Grupo de trabajo de ingeniería de Internet (Internet Engineering Task Force, IETF). Consulte www.ietf.org.

- En general, deberá mantener los nombres de host y los FQDN que haya planificado para los sistemas vRealize Automation. No siempre se puede cambiar un nombre de host. Cuando es posible, puede resultar un procedimiento complicado.
- Se recomienda reservar y utilizar direcciones IP estáticas para todos los dispositivos de vRealize Automation y los servidores de Windows de IaaS. vRealize Automation admite DHCP, pero se recomiendan las direcciones IP estáticas en implementaciones a largo plazo, como entornos de producción.
 - Debe aplicar una dirección IP en el dispositivo de vRealize Automation durante una implementación de OVF o de OVA.
 - Para los servidores Windows de IaaS, siga el procedimiento habitual del sistema operativo. Configure la dirección IP antes de instalar IaaS de vRealize Automation.

Latencia y ancho de banda

vRealize Automation admite la instalación distribuida en varios sitios, pero el volumen y la velocidad en la transmisión de datos deben cumplir unos requisitos previos mínimos.

vRealize Automation necesita un entorno con una latencia de red de 5 ms o inferior y un ancho de banda de 1 GB o superior, entre los siguientes componentes.

- Dispositivo de vRealize Automation
- Servidor web de IaaS
- Host de Model Manager de IaaS
- Host de Manager Service de IaaS
- Base de datos de SQL Server de IaaS
- Orquestador de DEM de IaaS

El siguiente componente podría funcionar en un sitio con una latencia más alta, pero no se recomienda esta práctica.

- Trabajo de DEM de IaaS

Puede instalar el siguiente componente en el sitio del endpoint con el que se comunica.

- Agente de proxy de IaaS

Dispositivo de vRealize Automation

La mayoría de los requisitos del dispositivo de vRealize Automation están preconfigurados en el archivo OVF u OVA que se implementa. Los mismos requisitos se aplican a los dispositivos de vRealize Automation independientes, principales o de réplica.

El hardware mínimo para la máquina virtual en el que puede realizar la implementación es la versión 7, o ESX/ESXi 4.x o posterior. Consulte [Artículo 2007240 de la base de conocimientos de VMware](#). Debido a la demanda de recursos de hardware, no implemente en VMware Workstation.

El dispositivo ejecuta SUSE Linux Enterprise 11 de 64 bits. VMware no admite personalizaciones ni modificaciones de dispositivos. Nunca agregue, elimine ni actualice paquetes o scripts personalizados, incluido el software antivirus.

Después de la implementación, podría utilizar vSphere para ajustar la configuración del hardware del dispositivo de vRealize Automation y así poder cumplir los requisitos de Active Directory. Consulte la siguiente tabla.

Tabla 2-1. Requisitos de hardware del dispositivo de vRealize Automation para Active Directory

Dispositivo de vRealize Automation para directorios activos pequeños	Dispositivo de vRealize Automation para directorios activos grandes
<ul style="list-style-type: none"> ■ 4 CPU ■ 18 GB de memoria ■ 140 GB de almacenamiento en disco 	<ul style="list-style-type: none"> ■ 4 CPU ■ 22 GB de memoria ■ 140 GB de almacenamiento en disco

Un Active Directory pequeño tiene hasta 25.000 usuarios en la unidad organizativa que se va a sincronizar en la configuración del almacén de ID. Un Active Directory grande tiene más de 25.000 usuarios en la unidad organizativa.

Puertos de dispositivo de vRealize Automation

Los puertos del dispositivo de vRealize Automation están normalmente preconfigurados en el archivo OVF u OVA que se implementa.

El dispositivo de vRealize Automation utiliza los siguientes puertos.

Tabla 2-2. Puertos entrantes

Puerto	Protocolo	Comentarios
22	TCP	Opcional. Acceso para sesiones de SSH.
80	TCP	Opcional. Redirige a 443.
88	TCP (UDP opcional)	Autenticación Kerberos de KDC en la nube desde dispositivos móviles externos.
443	TCP	Acceso a la consola de vRealize Automation y a las llamadas API. Acceso para máquinas para descargar el agente invitado y el agente de arranque de software. Acceso para el equilibrador de carga, navegador.
4369, 5671, 5672, 25672	TCP	Mensajes de RabbitMQ.
5480	TCP	Acceso a la interfaz de administración del dispositivo virtual.

Tabla 2-2. Puertos entrantes (continuación)

Puerto	Protocolo	Comentarios
		Utilizado por el agente de administración.
5488, 5489	TCP	El dispositivo de vRealize Automation se utiliza internamente para actualizaciones.
8230, 8280, 8281, 8283	TCP	Instancia de vRealize Orchestrator interna.
8443	TCP	Acceso para el navegador. Puerto del administrador de Identity Manager a través de HTTPS.
8444	TCP	Comunicación de proxy de consola para las conexiones de VMware Remote Console de vSphere.
8494	TCP	Sincronización de clúster de servicio de contenedor
9300-9400	TCP	Acceso para las auditorías de Identity Manager.
54328	UDP	
40002, 40003	TCP	Sincronización de clúster de vIDM
8090, 8092	TCP	Se utiliza en el servicio de estado para la conexión entre nodos de vRA

Tabla 2-3. Puertos salientes

Puerto	Protocolo	Comentarios
25, 587	TCP, UDP	SMTP para enviar correos electrónicos de notificación salientes.
53	TCP, UDP	Servidor 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.
88, 464, 135	TCP, UDP	Controlador de dominio.
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.
389	TCP	Acceso a View Connection Server.
389, 636, 3268, 3269	TCP	Active Directory. Se muestran los puertos predeterminados, pero se pueden configurar.
443	TCP	Comunicación con IaaS Manager Service y con los hosts de endpoint de infraestructura sobre HTTPS.
		Comunicación con el servicio del software vRealize Automation a través de HTTPS.
		Acceso al servidor de actualización de Identity Manager.

Tabla 2-3. Puertos salientes (continuación)

Puerto	Protocolo	Comentarios
		Acceso a View Connection Server.
445	TCP	Acceso al repositorio de ThinApp para Identity Manager.
902	TCP	Operaciones de copia de archivo de red de ESXi y conexiones con VMware Remote Console.
5050	TCP	Opcional. Para comunicarse con vRealize Business for Cloud.
5432	TCP, UDP	Opcional. Para comunicarse con otra base de datos de PostgreSQL del dispositivo.
5500	TCP	Sistema RSA SecurID. Se muestra el puerto predeterminado, pero se puede configurar.
8281	TCP	Opcional. Para comunicarse con una instancia de vRealize Orchestrator externa.
8494	TCP	Sincronización de clúster de servicio de contenedor
9300-9400	TCP	Acceso para las auditorías de Identity Manager.
54328	UDP	
40002, 40003	TCP	Sincronización de clúster de vIDM

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

Servidores de Windows de IaaS

Todos los servidores Windows que alojan componentes de IaaS deben cumplir ciertos requisitos. Ocúpese de los requisitos antes de ejecutar el Asistente de instalación de vRealize Automation o el instalador estándar basado en Windows.

Importante La instalación deshabilita el firewall de Windows. Si las directivas del sitio requieren el firewall de Windows, vuelva a habilitarlo después de la instalación y abra de forma individual los puertos del servidor de Windows de IaaS. Consulte [Puertos en servidores de Windows de IaaS](#).

- Coloque todos los servidores Windows de IaaS en el mismo dominio. No utilice grupos de trabajo.
- Cada servidor debe tener el siguiente hardware mínimo.
 - 2 CPU
 - 8 GB de memoria
 - 40 GB de almacenamiento en disco

Un servidor que aloja la base de datos SQL junto con los componentes de IaaS podría necesitar hardware adicional.

- Los servidores de Windows de IaaS y el host de base de datos de SQL Server deben poder resolverse mutuamente mediante el nombre NetBIOS. Si es necesario, agregue los nombres NetBIOS al archivo `/etc/hosts` en cada servidor de Windows de IaaS y el host de base de datos de SQL Server, y reinicie las máquinas.
- Debido a la demanda de recursos de hardware, no implemente en VMware Workstation.
- Instale Microsoft .NET Framework 3.5.
- Instale Microsoft .NET Framework 4.5.2 o posterior.

Hay disponible una copia de .NET en cualquier dispositivo de vRealize Automation:

<https://vrealize-automation-appliance-FQDN:5480/installer>

Si usa Internet Explorer para la descarga, asegúrese de que la configuración de seguridad mejorada no está habilitada. Desplácese hasta `res://iesetup.dll/SoftAdmin.htm` en el servidor de Windows.

- Instale Microsoft PowerShell 3.0 o 4.0, según su versión de Windows.
Tenga en cuenta que algunas actualizaciones o migraciones de vRealize Automation podrían requerir la versión más antigua o más reciente de PowerShell, además de la versión que ya está en ejecución actualmente.
- Para cualquier implementación con un tamaño superior al mínimo, establezca la configuración regional en inglés para los servidores Windows de IaaS.
- Si instala más de un componente de IaaS en el mismo servidor de Windows, planifique instalarlos en la misma carpeta de instalación. No utilice rutas de acceso diferentes.
- Los servidores de IaaS usan TLS para la autenticación, que está habilitada de forma predeterminada en algunos servidores Windows.

Algunos sitios deshabilitan TLS por motivos de seguridad, pero habrá que dejar al menos un protocolo TLS habilitado. Esta versión de vRealize Automation es compatible con TLS 1.2.

- Habilite el servicio de Coordinador de transacciones distribuidas (DTC). 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](#).

Habilite también el DTC del servidor que aloja la base de datos SQL, si es diferente a IaaS. Para obtener más información sobre cómo habilitar DTC, consulte [Artículo 2038943 de la base de conocimientos de VMware](#).

- Compruebe que se está ejecutando el servicio de inicio de sesión secundario. Si lo desea, puede detener el servicio una vez que se haya completado la instalación.

Puertos en servidores de Windows de IaaS

Los puertos en los servidores de Windows de IaaS deben configurarse antes de instalar vRealize Automation.

Abra los puertos entre todos los servidores de Windows de IaaS según las siguientes tablas. Incluya el servidor que aloja la base de datos SQL, si es independiente de IaaS. Por otro lado, si permite la política del sitio, deshabilite los firewalls entre los servidores de Windows de IaaS y SQL Server.

Tabla 2-4. Puertos entrantes

Puerto	Protocolo	Componente	Comentarios
443	TCP	Manager Service	Comunicación con los componentes IaaS y el dispositivo de vRealize Automation a través de HTTPS
443	TCP	Dispositivo de vRealize Automation	Comunicación con los componentes IaaS y el dispositivo de vRealize Automation a través de HTTPS
443	TCP	Hosts de endpoint de infraestructura	Comunicación con los componentes IaaS y el dispositivo de vRealize Automation a través de HTTPS. Normalmente, 443 es el puerto de comunicaciones predeterminado para los hosts de endpoint de infraestructura virtual y de nube, pero consulte la documentación suministrada por sus hosts de infraestructura para obtener una lista completa de los puertos predeterminados o requeridos.
443	TCP	Agente invitado agente de arranque de software	Comunicación con Manager Service sobre HTTPS.
443	TCP	trabajo de DEM	Comunicación con NSX Manager
1433	TCP	Instancia de SQL Server	MSSQL.

Tabla 2-5. Puertos salientes

Puerto	Protocolo	Componente	Comentarios
53	TCP, UDP	Todo	DNS.
67, 68, 546, 547	TCP, UDP	Todo	DHCP
123	TCP, UDP	Todo	Opcional. NTP
443	TCP	Manager Service	Comunicación con el dispositivo de vRealize Automation a través de HTTPS
443	TCP	Distributed Execution Managers	Comunicación con Manager Service sobre HTTPS.
443	TCP	Agentes de proxy	Comunicación con Manager Service y con los hosts de endpoint de infraestructura sobre HTTPS.

Tabla 2-5. Puertos salientes (continuación)

Puerto	Protocolo	Componente	Comentarios
443	TCP	Agente de administración	Comunicación con el dispositivo de vRealize Automation
443	TCP	Agente invitado agente de arranque de software	Comunicación con Manager Service sobre HTTPS.
1433	TCP	Manager Service Sitio web	MSSQL.
5480	TCP	Todo	Comunicación con el dispositivo de vRealize Automation

Además, al habilitar DTC entre todos los servidores, DTC requiere el puerto 135 en TCP y un puerto aleatorio entre 1024 y 65535. Tenga en cuenta que el Comprobador de requisitos previos valida que DTC se está ejecutando y los puertos necesarios están abiertos.

Servidor web de IaaS

Un servidor de Windows que aloja el componente web debe cumplir con los requisitos adicionales, además de los de todos los servidores de Windows de IaaS.

Los requisitos son los mismos, independientemente de si el componente web aloja Model Manager o no.

- Configure Java.
 - Instale la actualización 201 de Java 1.8 de 64 bits o posterior. No utilice la versión de 32 bits.
JRE es suficiente. No es necesario contar con una instancia completa de JDK.
 - Configure la variable de entorno JAVA_HOME en la carpeta de instalación de Java.
 - Compruebe que %JAVA_HOME%\bin\java.exe esté disponible.
- Configure Internet Information Services (IIS) según la tabla siguiente.
Necesita IIS 7.5 para variantes de Windows 2008, IIS 8 para Windows 2012, IIS 8.5 para Windows 2012 R2 e IIS 10 para Windows 2016.

Además de las opciones de configuración, evite alojar otros sitios web en IIS. vRealize Automation establece el enlace en su puerto de comunicación en todas las direcciones IP sin asignar, de forma que sea imposible establecer enlaces adicionales. El puerto de comunicación predeterminado de vRealize Automation es 443.

Tabla 2-6. IaaS Internet Information Services

Componente de IIS	Configuración
funciones de Internet Information Services (IIS)	<ul style="list-style-type: none"> ■ Autenticación de Windows ■ Contenido estático ■ Documento predeterminado ■ ASPNET 3.5 y ASPNET 4.5 ■ Extensiones ISAPI ■ Filtro ISAPI
Funciones de Servicio de activación de procesos de Windows de IIS	<ul style="list-style-type: none"> ■ API de configuración ■ Entorno de red ■ Modelo de proceso ■ Activación WCF (solo variantes de Windows 2008) ■ Activación HTTP ■ Activación no HTTP (solo variantes de Windows 2008) <p>(Variantes de Windows 2012: vaya a Características > Características de .Net Framework 3.5 > Activación no HTTP)</p>
Configuración de autenticación de IIS	<p>Establezca los siguientes valores no predeterminados.</p> <ul style="list-style-type: none"> ■ Autenticación de Windows habilitada ■ Autenticación anónima deshabilitada <p>No cambie los siguientes valores predeterminados.</p> <ul style="list-style-type: none"> ■ Proveedor Negotiate habilitado ■ Proveedor NTLM habilitado ■ Modo kernel de autenticación de Windows habilitado ■ Protección ampliada de autenticación de Windows deshabilitada ■ Para los certificados que usan SHA512, TLS1.2 debe estar deshabilitado en las variantes de Windows 2012.

Host de Manager Service de IaaS

Un servidor Windows que aloja el componente de Manager Service debe cumplir algunos requisitos adicionales, además de los comunes a todos los servidores Windows de IaaS.

No puede haber ningún firewall entre un host de Manager Service y el host de DEM. Para obtener información sobre el puerto, consulte [Puertos en servidores de Windows de IaaS](#).

Los requisitos son los mismos tanto si el host de Manager Service es una instancia principal o una copia de seguridad.

Host de SQL Server en IaaS

Un servidor de Windows que aloja la base de datos SQL en IaaS debe cumplir ciertos requisitos.

La instancia de SQL Server puede residir en uno de los servidores de Windows de IaaS o en un host independiente. Si se aloja junto con los componentes de IaaS, estos requisitos se añaden a los de todos los servidores Windows de IaaS.

- Esta versión de vRealize Automation no es compatible con el modo de compatibilidad 130 de SQL Server 2016 predeterminado. Si crea una base de datos SQL Server 2016 vacía por separado para usarla con IaaS, use el modo de compatibilidad 100 o 120.

Si crea la base de datos mediante el instalador de vRealize Automation, la compatibilidad ya está configurada.

El mismo comportamiento también se aplica a SQL Server 2017.

- El grupo de disponibilidad AlwaysOn (AlwaysOn Availability Group, AAG) solo es compatible con SQL Server 2016 Enterprise o SQL Server 2017 Enterprise. Cuando se utilice AAG, especifique el FQDN del agente de escucha de AAG como el host de SQL Server. Al crear el AAG, establezca `DTC_Support = Per_DB`. No se podrá establecer después de crear el AAG.
- Si se aloja junto con los componentes de IaaS, debe configurar Java.
 - Instale la actualización 201 de Java 1.8 de 64 bits o posterior. No utilice la versión de 32 bits.
JRE es suficiente. No es necesario contar con una instancia completa de JDK.
 - Configure la variable de entorno `JAVA_HOME` en la carpeta de instalación de Java.
 - Compruebe que `%JAVA_HOME%\bin\java.exe` esté disponible.
- Use una versión de SQL Server compatible de la [matriz de compatibilidad de vRealize Automation](#).
- Habilite el protocolo TCP/IP para SQL Server.
- SQL Server incluye una base de datos de modelo que sirve de plantilla para todas las bases de datos creadas en la instancia de SQL. Para que IaaS se instale correctamente, no cambie el tamaño de la base de datos de modelo.
- Por lo general, el servidor requiere más hardware que los requisitos mínimos descritos en [Servidores de Windows de IaaS](#).
Para obtener más información, consulte *Especificaciones de hardware y valores máximos de capacidad* en la guía de vRealize Automation *Arquitectura de referencia*.
- Antes de ejecutar el instalador de vRealize Automation, debe identificar las cuentas y agregar permisos en SQL. Consulte [Cuentas y contraseñas](#).

Host de Distributed Execution Manager de IaaS

Un servidor Windows que aloja el componente de orquestador o trabajo de Distributed Execution Manager (DEM) debe cumplir algunos requisitos adicionales, además de los comunes a todos los servidores Windows de IaaS.

No debe haber ningún firewall entre un host de DEM y un host de Manager Service. Para obtener información sobre el puerto, consulte [Puertos en servidores de Windows de IaaS](#).

Es posible que el trabajo de DEM tenga otros requisitos en función de los recursos de aprovisionamiento con los que interactúen.

Los trabajos de DEM con Amazon Web Services

Un trabajo de DEM de IaaS de vRealize Automation que se comunica con Amazon Web Services (AWS) debe cumplir unos requisitos adicionales, además de los comunes a todos los servidores Windows de IaaS y DEM.

Un trabajo de DEM se puede comunicar con AWS para el aprovisionamiento. El trabajo de DEM se comunica con una cuenta de Amazon EC2 y recopila datos de ella.

- El trabajo de DEM debe tener acceso a Internet.
- Si el trabajo de DEM está detrás de un firewall, se debe permitir el tráfico HTTPS a `aws.amazon.com` y desde él, así como a las direcciones URL de las regiones de EC2 a las que tienen acceso sus cuentas de AWS, como `ec2.us-east-1.amazonaws.com` para la región del este de EE. UU.

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.

- Si el trabajo de DEM llega a Internet a través de un servidor proxy, el servicio DEM se debe ejecutar con credenciales que pueda autenticar este servidor.

Trabajos de DEM con Openstack o PowerVC

Un trabajo de DEM de IaaS de vRealize Automation que comunica con Openstack o PowerVC y recopila datos de estas soluciones debe cumplir requisitos adicionales, además de los de todos los servidores Windows de IaaS y DEM en general.

Tabla 2-7. requisitos de trabajo DEM con Openstack y PowerVC

Su instalación	Requisitos
Todo	<p>En el Registro de Windows, habilite la compatibilidad de TLS v1.2 con .NET Framework. Por ejemplo:</p> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre>
Host DEM en Windows 2008	<p>En el Registro de Windows, habilite el protocolo TLS v1.2. Por ejemplo:</p> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre>
Certificados autofirmados en el host de endpoint de infraestructuras	<p>Si la instancia de PowerVC u OpenStack no usa certificados de confianza, importe el certificado SSL de la instancia de PowerVC u OpenStack en el almacén de entidades emisoras raíz de confianza en cada uno de los servidores Windows de IaaS donde tenga previsto instalar un DEM de vRealize Automation.</p>

Trabajos de DEM con Red Hat Enterprise Virtualization

Un trabajo de DEM de IaaS de vRealize Automation que comunica con Red Hat Enterprise Virtualization (RHEV) y recopila datos de esta solución debe cumplir con requisitos adicionales, además de los de todos los servidores de Windows de IaaS y DEM en general.

- Cada entorno de RHEV se debe unir al dominio que contiene el servidor de trabajo de DEM.
- Las credenciales utilizadas para administrar el endpoint que representa un entorno de RHEV deben tener privilegios de administrador en el entorno de RHEV. Cuando se utiliza RHEV para el aprovisionamiento, el trabajo de DEM comunica con dicha cuenta y recopila datos de ella.
- Las credenciales también deben tener suficientes privilegios para crear objetos en los hosts en el mismo entorno.

Trabajos de DEM con SCVMM

Un trabajo de DEM de IaaS de vRealize Automation que administra las máquinas virtuales a través de System Center Virtual Machine Manager (SCVMM) debe cumplir con los requisitos adicionales, además de los de todos los servidores de Windows de IaaS y DEM en general.

- Instale el trabajo de DEM en la misma máquina con la consola de SCVMM.

Una práctica recomendada consiste en instalar la consola de SCVMM en un trabajo de DEM distinto.

- El trabajo de DEM debe tener acceso al módulo PowerShell de SCVMM instalado con la consola.
- La política de ejecución de PowerShell debe estar establecida en RemoteSigned o Unrestricted.

Para comprobar 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 trabajos de DEM en la instancia no están en máquinas que cumplan estos requisitos, utilice comandos Skill para dirigir flujos de trabajo relacionados con SCVMM a los trabajos de DEM que lo estén.

vRealize Automation no admite un entorno de implementación en el que se use una configuración de nube privada de SCVMM. Actualmente vRealize Automation no puede recopilar realizar asignaciones a nubes privadas de SCVMM ni recopilar o aprovisionar de ellas.

Los siguientes requisitos adicionales también se aplican a SCVMM.

- vRealize Automation admite SCVMM 2012 R2, que requiere PowerShell 3 o posterior.
- Instale la consola de SCVMM antes de instalar los trabajos de DEM de vRealize Automation que consumen los elementos de trabajo de SCVMM.

Si instala el trabajo de DEM antes que la consola de SCVMM, verá errores de log similares al siguiente ejemplo.

```
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. Compruebe la ortografía del nombre o, si se incluyó
una ruta, compruebe que la ruta sea correcta e inténtelo de nuevo.
```

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

- 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.

Las credenciales también deben tener privilegios de administrador en los servidores de Hyper-V en la instancia.

- Para aprovisionar máquinas en un recurso de SCVMM, el usuario de vRealize Automation que solicita el elemento del catálogo debe tener la función de administrador en la instancia de SCVMM.

- 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 4.5.2 o posterior debe estar instalado; y Windows Management Instrumentation (WMI) debe estar habilitado.
- Para aprovisionar una máquina Generation-2 en un recurso de SCVMM 2012 R2, debe agregar las siguientes propiedades en el blueprint.

```
Scvmm.Generation2 = true
Hyperv.Network.Type = synthetic
```

Los blueprints de Generation-2 deben tener un disco duro virtual (VHD) con datos recogidos en la página de información del blueprint. Si está en blanco, ocurrirá un error en el aprovisionamiento de Generation-2.

Para obtener más información sobre la preparación del entorno de SCVMM, consulte *Configuración de vRealize Automation*.

Certificados

vRealize Automation usa certificados SSL para poder establecer una comunicación segura entre los componentes e instancias de IaaS del 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, el soporte y los requisitos de confianza de los certificados, consulte [Artículo 2106583 de la base de conocimientos de VMware](#).

Nota vRealize Automation admite certificados SHA2. Los certificados autofirmados generados por el sistema utilizan SHA-256 con cifrado RSA. Puede que tenga que actualizar los certificados SHA2 debido a los requisitos del sistema operativo o del navegador.

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.

Cambios en el certificado si se personaliza la URL de inicio de sesión de vRealize Automation

Si desea que los usuarios inicien sesión en un nombre de URL diferente de un nombre de equilibrador de carga o dispositivo de vRealize Automation, consulte los pasos previos y posteriores a la instalación de CNAME en [Establecer la URL de inicio de sesión de vRealize Automation como un nombre personalizado](#).

Requisitos de los certificados de vRealize Automation

Al utilizar sus propios certificados con vRealize Automation, los certificados deben cumplir ciertos requisitos.

Tipos de certificados admitidos

En muchas organizaciones, los certificados son emitidos o solicitados por entidades externas de acuerdo con los requisitos de la empresa.

Los siguientes requisitos tratan el formato de identidad común y los tipos de certificados utilizados con las implementaciones típicas de vRealize Automation.

Propiedad de certificado	Requisitos
Algoritmo de hash	SHA1, SHA2, (256, 584, 512)
Algoritmo de firma	RSASSA-PKCS1_V1_5
Longitud de clave	2084, 4096

Nota No se admite la firma de RSASSA-PSS para implementaciones de vRealize Automation. La firma es la predeterminado para una entidad de certificación de Microsoft en Windows 2012 R2. La firma es un parámetro configurable, por lo que debe asegurarse de que esté configurada correctamente cuando se utilice una entidad de certificación de Microsoft.

vRealize Automation Matriz de compatibilidad de certificados

Algoritmo de hash	SHA1		SHA2-256					
Algoritmo de firma	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS	
Tamaño de clave	2048	4096	2048	4096	2048	4096	2048	4096
Compatibilidad con vRealize Automation	Compatibilidad verificada	Compatibilidad verificada	No compatible	No compatible	Compatibilidad verificada	Compatibilidad verificada	No compatible	No compatible

Algoritmo de hash	SHA2-384		SHA2-512					
Algoritmo de firma	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS	
Tamaño de clave	2048	4096	2048	4096	2048	4096	2048	4096
Compatibilidad con vRealize Automation	Compatibilidad verificada	Compatibilidad verificada	No compatible	No compatible	Compatibilidad verificada	Compatibilidad verificada	No compatible	No compatible

Extraer certificados y claves privadas

Los certificados de los dispositivos virtuales deben estar en formato PEM.

Si la entidad de certificación proporcionó un certificado en formato PFX, use OpenSSL para convertir PFX a PEM.

```
openssl pkcs12 -in path-to-pfx -out desired-path-to-pem -nodes
```

Por ejemplo:

```
openssl pkcs12 -in C:\vra-cert.pfx -out C:\vra-cert.pem -nodes
```

Es posible que se le solicite que introduzca una frase de contraseña si el certificado PFX incluía una.

Implementar el dispositivo de vRealize Automation

3

El dispositivo de vRealize Automation se suministra como un archivo de virtualización de código abierto que se puede implementar en la infraestructura virtualizada existente.

Este capítulo incluye los siguientes temas:

- [Acerca de la implementación del dispositivo de vRealize Automation](#)
- [Implementar el dispositivo de vRealize Automation](#)
- [Añadir controladores de interfaz de red antes de ejecutar el instalador](#)

Acerca de la implementación del dispositivo de vRealize Automation

Todas las instalaciones requieren la implementación de un dispositivo de vRealize Automation sin configurar antes de continuar con una de las opciones de instalación de vRealize Automation reales.

- El asistente de instalación consolidado basado en navegador.
- Una configuración del dispositivo basada en navegador e independiente, seguida de instalaciones de Windows independientes para servidores de IaaS.
- Un instalador silencioso basado en la línea de comandos que acepta entradas de un archivo de propiedades de respuesta.
- La API de REST de instalación que acepta entradas con formato JSON.

Implementar el dispositivo de vRealize Automation

Antes de que pueda utilizar cualquiera de las rutas de instalación, vRealize Automation requiere que implemente al menos un dispositivo de vRealize Automation.

Para crear el dispositivo, utilice vSphere Client para descargar e implementar una máquina virtual configurada de forma parcial desde una plantilla. Si desea crear una implementación empresarial para alta disponibilidad y conmutación por error, es posible que deba realizar el procedimiento varias veces. Por lo general, una implementación de este tipo tiene varios dispositivos de vRealize Automation detrás de un equilibrador de carga.

Requisitos previos

- Inicie sesión en vSphere Client con una cuenta que tenga permiso para implementar plantillas de OVF en el inventario.
- Descargue el archivo .ovf o el archivo .ova del dispositivo de vRealize Automation en una ubicación a la que vSphere Client pueda acceder.

Procedimiento

- 1 Seleccione la opción **Implementar plantilla de OVF** de vSphere.
- 2 Introduzca la ruta al archivo .ovf o al archivo .ova del dispositivo de vRealize Automation.
- 3 Revise los detalles de la plantilla.
- 4 Lea y acepte el contrato de licencia para el usuario final.
- 5 Introduzca una ubicación de inventario y un nombre de dispositivo.

Al implementar dispositivos, utilice un nombre diferente para cada uno de ellos y absténgase de utilizar caracteres que no sean alfanuméricos en los nombres, como guiones bajos (_).

- 6 Seleccione el host y el clúster en el que residirá el dispositivo.
- 7 Seleccione el grupo de recursos en el que residirá el dispositivo.
- 8 Seleccione el almacenamiento que alojará el dispositivo.
- 9 Seleccione un formato de disco.

Los formatos gruesos mejoran el rendimiento, mientras que los formatos finos permiten ahorrar espacio de almacenamiento.

El formato no afecta al tamaño de disco del dispositivo. Si un dispositivo necesita más espacio para los datos, añada un disco mediante vSphere después de la implementación.

- 10 En el menú desplegable, seleccione una red de destino.
- 11 Complete las propiedades del dispositivo.

- a Introduzca y confirme una contraseña raíz.

Las credenciales de la cuenta raíz le permiten iniciar sesión en la interfaz de administración basada en navegador que el dispositivo aloja, o bien en la consola de línea de comandos del sistema operativo del dispositivo.

- b Determine si desea permitir conexiones de SSH remotas a la consola de línea de comandos.

La deshabilitación de SSH ofrece más seguridad, pero requiere que se acceda a la consola directamente en vSphere en lugar de hacerlo mediante un cliente de terminal independiente.

- c En **Nombre de host**, introduzca el nombre de dominio completo del dispositivo.

Para obtener mejores resultados, escriba el nombre de dominio completo, incluso si utiliza DHCP.

Nota vRealize Automation es compatible con DHCP, pero se recomiendan las direcciones IP estáticas para las implementaciones de producción.

- d En Propiedades de red, cuando utilice direcciones IP estáticas, escriba los valores de la puerta de enlace, la máscara de red y los servidores de DNS. También debe especificar la dirección IP, el nombre de dominio completo y el dominio del dispositivo, tal como se muestra en el ejemplo siguiente.

Figura 3-1. Ejemplo de propiedades de dispositivo virtual

▼ Application	3 settings
Enable SSH service in the appliance	This will be used as an initial status of the SSH service in the appliance. You can change it later from the appliance Web console. <input checked="" type="checkbox"/>
Hostname	The host name for this virtual machine. Provide the fully qualified domain name if you use a static IP. Leave blank to try to reverse look up the IP address if you use DHCP. <input type="text" value="va1.mycompany.com"/>
Initial root password	This will be used as an initial password for the root user account. You can change the password later (by using the passwd command or from the appliance Web console). Enter password <input type="password" value="*****"/> Confirm password <input type="password" value="*****"/>
▼ Networking Properties	6 settings
Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired. <input type="text" value="12.34.56.79"/>
Domain Name	The domain name of this VM. Leave blank if DHCP is desired. <input type="text" value="mycompany.com"/>
Domain Name Servers	The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired. <input type="text" value="12.34.56.80, 12.34.56.81"/>
Domain Search Path	The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired. <input type="text" value="mycompany.com"/>
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. <input type="text" value="12.34.56.78"/>
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired. <input type="text" value="255.255.254.0"/>

- 12 En función de la configuración de DNS, la implementación y la instancia de vCenter Server, seleccione uno de los siguientes métodos para finalizar la implementación y encender el dispositivo.

- Si implementó en vSphere y la opción **Encender tras implementación** está disponible en la página Listo para completar, realice los siguientes pasos.

- a Seleccione **Encender tras implementación** y haga clic en **Finalizar**.

- b Una vez que el archivo termine de implementarse en vCenter Server, haga clic en **Cerrar**.
 - c Espere a que la máquina virtual se inicie, lo que podría tardar unos 5 minutos.
 - Si implementó en vSphere y la opción **Encender tras implementación** no está disponible en la página Listo para completar, realice los siguientes pasos.
 - a Una vez que el archivo termine de implementarse en vCenter Server, haga clic en **Cerrar**.
 - b Encienda el dispositivo de vRealize Automation.
 - c Espere a que la máquina virtual se inicie, lo que podría tardar unos 5 minutos.
 - d Para comprobar que se ha implementado el dispositivo de vRealize Automation, haga ping a su nombre de dominio completo. Si no puede hacer ping al dispositivo, reinicie la máquina virtual.
 - e Espere a que la máquina virtual se inicie, lo que podría tardar unos 5 minutos.
 - Si ha implementado el dispositivo de vRealize Automation en vCloud mediante vCloud Director, vCloud podría reemplazar la contraseña que ha introducido durante la implementación de OVA. Para evitar que esto suceda, realice estos pasos.
 - a Tras la implementación en vCloud Director, haga clic en la vApp para ver el dispositivo de vRealize Automation.
 - b Haga clic con el botón derecho en el dispositivo de vRealize Automation y seleccione **Propiedades**.
 - c Haga clic en la pestaña **Personalización del SO invitado**.
 - d En **Restablecimiento de contraseña**, borre la opción **Permitir la contraseña del administrador local** y haga clic en **Aceptar**.
 - e Encienda el dispositivo de vRealize Automation.
 - f Espere a que la máquina virtual se inicie, lo que podría tardar unos 5 minutos.
- 13** Para comprobar que se ha implementado el dispositivo de vRealize Automation, haga ping a su nombre de dominio completo.

Pasos siguientes

- (Opcional) Añada NIC. Consulte [Añadir controladores de interfaz de red antes de ejecutar el instalador](#).
- Inicie sesión en la interfaz de administración basada en navegador para ejecutar el asistente de instalación consolidado o configurar el dispositivo de forma manual.
`https://vrealize-automation-appliance-FQDN:5480`
- Opcionalmente, puede omitir el inicio de sesión para aprovechar la instalación silenciosa o basada en la API de vRealize Automation.

Añadir controladores de interfaz de red antes de ejecutar el instalador

vRealize Automation admite varios controladores de interfaz de red (Network Interface Controller, NIC). Antes de ejecutar el instalador, es posible añadir varios NIC al dispositivo de vRealize Automation o la instancia de Windows Server de IaaS.

Si necesita que varios NIC estén en posición antes de ejecutar el asistente de instalación de vRealize Automation, agréguelos después de la implementación en vCenter, pero antes de iniciar el asistente. A continuación se presentan algunas razones por las que le interesaría colocar NIC adicionales de manera anticipada:

- Desea disponer de redes de infraestructura y de usuario distintas.
- Necesita un NIC adicional para que los servidores de IaaS puedan unirse a un dominio de Active Directory.

Para obtener más información sobre escenarios con varios NIC, consulte esta [publicación de blog de VMware Cloud Management](#).

Para tres o más NIC, tenga en cuenta las siguientes limitaciones.

- VIDM necesita acceder a la base de datos de Postgres y Active Directory.
- En un clúster de alta disponibilidad, VIDM necesita acceder a la URL del equilibrador de carga.
- Las conexiones de VIDM anteriores deben proceder de los dos primeros NIC.
- Los NIC que siguen al segundo NIC no deben utilizarse ni ser reconocidos por VIDM.
- Los NIC que siguen al segundo NIC no deben utilizarse para conectarse a Active Directory.

Utilice el primer o el segundo NIC al configurar un directorio en vRealize Automation.

Requisitos previos

Implemente el OVF del dispositivo de vRealize Automation y las máquinas virtuales de Windows, pero no inicie sesión ni inicie el asistente de instalación.

Procedimiento

- 1 En vCenter, agregue los NIC a cada dispositivo de vRealize Automation.
 - a Haga clic con el botón secundario en el dispositivo recién implementado y seleccione **Editar configuración**.
 - b Agregue los NIC de VMXNETn.
 - c Si el dispositivo está encendido, reinícielo.
- 2 Inicie sesión en la línea de comandos del dispositivo de vRealize Automation como raíz.

3 Configure los NIC ejecutando el siguiente comando para cada NIC.

Asegúrese de incluir la dirección de puerta de enlace predeterminada. Puede configurar rutas estáticas tras finalizar este procedimiento.

```
/opt/vmware/share/vami/vami_set_network network-interface (STATICV4|STATICV4+DHCPV6|
STATICV4+AUTOV6) IPv4-addressnetmaskgateway-v4-address
```

Por ejemplo:

```
/opt/vmware/share/vami/vami_set_network eth1 STATICV4 192.168.100.20 255.255.255.0
192.168.100.1
```

- 4 Compruebe que todos los nodos de vRealize Automation pueden resolverse mutuamente por nombre de DNS.
- 5 Compruebe que todos los nodos de vRealize Automation pueden acceder a cualquier FQDN con equilibrio de carga para los componentes de vRealize Automation.
- 6 Si utiliza DNS de cerebro dividido, compruebe que todos los VIP y los nodos de vRealize Automation tengan el mismo FQDN en DNS para el VIP y la IP de cada nodo.
- 7 En vCenter, agregue los NIC a instancias de Windows Server de IaaS.
 - a Haga clic con el botón secundario en el servidor de IaaS y seleccione **Editar configuración**.
 - b Añada los NIC a la máquina virtual del servidor de IaaS.
- 8 En Windows, configure los NIC del servidor de IaaS agregado y sus direcciones IP. Si es necesario, consulte la documentación de Microsoft.

Pasos siguientes

- (Opcional) Si necesita rutas estáticas, siga las directrices de [Configurar rutas estáticas](#) antes de continuar con la instalación.
- Inicie sesión en la interfaz de administración basada en navegador para ejecutar el asistente de instalación consolidado o configurar el dispositivo de forma manual.

`https://vrealize-automation-appliance-FQDN:5480`
- Opcionalmente, puede omitir el inicio de sesión para aprovechar la instalación silenciosa o basada en la API de vRealize Automation.

Instalar vRealize Automation con el Asistente de instalación

4

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

Antes de ejecutar el asistente, debe implementar un dispositivo de vRealize Automation y configurar los servidores de Windows de IaaS para satisfacer los requisitos previos. El asistente de instalación aparece cuando inicia sesión por primera vez en el dispositivo de vRealize Automation recién implementado.

- Para detener el asistente y reanudarlo más adelante, haga clic en **Cerrar sesión**.
- Para deshabilitar el asistente, haga clic en **Cancelar** o cierre la sesión e inicie la instalación manual a través de las interfaces estándar.

El asistente es su principal herramienta para las nuevas instalaciones de vRealize Automation. Si desea expandir una implementación de vRealize Automation existente después de ejecutar el asistente, vea los procedimientos en [Capítulo 5 Las interfaces estándar de instalación de vRealize Automation](#).

Este capítulo incluye los siguientes temas:

- [Usar el asistente de instalación en implementaciones mínimas](#)
- [Usar el asistente de instalación en implementaciones empresariales](#)

Usar el asistente de instalación en implementaciones mínimas

Las implementaciones mínimas demuestran cómo funciona vRealize Automation, pero por lo general no tienen suficiente capacidad para admitir entornos de producción empresariales.

Instale una implementación mínima para una prueba de concepto o para familiarizarse con vRealize Automation.

Iniciar el asistente de instalación para una implementación mínima

Las implementaciones mínimas suelen consistir en un dispositivo de vRealize Automation, una instancia de servidor de Windows de IaaS y el agente de vSphere para los endpoints. Una instalación mínima coloca todos los componentes de IaaS en un único servidor de Windows.

Requisitos previos

- Ocúpese de los requisitos previos de [Capítulo 2 Preparar la instalación de vRealize Automation](#).
- Cree un dispositivo sin configurar. Consulte [Implementar el dispositivo de vRealize Automation](#).

Procedimiento

- 1 Inicie sesión como raíz en la interfaz de administración del dispositivo de vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`
- 2 Cuando aparezca el asistente de instalación, haga clic en **Siguiente**.
- 3 Acepte el acuerdo de licencia y haga clic en **Siguiente**.
- 4 En la página Tipo de implementación, seleccione **Implementación mínima e Instalar infraestructura como servicio**, y haga clic en **Siguiente**.
- 5 En la página Requisitos previos de instalación, tiene que hacer una pausa para iniciar sesión en su servidor de Windows de IaaS e instalar el agente de administración. El agente de administración permite a vRealize Automation detectar el servidor de IaaS y conectarse a él.

Pasos siguientes

Instale el agente de administración en las instancias de servidor de Windows de IaaS. Consulte [Instalación del agente de administración de vRealize Automation](#).

Instalación del agente de administración de vRealize Automation

Todos los servidores de IaaS de Windows requieren el agente de administración, que los vincula a su dispositivo de vRealize Automation específico.

Si aloja la base de datos de SQL Server de vRealize Automation en una máquina de Windows independiente que no aloje componentes de IaaS, la máquina de SQL Server no necesitará el agente de administración.

El agente de administración registra el servidor de IaaS de Windows en el dispositivo de vRealize Automation específico, automatiza la instalación y la administración de los componentes de IaaS, y recopila información de soporte y telemetría. El agente de administración se ejecuta como un servicio de Windows en una cuenta de dominio con derechos de administrador en los servidores de IaaS de Windows.

Requisitos previos

Cree un dispositivo de vRealize Automation e inicie el asistente de instalación.

Consulte [Implementar el dispositivo de vRealize Automation](#) y [Iniciar el asistente de instalación para una implementación mínima](#).

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
```
- 3 Copie la huella digital para verificarla más tarde. Por ejemplo:

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```
- 4 Inicie sesión en el servidor Windows de IaaS mediante una cuenta con derechos de administrador.
- 5 Abra un navegador web en la URL del instalador del dispositivo de vRealize Automation.

```
https://vrealize-automation-appliance-FQDN:5480/installer
```
- 6 Haga clic en el **instalador del agente de administración**, y guarde y ejecute el archivo MSI.
- 7 Lea el mensaje de bienvenida.
- 8 Acepte el contrato de licencia para el usuario final.
- 9 Acepte o cambie la carpeta de instalación.

```
Archivos de programa (x86)\VMware\vCAC\Management Agent
```
- 10 Introduzca los detalles del dispositivo de vRealize Automation:
 - a Introduzca la dirección HTTPS del dispositivo, incluidos el nombre de dominio completo y el número de puerto 5480.
 - b Introduzca las credenciales de cuenta raíz del dispositivo.
 - c Haga clic en **Cargar**, y confirme que la huella digital coincide con la que copió anteriormente. Omita los dos puntos.

Si las huellas digitales no coinciden, compruebe que la dirección del dispositivo sea correcta.

Figura 4-1. Agente de administración: detalles del dispositivo de vRealize Automation

vRA appliance address:

 Specify the scheme and the port (hosted by default on 5480). Example: https://va-address:5480
 Root username: Password:
 Provide vRealize Automation appliance root user credentials
 Management Site Service certificate SHA1 fingerprint:

☒ I confirm the fingerprint matches the Management Site Service SSL certificate

- 11 Introduzca el nombre de dominio o el nombre de usuario y la contraseña de la cuenta de servicio.

La cuenta de servicio debe ser una cuenta de dominio con derechos de administrador en los servidores de IaaS de Windows. Utilice siempre la misma cuenta de servicio.

- 12 Siga las indicaciones para finalizar la instalación del agente de administración.

Resultados

Nota Debido a que están vinculados, deberá volver a instalar al agente de administración si reemplaza el dispositivo de vRealize Automation.

La desinstalación de IaaS de un servidor de Windows no elimina el agente de administración. Para desinstalar un agente de administración, use la opción Agregar o quitar programas de Windows.

Pasos siguientes

Vuelva al asistente de instalación basado en el navegador. Los servidores de IaaS de Windows con el agente de administración instalado se muestran en Hosts detectados.

Completar el asistente de instalación

Después de instalar el agente de administración, vuelva al asistente y siga las indicaciones. Si necesita instrucciones adicionales sobre la configuración, haga clic en el vínculo de ayuda situado en la parte superior derecha del asistente.

- Cuando finalice el asistente, aparecerá en la última página la ruta de acceso y el nombre de un archivo de propiedades. Puede editar el archivo y usarlo para realizar una instalación silenciosa de vRealize Automation con una configuración idéntica o similar a la de su sesión del asistente. Consulte [Capítulo 6 Instalación silenciosa de vRealize Automation](#).
- Si ha creado usted el contenido inicial, podrá iniciar sesión en el tenant predeterminado como usuario configurationadmin y solicitar los elementos del catálogo.
- Para configurar el acceso al tenant predeterminado para otros usuarios, consulte [Configurar el acceso al tenant predeterminado](#).

Usar el asistente de instalación en implementaciones empresariales

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 varios dispositivos de vRealize Automation e instancias de servidores web activos genera errores en la instalación. Durante la instalación, solo deben estar activos una instancia de servidor web y un dispositivo de vRealize Automation.

Iniciar el asistente de instalación para una implementación empresarial

Las implementaciones empresariales son lo suficientemente grandes 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, notifíquelo 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.

Requisitos previos

- Ocúpese de los requisitos previos de [Capítulo 2 Preparar la instalación de vRealize Automation](#).
- Cree un dispositivo sin configurar. Consulte [Implementar el dispositivo de vRealize Automation](#).

Procedimiento

- 1 Inicie sesión como raíz en la interfaz de administración del dispositivo de vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`
- 2 Cuando aparezca el asistente de instalación, haga clic en **Siguiente**.
- 3 Acepte el Contrato de licencia para el usuario final y haga clic en **Siguiente**.
- 4 En la página Tipo de implementación, seleccione **Implementación empresarial** e **Instalar infraestructura como servicio**.
- 5 En la página Requisitos previos de instalación, tiene que hacer una pausa para iniciar sesión en sus servidores de Windows de IaaS e instalar el agente de administración. El agente de administración permite al dispositivo de vRealize Automation descubrir y conectarse a dichos servidores de IaaS.

Pasos siguientes

Instale el agente de administración en sus servidores de IaaS de Windows. Consulte [Instalación del agente de administración de vRealize Automation](#).

Instalación del agente de administración de vRealize Automation

Todos los servidores de Windows de IaaS requieren el agente de administración, que los vincula a su dispositivo de vRealize Automation principal.

Si aloja la base de datos de SQL Server de vRealize Automation en una máquina de Windows independiente que no aloje componentes de IaaS, la máquina de SQL Server no necesitará el agente de administración.

El agente de administración registra el servidor de Windows de IaaS en el dispositivo de vRealize Automation principal, automatiza la instalación y la administración de los componentes de IaaS, y recopila la información de soporte y telemetría. El agente de administración se ejecuta como un servicio de Windows en una cuenta de dominio con derechos de administrador en los servidores de IaaS de Windows.

Requisitos previos

Cree un dispositivo de vRealize Automation, o varios, e inicie el asistente de instalación.

Consulte [Implementar el dispositivo de vRealize Automation](#) y [Iniciar el asistente de instalación para una implementación empresarial](#).

Procedimiento

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

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```
- 3 Copie la huella digital para verificarla más tarde. Por ejemplo:

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```
- 4 Inicie sesión en el servidor Windows de IaaS mediante una cuenta con derechos de administrador.
- 5 Abra un navegador web en la URL del instalador del dispositivo de vRealize Automation principal.

```
https://vrealize-automation-appliance-FQDN:5480/installer
```
- 6 Haga clic en el **instalador del agente de administración**, y guarde y ejecute el archivo msí.
- 7 Lea el mensaje de bienvenida.
- 8 Acepte el contrato de licencia para el usuario final.
- 9 Acepte o cambie la carpeta de instalación.

```
Archivos de programa (x86)\VMware\vCAC\Management Agent
```

10 Introduzca los detalles del dispositivo de vRealize Automation principal:

- Introduzca la dirección HTTPS del dispositivo principal, incluidos el FQDN y el número de puerto 5480.
- Introduzca las credenciales de cuenta raíz del dispositivo principal.
- Haga clic en **Cargar**, y confirme que la huella digital coincide con la que copió anteriormente. Omita los dos puntos.

Si las huellas digitales no coinciden, compruebe que la dirección del dispositivo sea correcta.

Figura 4-2. Agente de administración: detalles del dispositivo de vRealize Automation

11 Introduzca el nombre de dominio o el nombre de usuario y la contraseña de la cuenta de servicio.

La cuenta de servicio debe ser una cuenta de dominio con derechos de administrador en los servidores de IaaS de Windows. Utilice siempre la misma cuenta de servicio.

12 Siga las indicaciones para finalizar la instalación del agente de administración.

Resultados

Repita el procedimiento para todos los servidores de Windows que alojarán componentes de IaaS.

Nota Debido a que están vinculados, deberá volver a instalar al agente de administración si reemplaza el dispositivo de vRealize Automation.

La desinstalación de IaaS de un servidor de Windows no elimina el agente de administración. Para desinstalar un agente de administración, use la opción Agregar o quitar programas de Windows.

Pasos siguientes

Vuelva al asistente de instalación basado en el navegador. Los servidores de IaaS de Windows con el agente de administración instalado se muestran en Hosts detectados.

Completar el asistente de instalación

Después de instalar el agente de administración, vuelva al asistente y siga las indicaciones. Si necesita instrucciones adicionales sobre la configuración, haga clic en el vínculo de ayuda situado en la parte superior derecha del asistente.

- Cuando finalice el asistente, aparecerá en la última página la ruta de acceso y el nombre de un archivo de propiedades. Puede editar el archivo y usarlo para realizar una instalación silenciosa de vRealize Automation con una configuración idéntica o similar a la de su sesión del asistente. Consulte [Capítulo 6 Instalación silenciosa de vRealize Automation](#).
- Si ha creado usted el contenido inicial, podrá iniciar sesión en el tenant predeterminado como usuario configurationadmin y solicitar los elementos del catálogo.
- Para configurar el acceso al tenant predeterminado para otros usuarios, consulte [Configurar el acceso al tenant predeterminado](#).

Las interfaces estándar de instalación de vRealize Automation

5

Tras ejecutar el asistente de instalación, es posible que necesite o quiera realizar determinadas tareas manualmente a través de las interfaces estándar.

El asistente de instalación que se describe en [Capítulo 4 Instalar vRealize Automation con el Asistente de instalación](#) es su herramienta principal para las nuevas instalaciones de vRealize Automation. Sin embargo, después de ejecutar el asistente, algunas operaciones seguirán necesitando el proceso de instalación manual anterior.

Los pasos manuales son necesarios si quiere expandir una implementación de vRealize Automation o si el asistente se ha detenido por algún motivo. Las situaciones en las que podría necesitar consultar los procedimientos de esta sección incluyen los siguientes ejemplos.

- Eligió cancelar el asistente antes de terminar la instalación.
- Se ha producido un error al instalar mediante el asistente.
- Quiere añadir otro dispositivo de vRealize Automation para obtener alta disponibilidad.
- Quiere añadir otro servidor web de IaaS para obtener alta disponibilidad.
- Necesita otro agente proxy.
- Necesita otro orquestador o trabajo de DEM.

Podría utilizar todos los procesos manuales o solo algunos de ellos. Revise el material a lo largo de esta sección y siga los procedimientos que se aplican a su situación.

Este capítulo incluye los siguientes temas:

- [Usar interfaces estándar en implementaciones mínimas](#)
- [Usar interfaces estándar para implementaciones distribuidas](#)
- [Instalar agentes de vRealize Automation](#)

Usar interfaces estándar en implementaciones mínimas

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

vRealize Automation se instala en una configuración mínima para tareas de prueba de concepto o desarrollo. En las implementaciones mínimas hay que dar menos pasos para realizar las instalaciones, pero no tienen la capacidad de producción de una implementación empresarial.

Complete las tareas de alto nivel en el siguiente orden.

Tabla 5-1. Lista de comprobación de implementación mínima

Tarea	Detalles
<input type="checkbox"/> Planifique el entorno y compruebe que los requisitos previos de instalación se cumplen.	Capítulo 2 Preparar la instalación de vRealize Automation
<input type="checkbox"/> Cree un dispositivo de vRealize Automation sin configurar.	Implementar el dispositivo de vRealize Automation
<input type="checkbox"/> Configure manualmente el dispositivo de vRealize Automation.	Configurar el dispositivo de vRealize Automation
<input type="checkbox"/> Instalar los componentes de IaaS en un solo servidor de Windows.	Instalar componentes de IaaS
<input type="checkbox"/> Instalar agentes adicionales, si corresponde.	Instalar agentes de vRealize Automation
<input type="checkbox"/> Llevar a cabo tareas posteriores a la instalación como la configuración del tenant predeterminado.	Configurar el acceso al tenant predeterminado

Configurar el dispositivo de vRealize Automation

El dispositivo de vRealize Automation es una máquina virtual configurada parcialmente que aloja el portal web de usuarios y el servidor de vRealize Automation. Descargue la plantilla del formato de virtualización abierta (Open Virtualization Format, OVF) del dispositivo e impleméntela en vCenter Server o el inventario de ESX/ESXi.

Requisitos previos

- Cree un dispositivo sin configurar. Consulte [Implementar el dispositivo de vRealize Automation](#).
- Obtenga un certificado de autenticación para el dispositivo de vRealize Automation.

Procedimiento

- 1 Inicie sesión en la interfaz de administración del dispositivo de vRealize Automation sin configurar como raíz.

`https://vrealize-automation-appliance-FQDN:5480`

Continúe aunque aparezcan advertencias de certificado.

- 2 Si aparece el asistente de instalación, cáncelo de modo que pueda ir a la interfaz de administración en su lugar.

- 3 Seleccione **Administración > Configuración horaria** y establezca el origen de sincronización de hora.

Opción	Descripción
Hora del host	Sincronización con el host ESXi del dispositivo de vRealize Automation.
Servidor de hora	Sincronización con un servidor externo de protocolo de hora de red (Network Time Protocol, NTP). Escriba el FQDN o la dirección IP del servidor NTP.

Debe sincronizar los dispositivos de vRealize Automation y las instancias de Windows Server de IaaS con el mismo origen de hora. No combine orígenes de hora dentro de una implementación de vRealize Automation.

- 4 Seleccione **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-loadbalancename.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 configurar el nombre de host.

- 5 Seleccione la acción apropiada del 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 del dispositivo de vRealize Automation y para cualquier equilibrador de carga mediante el uso de certificados de nombre alternativo del firmante (Subject Alternative Name, SAN).

Si desea generar una solicitud de CSR de un nuevo certificado que pueda enviar a una entidad de certificación, seleccione **Generar solicitud de firma**. Una CSR ayuda a la entidad de certificación a crear un certificado con los valores correctos para importarlo.

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 del host tal como aparece en la parte superior de la página. Si hay instancias adicionales disponibles del 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.
Generar solicitud de firma	<ul style="list-style-type: none"> a Seleccione Generar solicitud de firma. b Revise las entradas de los cuadros de texto Organización, Unidad organizativa, Código de país y Nombre común. Estas entradas se rellenan a partir del certificado existente. Estas entradas se pueden editar en caso necesario. c Haga clic en Generar CSR para crear una solicitud de firma de certificado y, a continuación, haga clic en el vínculo Descargar aquí la CSR generada para abrir un cuadro de diálogo y guardar la CSR en una ubicación desde donde se pueda enviar a una entidad de certificación. d Cuando reciba el certificado preparado, haga clic en Importar y siga las instrucciones para importarlo a vRealize Automation.
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. <p>Nota En el caso de certificados encadenados, puede haber atributos adicionales disponibles.</p> <ul style="list-style-type: none"> 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 Defina la configuración de SSO.
- 8 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.
- 9 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.
- 10 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.

- 11 Introduzca la información de licencia.
 - a Haga clic en **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.

- 12 Confirme que puede iniciar sesión en vRealize Automation.
 - a Abra un navegador web en la dirección URL de la interfaz de producto de vRealize Automation.
`https://vrealize-automation-appliance-FQDN/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 interfaz en la pestaña **Administración** de la página Tenants. La lista contiene un solo tenant denominado `vsphere.local`.

Resultados

Ya ha terminado la implementación y configuración de su 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.

Pasos siguientes

Consulte [Instalar los componentes de la infraestructura](#).

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](#) 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 utiliza el asistente de instalación para instalar los servicios de IaaS en la máquina física o virtual de Windows.

Requisitos previos

- Compruebe que el servidor cumple los requisitos de [Servidores de Windows de IaaS](#).
- [Habilitar la sincronización de hora en el servidor de Windows](#).
- Confirme que ha implementado y configurado por completo el dispositivo de vRealize Automation; asimismo, verifique que los servicios necesarios se están ejecutando (plugin-service, catalog-service e iaas-proxy-provider).

Procedimiento

1 [Descargar el instalador de IaaS para vRealize Automation](#)

Para instalar IaaS en el servidor de Windows físico o virtual mínimo, debe descargar una copia del instalador de IaaS desde el dispositivo de vRealize Automation.

2 [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.

3 [Comprobar los requisitos previos](#)

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

4 [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.

5 [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.

6 Registrar los componentes de IaaS

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

7 Finalizar la instalación

El administrador del sistema finaliza la instalación de IaaS.

Descargar el instalador de IaaS para vRealize Automation

Para instalar IaaS en el servidor de Windows físico o virtual mínimo, debe descargar una copia del instalador de IaaS desde el dispositivo de vRealize Automation.

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

Requisitos previos

- Revise los requisitos de Windows Server de IaaS. Consulte [Servidores de Windows de IaaS](#).
- Si usa Internet Explorer para la descarga, asegúrese de que la configuración de seguridad mejorada no está habilitada. Desplácese hasta `res://iesetup.dll/SoftAdmin.htm` en el servidor de Windows.

Procedimiento

- 1 Inicie sesión en el servidor Windows de IaaS mediante una cuenta con derechos de administrador.
- 2 Abra un navegador web directamente en la URL del instalador del dispositivo de vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480/installer`

- 3 Haga clic en **Instalador de IaaS**.
- 4 Guarde `setup__vrealize-automation-appliance-FQDN@5480` en el servidor Windows.
No modifique el nombre de archivo del instalador. Sirve para conectar la instalación con 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.

Requisitos previos

[Descargar el instalador de IaaS para vRealize Automation](#).

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.

Requisitos previos

[Seleccionar el tipo de instalación.](#)

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**.

Resultados

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.

Requisitos previos

[Comprobar los requisitos previos.](#)

Procedimiento

- 1 En las páginas **Configuración del servidor y la cuenta** o **Configuración detectada**, escriba el nombre de usuario y la contraseña de la cuenta del servicio de Windows. Esta cuenta del servicio debe ser una cuenta de administrador local que también tenga privilegios administrativos de SQL.

- 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 Para instalar la instancia de la base de datos en el mismo servidor con los componentes de IaaS, acepte el servidor predeterminado en el cuadro de texto **Servidor** en la sección de Información de instalación de la base de datos de Microsoft SQL Server.

Si la base de datos está en una máquina diferente, escriba el servidor en el siguiente formato.

FQDN-de-maquina,numero-puerto\instancia-base-de-datos-designada

- 4 Acepte el valor predeterminado del cuadro de texto **Nombre de la 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.

Se recomienda la autenticación de Windows. Cuando elija la autenticación de SQL, la contraseña de la base de datos no cifrada aparece en ciertos archivos de configuración.

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 más información sobre la configuración de SSL en SQL Server, consulte [Artículo 189067 de Microsoft TechNet](#).

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.

Requisitos previos

[Especificar la configuración de cuenta y servidor](#).

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.

Requisitos previos

[Descargar el instalador de IaaS para vRealize Automation](#).

Procedimiento

- 1 Acepte el valor del **Servidor** predeterminado, que se rellena con el nombre de dominio completo del servidor del 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 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.

Requisitos previos

- [Registrar los componentes de IaaS](#).
- Compruebe que la máquina en la que está realizando la instalación está conectada a la red y se puede conectar al 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**.

Resultados

La instalación se ha completado.

Pasos siguientes

[Comprobar los servicios de IaaS](#).

Usar interfaces estándar para implementaciones distribuidas

Las implementaciones empresariales se han diseñado para disponer de una mayor capacidad de vRealize Automation en los entornos de producción y requieren que los componentes estén distribuidos en varias máquinas. Las implementaciones empresariales también pueden incluir sistemas redundantes detrás de los equilibradores de carga.

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 5-2. 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 de vRealize Automation
<input type="checkbox"/> Prever y obtener los certificados SSL.	Requisitos de confianza de certificados en una implementación distribuida
<input type="checkbox"/> Implementar el servidor principal del 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
<input type="checkbox"/> Configurar el equilibrador de carga para controlar el tráfico de dispositivos de vRealize Automation.	Configurar el equilibrador de carga
<input type="checkbox"/> Configurar el servidor principal del 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

Tabla 5-2. Lista de comprobación de implementación distribuida (continuación)

Tarea	Detalles
<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
<input type="checkbox"/> Si lo precisa, instalar los agentes que se van a integrar con sistemas externos.	Instalar agentes de vRealize Automation
<input type="checkbox"/> Configurar el tenant predeterminado y proporcionar la licencia de IaaS.	Configurar el acceso al tenant predeterminado

vRealize Orchestrator

El dispositivo de vRealize Automation incluye una versión integrada de vRealize Orchestrator cuya utilización se recomienda ahora con instalaciones nuevas. No obstante, en implementaciones más antiguas o en casos especiales, es posible que los usuarios conecten vRealize Automation a un vRealize Orchestrator independiente externo. Consulte <https://www.vmware.com/products/vrealize-orchestrator.html>.

Para obtener más información sobre la conexión de vRealize Automation y vRealize Orchestrator, consulte *Usar el complemento de vRealize Orchestrator para vRealize Automation*.

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 la guía *Configuración de vRealize Automation*.

Deshabilitar las comprobaciones de estado del equilibrador de carga

Con las comprobaciones de estado nos aseguramos de que un equilibrador de carga envíe el tráfico solo a los nodos que estén funcionando. El equilibrador de carga envía una comprobación de estado a una frecuencia determinada a cada nodo. Los nodos que superen el umbral de error no se podrán elegir para el tráfico nuevo.

Para la conmutación por error y la distribución de las cargas de trabajo, puede colocar varios dispositivos de vRealize Automation detrás de un equilibrador de carga. Además, puede colocar varios servidores web de IaaS y varios servidores de Manager Service de IaaS detrás de sus equilibradores de carga correspondientes.

Cuando use equilibradores de carga, no permita que envíen comprobaciones de estado durante la instalación, ya que podrían interferir en la instalación o causar que esta se comporte de un modo impredecible.

- Al implementar los componentes del dispositivo de vRealize Automation o IaaS detrás de equilibradores de carga existentes, deshabilite las comprobaciones de estado en todos los equilibradores de carga de la configuración propuesta antes de instalar cualquier componente.
- Después de instalar y configurar vRealize Automation por completo, incluidos todos los componentes del dispositivo de vRealize Automation e IaaS, puede volver a habilitar las comprobaciones de estado.

Requisitos de confianza de certificados en una implementación distribuida

vRealize Automation utiliza certificados para mantener las relaciones de confianza y proporcionar una comunicación segura entre los componentes de las implementaciones distribuidas.

En una implementación distribuida, o agrupada en clúster, la organización de los certificados sigue principalmente la arquitectura de tres niveles de vRealize Automation.

- Dispositivos de vRealize Automation
- Componentes web de IaaS
- Componentes de Manager Service de IaaS

En una implementación distribuida, cada máquina de un nivel particular comparte un certificado. Por ejemplo, cada dispositivo de vRealize Automation comparte un certificado común y cada host de Manager Service comparte un certificado común.

Cuando los componentes web y de Manager Service se alojan en la misma máquina, un certificado es suficiente para ambos niveles.

Certificados generados por el sistema

A partir de la versión 7.0, si el usuario no proporciona sus propios certificados, el asistente de instalación de vRealize Automation puede generar automáticamente certificados autofirmados y colocarlos en los almacenes de confianza adecuados de los componentes distribuidos que los requieran.

Si es necesario actualizar los certificados autofirmados que generó el sistema con los certificados suministrados por el usuario o la CA, consulte *Administración de vRealize Automation*.

Forma de proporcionar certificados propios

Cuando se ejecuta el instalador manual estándar, es necesario proporcionar certificados autofirmados generados por cuenta propia o certificados de la entidad de certificación (Certificate Authority, CA).

Si proporciona o genera sus propios certificados mediante OpenSSL u otro método, puede utilizar certificados comodín o certificados de nombre alternativo del firmante (Subject Alternative Name, SAN).

Los certificados de IaaS deben ser multiuso. Si proporciona certificados, debe obtener un certificado multiuso en el que se incluyan componentes de IaaS en el clúster y, a continuación, copiar el certificado en el almacén de confianza de cada componente.

Equilibradores de carga

Para la función de alta disponibilidad y la conmutación por error, es posible agregar equilibradores de carga delante de los componentes distribuidos de vRealize Automation. VMware recomienda utilizar una configuración de acceso directo para los equilibradores de carga de vRealize Automation. En una configuración de acceso directo, los equilibradores de carga pasan las solicitudes a los componentes sin descifrado. A continuación, los dispositivos de vRealize Automation y los hosts de IaaS ejecutan el descifrado correspondiente.

Si utiliza equilibradores de carga, debe incluir el FQDN del equilibrador de carga en la dirección de confianza de los certificados multiuso del clúster.

Para obtener más información sobre cómo usar y configurar equilibradores de carga, consulte *Equilibrio de carga de vRealize Automation*.

Requisitos de confianza de certificados

En la siguiente tabla, se resumen los requisitos que es necesario cumplir para realizar un registro de confianza de los diversos certificados importados.

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

Confianza de certificados y el instalador estándar

Cada vez que se ejecuta o se vuelve a ejecutar el instalador manual estándar para crear componentes de IaaS, es necesario configurar la confianza de certificados en esos componentes de IaaS. Por ejemplo, es posible utilizar el instalador estándar para escalar horizontalmente una implementación existente.

- Hosts web de IaaS y Manager Service

Importe los archivos `web.pfx` y `ms.pfx` a las siguientes ubicaciones.

```
Host Computer/Certificates/Personal certificate store
Host Computer/Certificates/Trusted People certificate store
```

- Hosts de agente de proxy, trabajo de DEM y orquestador de DEM de IaaS

Importe los archivos `web.pfx` y `ms.pfx` a la siguiente ubicación.

```
Host Computer/Certificates/Trusted People certificate store
```

En el almacén de certificados Personas de confianza, no es necesario importar la clave privada junto con el certificado. El proceso de instalación automática instala solo el certificado en el almacén de certificados Personas de confianza.

Configurar certificados de confianza para los hosts de componentes web, Manager Service y DEM

Los clientes que usan una impresión en miniatura con los archivos PFX preinstalados para permitir la autenticación de usuario deben configurar el certificado de confianza de la miniatura en las máquinas host del host web, Manager Service y el orquestador de DEM y el trabajo de DEM.

Los clientes que importen archivos PEM o usen certificados autofirmados pueden ignorar este procedimiento.

Requisitos previos

`web.pfx` y `ms.pfx` válidos disponibles para la autenticación de la impresión en miniatura.

Procedimiento

- 1 Importe los archivos `web.pfx` y `ms.pfx` en las siguientes ubicaciones de las máquinas host del componente web y Manager Service:

- `Host Computer/Certificates/Personal certificate store`
- `Host Computer/Certificates/Trusted People certificate store`

- 2 Importe los archivos `web.pfx` y `ms.pfx` en las siguientes ubicaciones de las máquinas host de orquestador de DEM y trabajo de DEM:

```
Host Computer/Certificates/Trusted People certificate store
```

- 3 Abra una ventana de Microsoft Management Console en cada una de las máquinas host del dispositivo.

Nota Las rutas y las opciones reales de Management Console pueden diferir en algún modo según cuál sea la versión de Windows y la configuración del sistema.

- a Seleccione **Agregar o quitar complemento**.
- b Seleccione **Certificados**.

- c Seleccione **Equipo local**.
- d Abra los archivos de certificados que importó antes y copie las impresiones de miniatura.

Pasos siguientes

Inserte la impresión de miniatura en la página de certificados del asistente de vRealize Automation para Manager Service, los componentes web y los componentes de DEM.

Hojas de trabajo de instalación

Las hojas de trabajo registran información importante que debe consultar durante la instalación.

En los valores de configuración se distinguen mayúsculas de minúsculas. Tenga en cuenta que se añaden espacios adicionales para más componentes si está instalando una implementación distribuida. Es posible que no necesite todos los espacios de las hojas de trabajo. Además, una máquina alojará más de un componente IaaS. Por ejemplo, puede que el servidor Web principal y el orquestador de DEM estén en el mismo nombre de dominio completo (FQDN).

Tabla 5-3. Dispositivo de vRealize Automation

Variable	Mi valor	Ejemplo
FQDN del dispositivo de vRealize Automation principal		automation.mycompany.com
Dirección IP del dispositivo de vRealize Automation principal Solo como referencia; no introduzca direcciones IP		123.234.1.105
FQDN del dispositivo de vRealize Automation adicional		automation2.mycompany.com
Dirección IP del dispositivo de vRealize Automation adicional Solo como referencia; no introduzca direcciones IP		123.234.1.106
FQDN del equilibrador de carga del dispositivo de vRealize Automation		automation-balance.mycompany.com
Dirección IP del equilibrador de carga del dispositivo de vRealize Automation Solo como referencia; no introduzca direcciones IP		123.234.1.201
Nombre de usuario de la interfaz de administración (https://appliance-FQDN:5480)	root (predeterminado)	root
Contraseña de la interfaz de administración		admin123
Tenant predeterminado	vsphere.local (predeterminado)	vsphere.local

Tabla 5-3. Dispositivo de vRealize Automation (continuación)

Variable	Mi valor	Ejemplo
Nombre de usuario del tenant predeterminado	administrador@vsphere.local (predeterminado)	administrator@vsphere.local
Contraseña del tenant predeterminado		login123

Tabla 5-4. Servidores de Windows de IaaS

Variable	Mi valor	Ejemplo
Servidor Web principal de IaaS con FQDN de los datos de Model Manager		web.mycompany.com
Servidor Web principal de IaaS con dirección IP de los datos de Model Manager Solo como referencia; no introduzca direcciones IP		123.234.1.107
FQDN del servidor Web adicional de IaaS		web2.mycompany.com
Dirección IP del servidor Web adicional de IaaS Solo como referencia; no introduzca direcciones IP		123.234.1.108
FQDN del equilibrador de carga del servidor Web de IaaS		web-balance.mycompany.com
Dirección IP del equilibrador de carga del servidor Web de IaaS Solo como referencia; no introduzca direcciones IP		123.234.1.202
FQDN del host activo de Manager Service de IaaS		mgr-svc.mycompany.com
Dirección IP del host activo de Manager Service de IaaS Solo como referencia; no introduzca direcciones IP		123.234.1.109
FQDN del host pasivo de Manager Service de IaaS		mgr-svc2.mycompany.com
Dirección IP del host pasivo de Manager Service de IaaS Solo como referencia; no introduzca direcciones IP		123.234.1.110
FQDN del equilibrador de carga del host de Manager Service de IaaS		mgr-svc-balance.mycompany.com

Tabla 5-4. Servidores de Windows de IaaS (continuación)

Variable	Mi valor	Ejemplo
Dirección IP del equilibrador de carga del host de Manager Service de IaaS Solo como referencia; no introduzca direcciones IP		123.234.203
Para los servicios de IaaS, una cuenta de dominio con privilegios de administrador en los hosts		SUPPORT\provisioner
Contraseña de la cuenta		login123

Tabla 5-5. Base de datos de SQL Server de IaaS

Variable	Mi valor	Ejemplo
Instancia de base de datos		IAASSQL
Nombre de la base de datos	vcac (predeterminado)	vcac
Frase de contraseña (utilizada en la instalación, actualización y migración)		login123

Tabla 5-6. Distributed Execution Managers de IaaS

Variable	Mi valor	Ejemplo
FQDN del host de DEM		dem.mycompany.com
Dirección IP del host de DEM Solo como referencia; no introduzca direcciones IP		123.234.1.111
FQDN del host de DEM		dem2.mycompany.com
Dirección IP del host de DEM Solo como referencia; no introduzca direcciones IP		123.234.1.112
Nombre exclusivo del orquestador de DEM		Orquestador-1
Nombre exclusivo del orquestador de DEM		Orquestador-2
Nombre exclusivo del trabajo de DEM		Trabajo-1
Nombre exclusivo del trabajo de DEM		Trabajo-2
Nombre exclusivo del trabajo de DEM		Trabajo-3
Nombre exclusivo del trabajo de DEM		Trabajo-4

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 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](#). Para obtener información sobre cómo extraer certificados, consulte [Extraer certificados y claves privadas](#).
- 5 Configure el equilibrador de carga para el tráfico de Dispositivo de vRealize Automation.
- 6 Configure los dispositivos para vRealize Automation. Consulte [Configurar dispositivos para vRealize Automation](#).

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 más información sobre los equilibradores de carga, consulte el documento técnico *Guía de configuración de equilibrio de carga de vRealize Automation*.

Para obtener más información sobre la escalabilidad y la alta disponibilidad, consulte la guía de *arquitectura de referencia de vRealize Automation*.

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 primer dispositivo de vRealize Automation en un clúster

El dispositivo de vRealize Automation es una máquina virtual configurada parcialmente que aloja el portal web de usuarios y el servidor de vRealize Automation. Descargue la plantilla del formato de virtualización abierta (Open Virtualization Format, OVF) del dispositivo e impleméntela en vCenter Server o el inventario de ESX/ESXi.

Requisitos previos

- Cree un dispositivo sin configurar. Consulte [Implementar el dispositivo de vRealize Automation](#).
- Obtenga un certificado de autenticación para el dispositivo de vRealize Automation.

Si la red o el equilibrador de carga lo requieren, en procedimientos posteriores se copia el certificado en el equilibrador de carga y en otros dispositivos.

Procedimiento

- 1 Inicie sesión en la interfaz de administración del dispositivo de vRealize Automation sin configurar como raíz.

`https://vrealize-automation-appliance-FQDN:5480`

Continúe aunque aparezcan advertencias de certificado.

- 2 Si aparece el asistente de instalación, cáncelo de modo que pueda ir a la interfaz de administración en su lugar.
- 3 Seleccione **Administración > Configuración horaria** y establezca el origen de sincronización de hora.

Opción	Descripción
Hora del host	Sincronización con el host ESXi del dispositivo de vRealize Automation.
Servidor de hora	Sincronización con un servidor externo de protocolo de hora de red (Network Time Protocol, NTP). Escriba el FQDN o la dirección IP del servidor NTP.

Debe sincronizar todos los dispositivos de vRealize Automation y las instancias de Windows Server de IaaS con el mismo origen de hora. No combine orígenes de hora dentro de una implementación de vRealize Automation.

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

Opción	Acción
Resolver automáticamente	Seleccione Resolver automáticamente para especificar el nombre del host actual del 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-loadbalancename.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 configurar el nombre de host.

- 5 Seleccione la acción apropiada del 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 del dispositivo de vRealize Automation y para cualquier equilibrador de carga mediante el uso de certificados de nombre alternativo del firmante (Subject Alternative Name, SAN).

Si desea generar una solicitud de CSR de un nuevo certificado que pueda enviar a una entidad de certificación, seleccione **Generar solicitud de firma**. Una CSR ayuda a la entidad de certificación a crear un certificado con los valores correctos para importarlo.

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 del host tal como aparece en la parte superior de la página. Si hay instancias adicionales disponibles del 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.

Opción	Acción
Generar solicitud de firma	<ul style="list-style-type: none"> a Seleccione Generar solicitud de firma. b Revise las entradas de los cuadros de texto Organización, Unidad organizativa, Código de país y Nombre común. Estas entradas se rellenan a partir del certificado existente. Estas entradas se pueden editar en caso necesario. c Haga clic en Generar CSR para crear una solicitud de firma de certificado y, a continuación, haga clic en el vínculo Descargar aquí la CSR generada para abrir un cuadro de diálogo y guardar la CSR en una ubicación desde donde se pueda enviar a una entidad de certificación. d Cuando reciba el certificado preparado, haga clic en Importar y siga las instrucciones para importarlo a vRealize Automation.
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. <hr/> <p>Nota En el caso de certificados encadenados, puede haber atributos adicionales disponibles.</p> <hr/> <ul style="list-style-type: none"> 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 interfaz de administración de dispositivos de vRealize Automation como raíz.

`https://vrealize-automation-appliance-FQDN:5480`

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 **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 vRealize Automation.

a Abra un navegador web en la dirección URL de la interfaz de producto de vRealize Automation.

`https://vrealize-automation-appliance-FQDN/vcac`

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

Configurar más instancias del dispositivo de 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.

Para cada dispositivo de vRealize Automation, se debe habilitar la sincronización de hora y añadir el dispositivo a un clúster. La información de configuración basada en los parámetros del dispositivo de vRealize Automation inicial (principal) se incorpora automáticamente cuando se añade el dispositivo 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.

Añadir otro dispositivo de vRealize Automation al clúster

Para alta disponibilidad, las instalaciones distribuidas pueden utilizar un equilibrador de carga delante de un clúster de nodos del dispositivo de vRealize Automation.

Debe utilizar la interfaz de administración en el nuevo dispositivo de vRealize Automation para unirlo a un clúster existente de uno o varios dispositivos. En la operación de unión se copia la información de configuración en el nuevo dispositivo que está añadiendo, incluida la información de certificados, SSO, licencias, bases de datos y mensajes.

Active Directory: cada dispositivo de vRealize Automation incluye un conector que admite la autenticación de usuarios, aunque normalmente solo hay un conector configurado para realizar la sincronización de directorios. Después de añadir otro dispositivo, recuerde configurar un segundo conector que corresponda al dispositivo añadido. El segundo conector se conecta al proveedor de identidad y apunta a la misma instancia de Active Directory. De este modo, si se produce un error en el primer dispositivo, el segundo asume la administración de la autenticación de usuario.

Los dispositivos se deben añadir a un clúster de uno en uno, no en paralelo.

Requisitos previos

- Tenga uno o varios dispositivos de vRealize Automation en el clúster, uno de los cuales debe ser el nodo principal. Consulte [Configurar el primer dispositivo de vRealize Automation en un clúster](#).

Solo puede determinar que un nuevo dispositivo sea el nodo principal después de unirlo al clúster.

- Cree el nuevo nodo de dispositivo. Consulte [Implementar el dispositivo de vRealize Automation](#).
- Compruebe que el equilibrador de carga esté configurado para poder utilizarlo con el nuevo dispositivo.
- Compruebe que el tráfico pueda pasar a través del equilibrador de cargas hasta alcanzar todos los nodos actuales y el nuevo nodo que está a punto de añadir.

- Compruebe que todos los servicios de vRealize Automation se inicien en los nodos actuales.

Procedimiento

- 1 Inicie sesión en la interfaz de administración del nuevo dispositivo de vRealize Automation como raíz.

https://vrealize-automation-appliance-FQDN:5480

Continúe aunque aparezcan advertencias de certificado.
- 2 Si aparece el asistente de instalación, cáncelo de modo que pueda ir a la interfaz de administración en su lugar.
- 3 Seleccione **Administración > Configuración horaria** y especifique el mismo origen de hora que el de los demás dispositivos del clúster.
- 4 Seleccione **vRA > Clúster**.
- 5 En el cuadro de texto **Nodo de clúster de encabezado**, escriba el FQDN de un dispositivo de vRealize Automation que se haya configurado anteriormente.

Puede usar el FQDN del dispositivo de vRealize Automation principal o de cualquier 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.

Resultados

Si una operación para unirse a un clúster tarda mucho tiempo y se termina agotando el tiempo de espera, consulte el [artículo 58708 de la Base de conocimientos de VMware](#).

Deshabilitar los servicios sin usar

Para conservar recursos internos en los casos en los que se use una instancia externa de vRealize Orchestrator, puede deshabilitar el servicio de vRealize Orchestrator integrado.

Requisitos previos

[Añadir otro dispositivo de vRealize Automation al clúster](#)

Procedimiento

- 1 Inicie sesión en la consola del dispositivo de vRealize Automation.

2 Detenga el servicio de vRealize Orchestrator.

```
service vco-server stop
chkconfig vco-server off
```

Validar la implementación distribuida

Después de implementar instancias adicionales del dispositivo de vRealize Automation, valide 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 Confirme que puede iniciar sesión en vRealize Automation a través de la dirección del equilibrador de carga:

`https://vrealize-automation-appliance-load-balancer-FQDN/vcac`
- 3 Tras comprobar que puede acceder al nuevo dispositivo de vRealize Automation mediante el equilibrador de carga, 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 deben ejecutarse con el mismo usuario de cuenta de servicio, que debe ser una cuenta de dominio con privilegios en todos los servidores de IaaS distribuidos. No use cuentas del sistema local.

Requisitos previos

- [Configurar el primer dispositivo de vRealize Automation en un clúster.](#)
- Si el sitio incluye varios dispositivos de vRealize Automation, consulte el documento [Añadir otro dispositivo de vRealize Automation al clúster.](#)
- Compruebe que el servidor cumple los requisitos de [Servidores de Windows de IaaS.](#)
- 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](#)

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 para vRealize Automation](#)

Para instalar IaaS en los servidores de Windows físicos o virtuales distribuidos, debe descargar una copia del instalador de IaaS desde el dispositivo de vRealize Automation.

3 [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.

4 [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.

5 [Instalar componentes del servidor web de IaaS adicionales](#)

El servidor web proporciona acceso a las capacidades de la infraestructura en vRealize Automation. Después de que se haya instalado el primer servidor web, podría aumentar el rendimiento instalando servidores web de IaaS adicionales.

6 [Instalar el Manager Service activo](#)

Manager Service activo es un servicio de Windows que coordina la comunicación entre IaaS Distributed Execution Managers, la base de datos, los agentes, los agentes de proxy y SMTP.

7 [Instalar un componente de copia de seguridad de Manager Service](#)

La copia de seguridad de Manager Service proporciona redundancia y alta disponibilidad, y se puede iniciar manualmente si el servicio activo se detiene.

8 [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.

9 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.

10 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.

Pasos siguientes

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

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.

Requisitos previos

En máquinas con Windows 2012, debe deshabilitar TLS1.2 para certificados que usan SHA512. Para obtener más información sobre cómo deshabilitar TLS1.2, consulte [Artículo 245030 de Microsoft Knowledge Base](#).

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`.

Pasos siguientes

[Descargar el instalador de IaaS para vRealize Automation.](#)

Descargar el instalador de IaaS para vRealize Automation

Para instalar IaaS en los servidores de Windows físicos o virtuales distribuidos, debe descargar una copia del instalador de IaaS desde el dispositivo de vRealize Automation.

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

Requisitos previos

- [Configurar el primer dispositivo de vRealize Automation en un clúster](#) y, opcionalmente, [Añadir otro dispositivo de vRealize Automation al clúster](#).
- Compruebe que el servidor cumple los requisitos de [Servidores de Windows de IaaS](#).
- 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 el servidor Windows de IaaS mediante una cuenta con derechos de administrador.
- 3 Abra un navegador web directamente en la URL del instalador del dispositivo de vRealize Automation. No use una dirección de equilibrador de carga.

<https://vrealize-automation-appliance-FQDN:5480/installer>
- 4 Haga clic en **Instalador de IaaS**.

- 5 Guarde `setup__vrealize-automation-appliance-FQDN@5480` en el servidor Windows.

No modifique el nombre de archivo del instalador. Sirve para conectar la instalación con el dispositivo de vRealize Automation.

- 6 Descargue el archivo del instalador en cada servidor Windows de IaaS en los que esté instalando componentes.

Pasos siguientes

Instale una base de datos de IaaS (consulte [Elegir un escenario de base de datos de IaaS](#)).

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 con la configuración de SSL en SQL Server, consulte [Artículo 189067 de Microsoft TechNet](#).

Tabla 5-7. 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.
Preparar una base de datos vacía y usar el instalador para rellenar el esquema de base de datos. Con esta opción, el instalador usa un usuario de base de datos con privilegios dbo para rellenar la base de datos.	Preparar una base de datos vacía .
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.

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.

Requisitos previos

- Instale Microsoft .NET Framework 4.5.2 o posterior 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 [Host de SQL Server en IaaS](#).
- Abra un navegador web en la URL del instalador del dispositivo de vRealize Automation y descargue los scripts de instalación de la base de datos de IaaS.

<https://vrealize-automation-appliance-FQDN: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 5-8. Valores de base de datos

Variable	Valor
<i>db_server</i>	Especifica la instancia de SQL Server con el formato dbhostname[,port number]\SQL instance. 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 db_server es localhost.
<i>db_name</i>	Nombre de la base de datos. El valor predeterminado es vra. 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).

Tabla 5-8. Valores de base de datos (continuación)

Variable	Valor
<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>	La versión de vRealize Automation, que se encuentra iniciando sesión en el dispositivo de vRealize Automation y haciendo clic en la pestaña Actualizar. Por ejemplo, la cadena de la versión 6.1 de vRealize Automation es 6.1.0.1200.

Resultados

La base de datos se ha creado.

Pasos siguientes

[Instalar los componentes de IaaS en una configuración distribuida.](#)

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.

Requisitos previos

- Confirme los requisitos previos de instalación de base de datos. Consulte [Host de SQL Server en IaaS](#).
- Abra un navegador web en la URL del instalador del dispositivo de vRealize Automation y descargue los scripts de instalación de la base de datos de IaaS.

<https://vrealize-automation-appliance-FQDN: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 los siguientes archivos y sustituya todas las instancias de las variables de la tabla por los valores correctos de su entorno.

```
CreateDatabase.sql
SetDatabaseSettings.sql
```

Tabla 5-9. Valores de base de datos

Variable	Valor
\$(DBName)	Nombre de la base de datos, por ejemplo vra. Los nombres de base de datos no deben tener más de 128 caracteres ASCII.
\$(DBDir)	Ruta al directorio de datos de la base de datos (quitando la barra diagonal final).
\$(LogDir)	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 `SetDatabaseSettings.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 Debajo del contenido de `CreateDatabase.sql`, pegue el contenido completo modificado de `SetDatabaseSettings.sql`.

- 11 Haga clic en **Ejecutar**.

El script se ejecutará y se creará la base de datos.

Pasos siguientes

[Instalar los componentes de IaaS en una configuración distribuida.](#)

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](#).

Requisitos previos

- 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 para vRealize Automation.](#)

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
 Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.
 Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.
 Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.
- 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, para admitir esta opción primero debe configurar SSL en SQL Server. Para obtener más información sobre la configuración de SSL en SQL Server, consulte [Artículo 189067 de Microsoft TechNet](#).

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.

Se recomienda la autenticación de Windows. Cuando elija la autenticación de SQL, la contraseña de la base de datos no cifrada aparece en ciertos archivos de configuración.

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**.

Resultados

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.

Requisitos previos

- Instale la base de datos de IaaS (consulte [Elegir un escenario de base de datos de IaaS](#)).
- Si ya ha instalado otros componentes de IaaS, ya conoce la frase de contraseña que ha creado.
- Si usa equilibradores de carga en su entorno, asegúrese de que reúnen los requisitos de configuración.

Procedimiento

1 [Instalar el primer componente del servidor web de IaaS](#)

Instale el componente del servidor web de IaaS para que proporcione acceso a las capacidades de la infraestructura en vRealize Automation.

2 [Configurar Model Manager Data](#)

El componente Model Manager se instala en la misma máquina que aloja el primer componente de servidor web. Model Manager Data solo se instala una vez.

Resultados

Se puede instalar más componentes de sitio web o instalar Manager Service. Consulte [Instalar componentes del servidor web de IaaS adicionales](#) o [Instalar el Manager Service activo](#).

Instalar el primer componente del servidor web de IaaS

Instale el componente del servidor web de IaaS para que proporcione acceso a las capacidades de la infraestructura en vRealize Automation.

Puede instalar varios servidores web de IaaS, pero solo el primero incluye a Model Manager Data.

Requisitos previos

- [Crear la base de datos de IaaS con el asistente de instalación.](#)
- Compruebe que el servidor cumple los requisitos de [Servidores de Windows de IaaS](#).
- Si ya ha instalado otros componentes de IaaS, ya conoce la frase de contraseña que ha creado.
- Si usa equilibradores de carga en su entorno, asegúrese de que reúnen los requisitos de configuración.

Procedimiento

- 1 Si utiliza un equilibrador de carga, deshabilite los demás nodos del equilibrador de carga y compruebe que el tráfico se dirige al nodo que desea.

Deshabilite también las comprobaciones de estado del equilibrador de carga hasta que se hayan instalado y configurado todos los componentes de vRealize Automation.
- 2 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.

Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.

Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.

Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.

- 10 Haga clic en **Siguiente**.
- 11 Seleccione **Sitio web** y **ModelManagerData** 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.

Configurar Model Manager Data

El componente Model Manager se instala en la misma máquina que aloja el primer componente de servidor web. Model Manager Data solo se instala una vez.

Requisitos previos

[Instalar el primer componente del servidor web de IaaS.](#)

Procedimiento

- 1 Haga clic en la pestaña **Model Manager Data**.
- 2 En el cuadro de texto **Servidor**, introduzca el nombre de dominio completo del dispositivo de vRealize Automation.

vrealize-automation-appliance.mycompany.com

No escriba una dirección IP.
- 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** e introduzca la contraseña que ha creado al configurar SSO en los cuadros de texto **Contraseña** y **Confirmar**.
- 8 (opcional) Haga clic en **Probar** para comprobar las credenciales.
- 9 En el cuadro de texto **Servidor de IaaS**, identifique el componente de servidor web de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente de servidor web de IaaS, <i>web-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente de servidor web de IaaS, <i>web.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

El puerto predeterminado es 443.

- 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 sobre la instalación del servidor** de la página Configuración del servidor y la cuenta, escriba el nombre de usuario y la contraseña del usuario de la cuenta de servicio que tenga privilegios administrativos en el servidor de instalación actual.

El usuario de la cuenta de servicio debe ser una cuenta de dominio con privilegios en cada servidor IaaS distribuido. No use cuentas del sistema local.

- 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**.

Pasos siguientes

Se puede instalar más componentes de servidor web o instalar Manager Service. Consulte [Instalar componentes del servidor web de IaaS adicionales](#) o [Instalar el Manager Service activo](#).

Instalar componentes del servidor web de IaaS adicionales

El servidor web proporciona acceso a las capacidades de la infraestructura en vRealize Automation. Después de que se haya instalado el primer servidor web, podría aumentar el rendimiento instalando servidores web de IaaS adicionales.

No instale Model Manager Data con un componente del servidor web adicional. Solo el primer componente del servidor web aloja a Model Manager Data.

Requisitos previos

- [Instalar un componente de sitio web de IaaS con Model Manager Data.](#)
- Compruebe que el nuevo servidor cumpla con los requisitos de [Servidores de Windows de IaaS](#).
- Utilice la interfaz de administración de dispositivos de vRealize Automation para reemplazar el certificado a fin de incluir el FQDN del nodo nuevo. Consulte *Reemplazar certificados en el dispositivo de vRealize Automation* en la guía *Administración de vRealize Automation*.
- Si ya ha instalado otros componentes de IaaS, ya conoce la frase de contraseña que ha creado.
- Si usa equilibradores de carga en su entorno, asegúrese de que reúnen los requisitos de configuración.

Procedimiento

- 1 Si utiliza un equilibrador de carga, deshabilite los demás nodos del equilibrador de carga y compruebe que el tráfico se dirige al nodo que desea.

Deshabilite también las comprobaciones de estado del equilibrador de carga hasta que se hayan instalado y configurado todos los componentes de vRealize Automation.
- 2 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.

- b Seleccione **Aceptar certificado**.

- c Haga clic en **Ver certificado**.

Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.

Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.

Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.

- 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 En el cuadro de texto del **servidor de IaaS**, identifique el primer componente del servidor web de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente de servidor web de IaaS, <i>web-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el primer componente del servidor web de IaaS, <i>web.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

El puerto predeterminado es 443.

- 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	<p>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.</p>

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

El usuario de la cuenta de servicio debe ser una cuenta de dominio con privilegios en cada servidor de IaaS distribuido. No use cuentas del sistema local.

- 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**.

Pasos siguientes

[Instalar el Manager Service activo](#) .

Instalar el Manager Service activo

Manager Service activo es un servicio de Windows que coordina la comunicación entre IaaS Distributed Execution Managers, la base de datos, los agentes, los agentes de proxy y SMTP.

A menos que se habilite la conmutación por error automática de Manager Service, la implementación de IaaS requiere que solo una máquina de Windows ejecute activamente Manager Service cada vez. El servicio debe estar detenido en las máquinas de copia de seguridad y configurado para iniciarse manualmente.

Consulte [Acerca de la conmutación por error automática de Manager Service](#) .

Requisitos previos

- Si ya ha instalado otros componentes de IaaS, ya conoce la frase de contraseña que ha creado.
- (opcional) Si desea instalar Manager Service en un sitio web que no sea el predeterminado, cree antes un sitio web en Internet Information Services.
- 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.](#)

Procedimiento

- 1 Si utiliza un equilibrador de carga, deshabilite los demás nodos del equilibrador de carga y compruebe que el tráfico se dirige al nodo que desea.

Deshabilite también las comprobaciones de estado del equilibrador de carga hasta que se hayan instalado y configurado todos los componentes de vRealize Automation.
- 2 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.

Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.

Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.

Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.

- 9 Haga clic en **Siguiente**.
- 10 Seleccione **Manager Service** en la página **Instalación personalizada de servidor de IaaS**.
- 11 En el cuadro de texto **Servidor de IaaS**, identifique el componente de servidor web de IaaS.

Opción	Descripción
Con un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente de servidor web de IaaS, <i>web-load-balancer.mycompany.com:443</i> . No escriba las direcciones IP.
Sin un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente de servidor web de IaaS, <i>web.mycompany.com:443</i> . No escriba las direcciones IP.

El puerto predeterminado es 443.

- 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 sobre la instalación del servidor** de la página Configuración del servidor y la cuenta, escriba el nombre de usuario y la contraseña del usuario de la cuenta de servicio que tenga privilegios administrativos en el servidor de instalación actual.

El usuario de la cuenta de servicio debe ser una cuenta de dominio con privilegios en cada servidor de IaaS distribuido. No use cuentas del sistema local.

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**.

Pasos siguientes

- 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](#).

- 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](#).

Instalar un componente de copia de seguridad de Manager Service

La copia de seguridad de Manager Service proporciona redundancia y alta disponibilidad, y se puede iniciar manualmente si el servicio activo se detiene.

A menos que se habilite la conmutación por error automática de Manager Service, la implementación de IaaS requiere que solo una máquina de Windows ejecute activamente Manager Service cada vez. El servicio debe estar detenido en las máquinas de copia de seguridad y configurado para iniciarse manualmente.

Consulte [Acerca de la conmutación por error automática de Manager Service](#).

Requisitos previos

- Si ya ha instalado otros componentes de IaaS, ya conoce la frase de contraseña que ha creado.
- (opcional) Si desea instalar Manager Service en un sitio web que no sea el predeterminado, cree antes un sitio web en Internet Information Services.
- Utilice la interfaz de administración de dispositivos de vRealize Automation para reemplazar el certificado a fin de incluir el FQDN del nodo nuevo. Consulte *Reemplazar certificados en el dispositivo de vRealize Automation* en la guía *Administración de vRealize Automation*.
- 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](#).

Procedimiento

- 1 Si utiliza un equilibrador de carga, deshabilite los demás nodos del equilibrador de carga y compruebe que el tráfico se dirige al nodo que desea.

Deshabilite también las comprobaciones de estado del equilibrador de carga hasta que se hayan instalado y configurado todos los componentes de vRealize Automation.
- 2 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.

- b Seleccione **Aceptar certificado**.

- c Haga clic en **Ver certificado**.

Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.

Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.

Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.

- 10 Haga clic en **Siguiente**.

- 11 Seleccione **Manager Service** en la página **Instalación personalizada de servidor de IaaS**.

- 12 En el cuadro de texto **Servidor de IaaS**, identifique el componente de servidor web de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente de servidor web de IaaS, <i>web-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente de servidor web de IaaS, <i>web.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

El puerto predeterminado es 443.

- 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 sobre la instalación del servidor** de la página Configuración del servidor y la cuenta, escriba el nombre de usuario y la contraseña del usuario de la cuenta de servicio que tenga privilegios administrativos en el servidor de instalación actual.

El usuario de la cuenta de servicio debe ser una cuenta de dominio con privilegios en cada servidor de IaaS distribuido. No use cuentas del sistema local.

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**.

Pasos siguientes

- 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](#).

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 [Host de Distributed Execution Manager de IaaS](#).

Instalar Distributed Execution Managers

Debe instalar al menos un DEM de trabajo y un DEM de 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.

Requisitos previos

[Descargar el instalador de IaaS para vRealize Automation](#).

Antes de instalar un nuevo DEM de trabajo, exporte el certificado del dispositivo virtual de instalación de vRA e impórtelo en la ubicación de almacenamiento de certificados raíz de confianza de la máquina local.

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.

Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.

Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.

- 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.

La cuenta de servicio debe tener privilegios de administrador local y debe ser la misma cuenta de dominio que se haya utilizado durante toda la instalación de IaaS. La cuenta de servicio tiene privilegios en cada servidor de IaaS distribuido y no debe ser una cuenta de sistema 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**.

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 los host y los puertos en los cuadros de texto **Nombre del host de Manager Service** y **Nombre del host de servicio web de Model Manager**.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de los equilibradores de carga del componente Manager Service y el servidor web que aloja Model Manager (<i>mgr-svc-load-balancer.mycompany.com:443</i> y <i>web-load-balancer.mycompany.com:443</i>).</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina en la que ha instalado el componente Manager Service y el servidor web que aloja Model Manager (<i>mgr-svc.mycompany.com:443</i> y <i>web.mycompany.com:443</i>).</p> <p>No escriba las direcciones IP.</p>

El puerto predeterminado es 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**.

Pasos siguientes

- 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 DEM para conectarse con SCVMM en una ruta de instalación diferente

De manera predeterminada, el archivo de configuración de trabajo de DEM utiliza la ruta de instalación predeterminada de la consola Microsoft System Center Virtual Machine Manager (SCVMM). Debe actualizar el archivo si instala la consola SCVMM en una ubicación que no sea la predeterminada.

Solo necesita este procedimiento si tiene endpoints y agentes de SCVMM.

Requisitos previos

- Averigüe cuál es la ruta de acceso no predeterminada en la que ha instalado la consola SCVMM.

La siguiente es la ruta predeterminada que debe sustituir en el archivo de configuración.

```
path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"
```

Procedimiento

- 1 Detenga el servicio Trabajo de DEM.
- 2 Abra el siguiente archivo en un editor de texto.
Archivos de programa (x86)\VMware\VCAC\Distributed Execution Manager*instance-name*\DynamicOps.DEM.exe.config
- 3 Localice la sección <assemblyLoadConfiguration>.
- 4 Actualice cada ruta con el siguiente ejemplo como guía.

```
<assemblyLoadConfiguration>
  <assemblies>
    <!-- List of required assemblies for Scvmm -->
    <add name="Errors" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Microsoft.SystemCenter.VirtualMachineManager" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Remoting" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="TraceWrapper" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Utils" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
  </assemblies>
</assemblyLoadConfiguration>
```

- 5 Guarde y cierre DynamicOps.DEM.exe.config.
- 6 Reinicie el servicio Trabajo de DEM.

Resultados

Para obtener más información, consulte [Trabajos de DEM con SCVMM](#).

Puede encontrar más información sobre la preparación del entorno de SCVMM y la creación de un endpoint de SCVMM en *Configuración de vRealize Automation*.

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.

Requisitos previos

- [Elegir un escenario de base de datos de IaaS.](#)
- 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**.

Resultados

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 servicio de Windows accede a la base de datos en tiempo de ejecución, incluso si la base de datos se configuró con autenticación de SQL. Se puede cambiar la autenticación en tiempo de ejecución de Windows a SQL.

Un motivo para cambiar la autenticación en tiempo de ejecución puede ser cuando, por ejemplo, la base de datos está en un dominio que no es de confianza.

Requisitos previos

Compruebe que existe la base de datos de SQL Server de vRealize Automation. Comience con [Elegir un escenario de base de datos de IaaS.](#)

Procedimiento

- 1 Si se utiliza una cuenta con privilegios de administrador, inicie sesión en el servidor de Windows de IaaS que aloja Manager Service.
- 2 En **Herramientas administrativas > Servicios**, detenga el servicio **VMware vCloud Automation Center**.
- 3 Abra los siguientes archivos en un editor de texto.

```
C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config
C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
```

- 4 En cada archivo, localice la sección <connectionStrings>.
- 5 Sustituya
`Integrated Security=True;`
 por
`User Id=database-username;Password=database-password;`
- 6 Guarde y cierre los archivos.

```
ManagerService.exe.config
Web.config
```

- 7 Inicie el servicio **VMware vCloud Automation Center**.
- 8 Utilice el comando `iisreset` para reiniciar IIS.

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**.

Instalar agentes de vRealize Automation

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](#).

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.

Para obtener más información sobre la política de ejecución de PowerShell, consulte [Artículo de Microsoft PowerShell sobre las políticas de ejecución](#). Si la política de ejecución de PowerShell se administra en el nivel de política de grupo, póngase en contacto con el equipo de asistencia de TI para obtener información sobre las restricciones en los cambios de política y consulte [Artículo de Microsoft PowerShell sobre la configuración de políticas de grupo](#).

Requisitos previos

- 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 Con una cuenta de administrador, inicie sesión en la máquina host de IaaS en la que el agente está instalado.
- 2 Seleccione **Inicio > Todos los programas > Versión de Windows PowerShell > Windows PowerShell**.
- 3 Para RemoteSigned, ejecute `Set-ExecutionPolicy RemoteSigned`.
- 4 Para Unrestricted, ejecute `Set-ExecutionPolicy Unrestricted`.
- 5 Compruebe que el comando no produce ningún error.
- 6 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 5-10. 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
Aprovisionar máquinas virtuales integrándose con un entorno de Microsoft Hyper-V Server.	Instalar el agente de proxy de Hyper-V o XenServer
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 ■ Instalar el agente de EPI de Citrix
Aprovisionar máquinas virtuales integrándose con un entorno de XenDesktop.	<ul style="list-style-type: none"> ■ Instalar el agente de VDI de XenDesktop ■ Instalar el agente de EPI de Citrix
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
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
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.

El privilegio `VApp.Import` permite implementar una máquina de vSphere mediante la configuración importada de un OVF. Los detalles sobre el privilegio de vSphere están disponibles en la [documentación de vSphere SDK](#). Si desea usar un endpoint de vSphere para implementar máquinas virtuales a partir de plantillas de OVF, compruebe que las credenciales incluyan el privilegio `VApp.Import` de vSphere en la instancia de vCenter Server asociada con el endpoint.

La siguiente tabla enumera los permisos que deben tener las credenciales de endpoint de vSphere para administrar una instancia vCenter Server. Los permisos deben estar habilitados para todos los clústeres de vCenter Server, no solo para los clústeres que alojarán endpoints.

Tabla 5-11. 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

Tabla 5-11. Permisos necesarios para que el agente de vSphere administre una instancia de vCenter Server (continuación)

Valor de atributo		Permiso
Clúster de almacén de datos		Configurar un clúster de almacén de datos
Carpeta		Crear carpeta
		Eliminar carpeta
Global		Administrar atributos personalizados
		Establecer atributo personalizado
Red		Asignar red
Permisos		Modificar permiso
vApp		Importar
		Configuración de aplicación vApp
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
		Mover
		Quitar
	Interacción	Configurar CD
		Interacción de consola
		Conexión de dispositivos
		Apagar
		Encender
		Restablecer
		Suspender
		Instalación de herramientas
	Configuración	Añadir disco existente
		Añadir disco nuevo
		Agregar o quitar dispositivo
		Quitar disco

Tabla 5-11. Permisos necesarios para que el agente de vSphere administre una instancia de vCenter Server (continuación)

Valor de atributo	Permiso
	Avanzado
	Cambiar recuento de CPU
	Cambiar recurso
	Extender disco virtual
	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.

Requisitos previos

- Instale IaaS, incluidos el servidor web y el host de Manager Service.

- Compruebe que la máquina donde se instala el agente esté en un dominio de confianza del dominio en el que están instalados los componentes de IaaS.
- Compruebe que los requisitos de [Requisitos del agente de vSphere](#) se cumplen.
- Si ya ha creado un endpoint de vSphere para utilizarlo con este agente, anote el nombre del endpoint.
- [Descargar el instalador de IaaS para vRealize Automation.](#)

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
 Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el puerto 5480.
- 5 Seleccione **Instalación personalizada** en la página Tipo de instalación.
- 6 En el área Selección de componentes, seleccione **Agentes de proxy**.
- 7 Acepte la ubicación de instalación raíz o haga clic en **Cambiar** y seleccione una ruta de instalación.
 Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.
 Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.
- 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 Para alta disponibilidad, puede añadir agentes redundantes y configurarlos de forma idéntica. De lo contrario, configure los agentes de modo que sean únicos.

Opción	Descripción
Agente redundante	<p>Instale agentes redundantes en distintos servidores.</p> <p>Configure los agentes redundantes de forma idéntica y asígneles el mismo nombre.</p>
Agente independiente	<p>Asigne un nombre único al agente.</p>

13 Configure una conexión con el host de Manager Service de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service, <i>mgr-svc.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

El puerto predeterminado es 443.

14 Configure una conexión al servidor web de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente de servidor web, <i>web-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente de servidor web, <i>web.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

El puerto predeterminado es 443.

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

16 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.

17 Haga clic en **Agregar**.

18 Haga clic en **Siguiente**.

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

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

20 Haga clic en **Siguiente**.

21 Haga clic en **Finalizar**.

22 Confirme que la instalación se ha realizado correctamente.

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

Pasos siguientes

[Configurar el agente de vSphere.](#)

Configurar el agente de vSphere

Configure el agente de vSphere para crear y utilizar los endpoints de vSphere en los blueprints de vRealize Automation.

Utilice la utilidad del agente proxy para modificar las partes cifradas del archivo de configuración del agente o para cambiar la directiva de eliminación de la máquina para las plataformas de virtualización. Solo está cifrada una parte del archivo de configuración del agente VRMAgent.exe.config. Por ejemplo, la sección serviceConfiguration no está cifrada.

Requisitos previos

Si se utiliza una cuenta con privilegios de administrador, inicie sesión en el servidor de Windows de IaaS donde instaló el agente de vSphere.

Procedimiento

1 Abra un símbolo del sistema de Windows como administrador.

2 Cambie a la carpeta de instalación del agente, donde *agent-name* es la carpeta que contiene el agente de vSphere.

```
cd %SystemDrive%\Program Files (x86)\VMware\vCAC\Agents\agent-name
```

3 (opcional) Para ver la configuración actual, introduzca el siguiente comando.

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

A continuación, se muestra un ejemplo de la salida del comando.

```
managementEndpointName: VCendpoint
doDeletes: True
```

- 4 (opcional) Para cambiar el nombre del endpoint que configuró en la instalación, utilice el siguiente comando.

```
set managementEndpointName
```

Por ejemplo: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName my-endpoint`

Utilice este proceso para cambiar el nombre del endpoint en vRealize Automation en lugar de cambiar los endpoints.

- 5 (opcional) Para configurar la directiva de eliminación de la máquina virtual, utilice el siguiente comando.

```
set doDeletes
```

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 VRMDeleted de vCenter Server.

- 6 Abra **Herramientas administrativas > Servicios** y reinicie el servicio vRealize Automation Agente – *agent-name*.

Pasos siguientes

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.

Requisitos previos

- Instale IaaS, incluidos el servidor web y el host de Manager Service.
- [Descargar el instalador de IaaS para vRealize Automation.](#)
- 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__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.

b Seleccione **Aceptar certificado**.

c Haga clic en **Ver certificado**.

Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.

Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.

Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.

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 Para alta disponibilidad, puede añadir agentes redundantes y configurarlos de forma idéntica. De lo contrario, configure los agentes de modo que sean únicos.

Opción	Descripción
Agente redundante	<p>Instale agentes redundantes en distintos servidores.</p> <p>Configure los agentes redundantes de forma idéntica y asígneles el mismo nombre.</p>
Agente independiente	<p>Asigne un nombre único al agente.</p>

- 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 host de Manager Service de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service, <i>mgr-svc.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

El puerto predeterminado es 443.

- 15** Configure una conexión al servidor web de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente de servidor web, <i>web-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente de servidor web, <i>web.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

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.

Pasos siguientes

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.

[Configurar el agente de Hyper-V o XenServer.](#)

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.

Requisitos previos

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.

Escriba `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
```

Pasos siguientes

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](#) 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](#).

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.

Requisitos previos

- Instale IaaS, incluidos el servidor web y el host de Manager Service.
- Compruebe que los requisitos de [Requisitos de XenDesktop](#) se cumplen.
- [Descargar el instalador de IaaS para vRealize Automation](#).

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.
 Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.

Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.

Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.

- 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 Para alta disponibilidad, puede añadir agentes redundantes y configurarlos de forma idéntica. De lo contrario, configure los agentes de modo que sean únicos.

Opción	Descripción
Agente redundante	<p>Instale agentes redundantes en distintos servidores.</p> <p>Configure los agentes redundantes de forma idéntica y asígneles el mismo nombre.</p>
Agente independiente	<p>Asigne un nombre único al agente.</p>

- 14 Configure una conexión con el host de Manager Service de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service, <i>mgr-svc.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

El puerto predeterminado es 443.

15 Configure una conexión al servidor web de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente de servidor web, <i>web-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente de servidor web, <i>web.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

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.

Pasos siguientes

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](#) 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](#).

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.

Requisitos previos

- Instale IaaS, incluidos el servidor web y el host de Manager Service.
- Compruebe que los requisitos de [Servidor de aprovisionamiento de Citrix](#) se cumplen.

- [Descargar el instalador de IaaS para vRealize Automation.](#)

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.

- b Seleccione **Aceptar certificado**.

- c Haga clic en **Ver certificado**.

Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.

Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.

Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.

- 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 Para alta disponibilidad, puede añadir agentes redundantes y configurarlos de forma idéntica. De lo contrario, configure los agentes de modo que sean únicos.

Opción	Descripción
Agente redundante	<p>Instale agentes redundantes en distintos servidores.</p> <p>Configure los agentes redundantes de forma idéntica y asígneles el mismo nombre.</p>
Agente independiente	<p>Asigne un nombre único al agente.</p>

13 Configure una conexión con el host de Manager Service de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service, <i>mgr-svc.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

El puerto predeterminado es 443.

14 Configure una conexión al servidor web de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente de servidor web, <i>web-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente de servidor web, <i>web.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

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.

Pasos siguientes

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 desaprovisionarla. 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 5-12. 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. Para más información, visite http://support.microsoft.com .
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: <div data-bbox="598 1428 1412 1522"> <pre>help about_signing help Set-ExecutionPolicy</pre> </div>

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.

Requisitos previos

- Instale IaaS, incluidos el servidor web y el host de Manager Service.

- Compruebe que los requisitos de [Requisitos de Visual Basic Scripting](#) se cumplen.
- [Descargar el instalador de IaaS para vRealize Automation](#).

Procedimiento

- 1 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Aceptar certificado**.
 - c Haga clic en **Ver certificado**.

Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.

Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.

Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.
- 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 Para alta disponibilidad, puede añadir agentes redundantes y configurarlos de forma idéntica. De lo contrario, configure los agentes de modo que sean únicos.

Opción	Descripción
Agente redundante	<p>Instale agentes redundantes en distintos servidores.</p> <p>Configure los agentes redundantes de forma idéntica y asígneles el mismo nombre.</p>
Agente independiente	<p>Asigne un nombre único al agente.</p>

13 Configure una conexión con el host de Manager Service de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service, <i>mgr-svc.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

El puerto predeterminado es 443.

14 Configure una conexión al servidor web de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente de servidor web, <i>web-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente de servidor web, <i>web.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

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.

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.

Requisitos previos

- Instale IaaS, incluidos el servidor web y el host de Manager Service.
- Compruebe que los requisitos de [Habilitar solicitudes de WMI remotas en máquinas de Windows](#) se cumplen.
- [Descargar el instalador de IaaS para vRealize Automation](#).

Procedimiento

1 Haga clic con el botón derecho en el archivo de instalación `setup__vrealize-automation-appliance-FQDN@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, proporcione las credenciales de administrador del 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 ha especificado al implementar el dispositivo de vRealize Automation.

b Seleccione **Aceptar certificado**.

c Haga clic en **Ver certificado**.

Compare la huella digital de certificado con la huella digital definida para el dispositivo de vRealize Automation. El certificado del dispositivo de vRealize Automation se puede ver en el navegador del cliente cuando se accede a la interfaz de administración de dispositivos de vRealize Automation en el 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.

Incluso en una implementación distribuida, podría en ocasiones instalar más de un componente de IaaS en el mismo servidor de Windows.

Si instala más de un componente de IaaS, instálelos siempre en la misma ruta de acceso.

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 Para alta disponibilidad, puede añadir agentes redundantes y configurarlos de forma idéntica. De lo contrario, configure los agentes de modo que sean únicos.

Opción	Descripción
Agente redundante	<p>Instale agentes redundantes en distintos servidores.</p> <p>Configure los agentes redundantes de forma idéntica y asígneles el mismo nombre.</p>
Agente independiente	<p>Asigne un nombre único al agente.</p>

13 Configure una conexión con el host de Manager Service de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente Manager Service, <i>mgr-svc.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

El puerto predeterminado es 443.

14 Configure una conexión al servidor web de IaaS.

Opción	Descripción
Con un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga del componente de servidor web, <i>web-load-balancer.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>
Sin un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina donde ha instalado el componente de servidor web, <i>web.mycompany.com:443</i>.</p> <p>No escriba las direcciones IP.</p>

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.

Instalación silenciosa de vRealize Automation

6

vRealize Automation incluye opciones para realizar instalaciones silenciosas mediante scripts desde la línea de comandos, así como instalaciones silenciosas basadas en API. Ambos métodos requieren preparar por adelantado los valores que se suelen introducir manualmente durante una instalación convencional.

Este capítulo incluye los siguientes temas:

- [Acerca de la instalación silenciosa de vRealize Automation](#)
- [Realizar una instalación silenciosa de vRealize Automation](#)
- [Realizar una instalación silenciosa del agente de administración de vRealize Automation](#)
- [Archivo de respuesta de la instalación silenciosa de vRealize Automation](#)
- [La línea de comando para la instalación de vRealize Automation](#)
- [La API de instalación de vRealize Automation](#)
- [Convertir entre las propiedades silenciosas de vRealize Automation y JSON](#)

Acerca de la instalación silenciosa de vRealize Automation

La instalación silenciosa de vRealize Automation utiliza un archivo ejecutable que hace referencia a un archivo de respuesta basado en texto.

En el archivo de respuesta, se preconfiguran los FQDN del sistema, las credenciales de cuenta y otros ajustes que se suelen introducir durante una instalación manual o basada en asistente convencional. La instalación silenciosa resulta de utilidad para los siguientes tipos de implementaciones.

- Implementar múltiples entornos casi idénticos.
- Volver a implementar de forma repetida el mismo entorno.
- Realizar instalaciones desatendidas.
- Realizar instalaciones mediante scripts.

Realizar una instalación silenciosa de vRealize Automation

Puede realizar una instalación silenciosa desatendida de vRealize Automation desde la consola de un dispositivo de vRealize Automation recién implementado.

Requisitos previos

- Cree un dispositivo sin configurar. Consulte [Implementar el dispositivo de vRealize Automation](#).
- Cree o identifique sus servidores de IaaS de Windows, y configure sus requisitos previos.
- Instale el agente de administración en sus servidores de IaaS de Windows.

Puede instalar el agente de administración mediante la descarga del archivo .msi tradicional o mediante el proceso silencioso descrito en [Realizar una instalación silenciosa del agente de administración de vRealize Automation](#).

Procedimiento

- 1 Inicie sesión en la consola del dispositivo de vRealize Automation como raíz.
- 2 Vaya al siguiente directorio.
`/usr/lib/vcac/tools/install`
- 3 Abra el archivo de respuesta `ha.properties` en un editor de texto.
- 4 Añada entradas específicas de su implementación en `ha.properties` y guarde y cierre el archivo.

Si lo desea, puede ahorrar tiempo copiando y modificando un archivo `ha.properties` procedente de otra implementación en lugar de editar todo el archivo predeterminado.

- 5 Desde ese mismo directorio, ejecute el siguiente comando para iniciar la instalación.

```
vra-ha-config.sh
```

La instalación podría tardar hasta más de una hora en finalizar, en función del entorno y del tamaño de la implementación.

- 6 (opcional) Una vez finalizada la instalación, revise el archivo de log.

```
/var/log/vcac/vra-ha-config.log
```

El instalador silencioso no guarda datos propietarios en el log, como pueden ser contraseñas, licencias o certificados.

Realizar una instalación silenciosa del agente de administración de vRealize Automation

Puede realizar una instalación del agente de administración de vRealize Automation basada en línea de comandos en cualquier servidor de IaaS de Windows.

La instalación silenciosa del agente de administración consiste en un script de Windows PowerShell en el que se personalizan algunos parámetros de configuración. Después de añadir una configuración específica para su implementación, puede instalar de forma silenciosa el agente de administración en todos los servidores de IaaS de Windows ejecutando copias del mismo script en cada uno.

Requisitos previos

- Cree un dispositivo sin configurar. Consulte [Implementar el dispositivo de vRealize Automation](#).
- Cree o identifique sus servidores de IaaS de Windows, y configure sus requisitos previos.

Procedimiento

- 1 Inicie sesión en el servidor Windows de IaaS mediante una cuenta con derechos de administrador.
- 2 Abra un navegador web en la URL del instalador del dispositivo de vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 3 Haga clic con el botón derecho en el vínculo al archivo de script `InstallManagementAgent.ps1` de PowerShell, y guárdelo en el Escritorio o en una carpeta en el servidor de IaaS de Windows.
- 4 Abra `InstallManagementAgent.ps1` en un editor de texto.
- 5 Cerca de la parte superior del archivo de script, añada los parámetros de configuración específicos de su implementación.
 - URL del dispositivo de vRealize Automation
`https://vrealize-automation-appliance-FQDN:5480`
 - Credenciales de la cuenta de usuario raíz del dispositivo de vRealize Automation
 - Credenciales de usuario del servicio de vRealize Automation, una cuenta de dominio con privilegios de administrador en los servidores de IaaS de Windows
 - La carpeta en la que desea instalar el agente de administración, Archivos de programa (x86) de forma predeterminada
 - (opcional) La huella digital del certificado con formato PEM que usa para la autenticación
- 6 Guarde y cierre `InstallManagementAgent.ps1`.
- 7 Para instalar de forma silenciosa el agente de administración, haga doble clic en `InstallManagementAgent.ps1`.
- 8 (opcional) Para comprobar que la instalación ha finalizado, localice el **Agente de administración de VMware vCloud Automation Center** en la lista Programas y características del Panel de control de Windows, y en la lista de servicios de Windows que se están ejecutando.

Las instalaciones silenciosas de vRealize Automation requieren que prepare con antelación un archivo de respuesta basado en texto.

Cualquier Dispositivo de vRealize Automation recién instalado contiene un archivo de respuesta predeterminado.

`/usr/lib/vcac/tools/install/ha.properties`

Para realizar una instalación silenciosa, debe usar un editor de texto para personalizar la configuración que hay en `ha.properties` a la implementación que desea instalar. A continuación se muestran algunos ejemplos de la configuración y la información que debe añadir.

- La clave de licencia de su vRealize Automation o del conjunto de utilidades
- Los FQDN del nodo del Dispositivo de vRealize Automation
- Credenciales de cuenta de usuario raíz del Dispositivo de vRealize Automation
- Los FQDN de los servidores de IaaS de Windows que actuarán como nodos web, nodos de Manager Service, etc.
- Credenciales de usuario del servicio de vRealize Automation, una cuenta de dominio con privilegios de administrador en los servidores de IaaS de Windows
- Los FQDN de los equilibradores de carga
- Parámetros de base de datos de SQL Server
- Parámetros del agente de proxy para conectarse a recursos de virtualización
- Indicaciones sobre si el instalador silencioso debería tratar de corregir los requisitos previos que faltan del servidor de IaaS de Windows

El instalador silencioso puede corregir muchos de los requisitos previos de Windows que falten. No obstante, el instalador silencioso no puede cambiar algunos problemas de configuración, como no disponer de suficiente CPU.

Para ahorrar tiempo, puede reutilizar y modificar un archivo `ha.properties` que se configuró para otra implementación, una en la que la configuración era similar. Asimismo, cuando realiza una instalación no silenciosa de vRealize Automation mediante el asistente de instalación, el asistente crea y guarda su configuración en el archivo `ha.properties`. El archivo podría ser de utilidad para modificarlo y reutilizarlo en la instalación silenciosa de una implementación similar.

El asistente no guarda la configuración propietaria en el archivo `ha.properties`, como son contraseñas, licencias o certificados.

La línea de comando para la instalación de vRealize Automation

vRealize Automation incluye una interfaz de línea de comandos basada en consola que se utiliza para realizar ajustes en la instalación que podrían ser necesarios tras la instalación inicial.

La interfaz de línea de comandos (CLI) puede ejecutar las tareas de instalación y configuración que dejan de estar disponibles a través de la interfaz basada en navegador tras la instalación inicial. Entre las funciones de CLI se incluyen la nueva comprobación de los requisitos previos, la instalación de los componentes de IaaS, la instalación de certificados o la configuración del nombre de host de vRealize Automation al que los usuarios dirigen su navegador web.

La interfaz de línea de comandos también es útil para los usuarios avanzados que quieran crear el script de determinadas operaciones. Algunas funciones de CLI se utilizan en la instalación silenciosa, por lo que conocer ambas funciones refuerza su conocimiento en la creación de scripts de instalación de vRealize Automation.

vRealize Automation Principios básicos de la línea de comandos de instalación

La interfaz de línea de comandos para la instalación de vRealize Automation incluye operaciones básicas de alto nivel.

Las operaciones básicas muestran los identificadores de nodo de vRealize Automation, ejecutan comandos, notifican el estado de los comandos o muestran la información de ayuda. Para mostrar estas operaciones y sus opciones en la pantalla de la consola, introduzca el siguiente comando sin opciones ni calificadores.

```
vra-command
```

Mostrar los identificadores de nodo

Se necesitan identificadores de nodo de vRealize Automation para que pueda ejecutar comandos en los sistemas de destino correctos. Para mostrar los identificadores de nodo, introduzca el siguiente comando.

```
vra-command list-nodes
```

Anote los identificadores de nodo antes de ejecutar los comandos en determinadas máquinas.

Ejecutar comandos

La mayoría de las funciones de la línea de comando ejecutando un comando en un nodo en el clúster de vRealize Automation. Para ejecutar un comando, utilice la siguiente sintaxis.

```
vra-command execute --node node-ID command-name --parameter-name parameter-value
```

Como se muestra en la sintaxis anterior, muchos comandos requieren parámetros y valores de parámetros seleccionados por el usuario.

Visualización del estado de los comandos

Algunos comandos tardan unos instantes o incluso más en completarse. Para supervisar el progreso de un comando que se ha introducido, introduzca el siguiente comando.

```
vra-command status
```

El comando de estado es especialmente valioso para supervisar una instalación silenciosa, que puede requerir mucho tiempo para las implementaciones de gran tamaño.

Mostrar ayuda

Para mostrar ayuda para todos los comandos disponibles, introduzca el siguiente comando.

```
vra-command help
```

Para mostrar ayuda para un solo comando, introduzca el siguiente comando.

```
vra-command help command-name
```

Nombres de comando para la instalación de vRealize Automation

Los comandos permiten a la consola acceder a muchas tareas de configuración e instalación de vRealize Automation que es probable que usted quiera realizar tras la instalación inicial.

Los ejemplos de comandos disponibles incluyen las siguientes funciones.

- Adición de otro dispositivo de vRealize Automation a una instalación existente
- Configuración del nombre de host al que los usuarios dirigen un navegador web cuando acceden a vRealize Automation
- Creación de la base de datos SQL Server de IaaS
- Ejecución del Comprobador de requisitos previos en un servidor de IaaS de Windows
- Importación de certificados

Para obtener una lista completa de los comandos de vRealize Automation disponibles, inicie sesión en la consola del dispositivo de vRealize Automation e introduzca el siguiente comando.

```
vra-command help
```

Ninguna otra documentación reproduce la larga lista de parámetros y nombres de comandos. Para usar la lista de manera efectiva, identifique un comando que le interese y restrinja su foco de atención introduciendo el siguiente comando.

```
vra-command help command-name
```

La API de instalación de vRealize Automation

La API de REST de instalación de vRealize Automation permite crear instalaciones controladas por software para vRealize Automation.

La API de instalación requiere una versión JSON de las mismas entradas que la instalación basada en CLI obtiene a partir del archivo de respuesta `ha.properties`. Las siguientes directrices le permiten familiarizarse con el funcionamiento de la API. A partir de ahí, debería poder diseñar llamadas programáticas en la API para instalar vRealize Automation.

- Para acceder a la documentación de la API, dirija un navegador web a la siguiente página de dispositivos de vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480/config`

Se necesita un dispositivo de vRealize Automation que no esté configurado. Consulte [Implementar el dispositivo de vRealize Automation](#).

- Para experimentar con la instalación basada en la API, localice y amplíe el siguiente comando PUT.

`PUT /vra-install`

- Copie la versión JSON sin rellenar del cuadro **install_json** al editor de texto. Rellene los valores de respuesta tal como lo haría para el archivo `ha.properties`. Cuando las respuestas JSON estén listas, vuelva a copiar el código en **install_json** y sobrescriba la versión JSON sin rellenar.

Si lo prefiere, puede editar la siguiente plantilla JSON y copiar el resultado en **install_json**.

`/usr/lib/vcac/tools/install/installationProperties.json`

También puede convertir un archivo `ha.properties` completado en JSON o viceversa.

- En el cuadro de acción, seleccione **validate** (Validar) y haga clic en **Try It Out** (Probar).

La acción de validación ejecuta el comprobador de requisitos previos y reparador de vRealize Automation.

- La respuesta de validación incluye un ID de comando alfanumérico que puede insertar en el siguiente comando GET.

`GET /commands/command-id/aggregated-status`

La respuesta al comando GET incluye el progreso de la operación de validación.

- Si la validación se realiza correctamente, puede ejecutar la instalación real repitiendo el proceso. En el cuadro de acción, seleccione **install** (instalar) en lugar de **validate** (validar).

La instalación puede durar mucho según el tamaño de la implementación. De nuevo, localice el ID de comando y utilice el comando GET de estado agregado para obtener el progreso de la instalación. La respuesta GET puede parecerse al siguiente ejemplo.

```
"progress": "78%", "counts": {"failed": 0, "completed": 14, "total": 18,
"queued": 3, "processing": 1}, "failed-commands": 0
```

- Si ocurre algún problema en la instalación, puede activar la recopilación de logs para todos los nodos mediante el siguiente comando.

`PUT /commands/log-bundle`

De forma similar a la instalación, el ID de comando alfanumérico devuelto permite supervisar el estado de la recopilación de logs.

Convertir entre las propiedades silenciosas de vRealize Automation y JSON

Para las instalaciones silenciosas basadas en la CLI o en la API de vRealize Automation, se puede convertir un archivo de respuesta de propiedades completado en JSON o viceversa. La instalación silenciosa de la CLI requiere el archivo de propiedades, mientras que la API requiere el formato JSON.

Requisitos previos

Un archivo de respuesta de propiedades completado o un archivo JSON completado

`/usr/lib/vcac/tools/install/ha.properties`

o

`/usr/lib/vcac/tools/install/installationProperties.json`

Procedimiento

1 Inicie sesión en la consola del dispositivo de vRealize Automation como usuario raíz.

2 Ejecute el script del convertidor correspondiente.

- Convertir JSON en propiedades

```
/usr/lib/vcac/tools/install/convert-properties --from-json
installationProperties.json
```

El script crea un nuevo archivo de propiedades con la marca de hora en el nombre; por ejemplo:

`ha.2016-10-17_13.02.15.properties`

- Convertir propiedades en JSON

```
/usr/lib/vcac/tools/install/convert-properties --to-json ha.properties
```

El script crea un nuevo archivo `installationProperties.json` con la marca de hora en el nombre; por ejemplo:

`installationProperties.2016-10-17_13.36.13.json`

Resultados

También se puede mostrar la Ayuda para el script.

```
/usr/lib/vcac/tools/install/convert-properties --help
```

Tareas posteriores a la instalación de vRealize Automation

7

Después de instalar vRealize Automation, es posible que deba ocuparse de algunas tareas posteriores a la instalación.

Este capítulo incluye los siguientes temas:

- [No cambiar la zona horaria de vRealize Automation](#)
- [Configurar el cifrado compatible con el Estándar federal de procesamiento de información \(FIPS\)](#)
- [Habilitar la conmutación por error automática de Manager Service](#)
- [Conmutación por error automática de una base de datos de PostgreSQL de vRealize Automation](#)
- [Reemplazar los certificados autofirmados por certificados proporcionados por una entidad](#)
- [Cambiar nombres de host y direcciones IP](#)
- [Eliminar un nodo de dispositivo de vRealize Automation](#)
- [Instalar el agente de vRealize Log Insighten servidores de IaaS](#)
- [Cambiar el puerto de proxy de VMware Remote Console](#)
- [Cambiar el FQDN del dispositivo de vRealize Automation por el FQDN original](#)
- [Configurar grupo de disponibilidad AlwaysOn de SQL](#)
- [Añadir controladores de interfaz de red después de instalar vRealize Automation](#)
- [Configurar rutas estáticas](#)
- [Acceder a la administración de revisiones](#)
- [Configurar el acceso al tenant predeterminado](#)

No cambiar la zona horaria de vRealize Automation

Deje siempre la zona horaria de vRealize Automation establecida como Etc/UTC, aunque la interfaz de administración del dispositivo de vRealize Automation ofrece una opción para cambiarla.

Se sabe que el uso de una zona horaria distinta de Etc/UTC provoca errores inusuales, como migraciones con errores y paquetes de logs que no contienen entradas de todos los nodos de vRealize Automation.

La opción de la interfaz de administración del dispositivo de vRealize Automation que debe evitar se encuentra en **Sistema > Zona horaria**.

Configurar el cifrado compatible con el Estándar federal de procesamiento de información (FIPS)

Puede habilitar o deshabilitar la criptografía compatible con el Estándar federal de procesamiento de información (Federal Information Processing Standard, FIPS) 140–2 para el tráfico de red entrante y saliente del dispositivo de vRealize Automation.

Para cambiar la configuración del estándar FIPS, es necesario reiniciar vRealize Automation. FIPS está deshabilitado de manera predeterminada.

Procedimiento

- 1 Inicie sesión como raíz en la interfaz de administración del dispositivo de vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`

- 2 Haga clic en **vRA > Configuración del host**.

- 3 Cerca de la parte superior derecha, haga clic en el botón para habilitar o deshabilitar FIPS.

Si está habilitado, el tráfico de red entrante y saliente del dispositivo de vRealize Automation en el puerto 443 utiliza el cifrado compatible con FIPS 140–2. Independientemente de la configuración de FIPS, vRealize Automation utiliza algoritmos compatibles con AES–256 para la protección de los datos almacenados en el dispositivo de vRealize Automation.

Nota Esta versión de vRealize Automation solo habilita parcialmente el cumplimiento del estándar FIPS porque algunos componentes internos no utilizan todavía módulos criptográficos certificados. En los casos en que los módulos certificados no se hayan implementado todavía, se utilizan algoritmos compatibles con AES–256.

- 4 Haga clic en **Sí** para reiniciar vRealize Automation.

Resultados

También puede configurar FIPS desde una sesión de la consola del dispositivo de vRealize Automation como raíz mediante los siguientes comandos.

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Habilitar la conmutación por error automática de Manager Service

La conmutación por error automática de Manager Service está deshabilitada de forma predeterminada si instala o actualiza Manager Service con el instalador estándar de Windows de vRealize Automation.

Para habilitar la conmutación por error automática de Manager Service después de ejecutar el instalador de Windows estándar, realice los siguientes pasos.

En una configuración de varios nodos, solo es necesario realizar los pasos una vez, en cualquier nodo del dispositivo de vRealize Automation.

Procedimiento

1 Inicie sesión como raíz en una sesión de consola en el dispositivo de vRealize Automation.

2 Vaya al siguiente directorio.

```
/usr/lib/vcac/tools/vami/commands
```

3 Introduzca el siguiente comando.

```
python ./manager-service-automatic-failover ENABLE
```

Resultados

Si, por el contrario, tiene que deshabilitar la conmutación por error automática en una implementación de IaaS, introduzca el siguiente comando.

```
python ./manager-service-automatic-failover DISABLE
```

Acerca de la conmutación por error automática de Manager Service

Manager Service de IaaS de vRealize Automation se puede configurar para que conmute en una copia de seguridad cuando se detenga la instancia principal de Manager Service.

A partir de vRealize Automation 7.3, ya no es necesario iniciar o detener manualmente Manager Service en cada servidor de Windows para controlar cuál actúa como principal o como copia de seguridad. La conmutación por error automática de Manager Service está habilitada de forma predeterminada en los siguientes casos.

- Cuando se instala vRealize Automation de forma silenciosa o con el asistente de instalación.
- Cuando se actualiza IaaS a través de la interfaz de administración o con el script de actualización automático.

La conmutación por error no está habilitada cuando se utiliza el instalador estándar basado en Windows para añadir un host de Manager Service o actualizar IaaS. Para habilitarla, consulte [Habilitar la conmutación por error automática de Manager Service](#).

Cuando la conmutación por error automática está habilitada, Manager Service se inicia automáticamente en todos los hosts de Manager Service, incluidas las copias de seguridad. La función de conmutación por error automática permite que los hosts se supervisen entre sí de forma transparente y realicen la conmutación por error cuando sea necesario. La función requiere que el servicio de Windows se esté ejecutando en todos los hosts.

Nota No está obligado a utilizar la conmutación por error automática. Puede deshabilitarla y seguir iniciando y deteniendo manualmente el servicio de Windows para controlar qué host actúa como principal o copia de seguridad. Si opta por el método de conmutación por error manual, solo tiene que iniciar el servicio en un host cada vez. Con la conmutación por error automática deshabilitada, al ejecutar el servicio simultáneamente en varios servidores de IaaS, vRealize Automation no se podrá usar.

No intente habilitar o deshabilitar la conmutación por error automática de forma selectiva. Siempre debe estar sincronizada como activada o desactivada, en cada host de Manager Service en una implementación de IaaS.

Si le da la sensación de que la conmutación por error automática no está funcionando, consulte *Actualización de vRealize Automation 7.1 o 7.2 a 7.3* para ver algunas sugerencias de solución de problemas.

Para obtener información sobre cómo equilibrar la carga de los hosts de Manager Service, consulte [Equilibrio de carga de vRealize Automation](#).

Conmutación por error automática de una base de datos de PostgreSQL de vRealize Automation

En una implementación de vRealize Automation de alta disponibilidad, algunas configuraciones permiten que la base de datos de PostgreSQL integrada de vRealize Automation conmute por error automáticamente.

La conmutación por error automática se habilita de forma silenciosa en las siguientes condiciones.

- La implementación de alta disponibilidad incluye tres dispositivos de vRealize Automation.
No se admite la conmutación por error automática con solo dos dispositivos.
- La replicación de base de datos se establece como modo síncrono en la pestaña Clúster de la interfaz de administración de vRealize Automation.

Por lo general, debe evitar realizar una conmutación por error manual cuando está habilitada la conmutación por error automática. Sin embargo, cuando se producen algunos problemas de nodo, la conmutación por error automática no llega a producirse incluso estando habilitada. En este caso, compruebe si necesita realizar una conmutación por error manual.

- 1 Cuando el nodo de base de datos de PostgreSQL principal falle, espere 5 minutos para que el resto del clúster se estabilice.

- 2 En un nodo de dispositivo de vRealize Automation que permanezca activo, abra un navegador en la siguiente dirección URL.

`https://vrealize-automation-appliance-FQDN:5434/api/status`

- 3 Busque `manualFailoverNeeded`.
- 4 Si `manualFailoverNeeded` es "true", realice una conmutación por error manual.

Para obtener información acerca de cómo realizar una conmutación por error manual, consulte *Administración de vRealize Automation*.

Reemplazar los certificados autofirmados por certificados proporcionados por una entidad

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*.

Cambiar nombres de host y direcciones IP

En general, deberá mantener los nombres de host, los FQDN y las direcciones IP que haya planificado para los sistemas vRealize Automation. Es posible realizar cambios tras la instalación, pero puede resultar complejo.

- Si cambia el nombre de host de la máquina de Windows que aloja la base de datos de SQL Server de IaaS, consulte *Administración de vRealize Automation*.
- Cuando se restauran los componentes de IaaS, si se cambia el nombre de un host, el host web de IaaS, el host de Manager Service o sus equilibradores de carga respectivos se pueden ver afectados. Restaure estos hosts o los equilibradores de carga de acuerdo con las instrucciones de copia de seguridad y restauración de *vRealize Suite*.

Para cambiar la dirección IP o un nombre de host del dispositivo de vRealize Automation, consulte las siguientes secciones.

Cambiar el nombre de host del dispositivo de vRealize Automation

Al mantener un entorno o una red, es posible que deba asignar un nombre de host diferente a un dispositivo de vRealize Automation.

Importante El cambio de nombre hace que vRealize Automation se desconecte durante varios minutos.

Se aplican los mismos pasos para los dispositivos independientes, principales y de réplica de vRealize Automation.

Procedimiento

- 1 En DNS, cree otro registro con el nuevo nombre de host del nodo.
No suprima todavía el registro de DNS existente con el nombre de host antiguo.
- 2 Espere que ocurra la replicación DNS y la distribución de zona.
- 3 Inicie sesión como raíz en la línea de comandos del dispositivo de vRealize Automation.
- 4 Ejecute el siguiente comando.

```
vcac-config hostname-change --host new-hostname --certificate certificate-file-name
```

De forma opcional, puede emplearse un archivo de certificado a menos que se haya utilizado el nombre anterior de host del dispositivo en un certificado. En ese caso, proporcione un certificado actualizado con el nuevo nombre de host.

Cuando se especifica un archivo de certificado, el comando de cambio de nombre también importa el certificado y devuelve el identificador de este.

El archivo de certificado debe estar en el mismo formato que la salida de texto del comando de la API de `/config/ssl/generate-certificate` y contener el nuevo nombre DNS en el campo SAN.

- 5 Espere 15 minutos o más hasta que se complete el proceso de cambio de nombre. Las acciones de comando tardan varios minutos, a los que hay que sumar algunos minutos más para el nuevo registro del servicio.
- 6 Si se ha utilizado el nombre anterior de host del dispositivo con un equilibrador de carga en un entorno de alta disponibilidad, compruebe el equilibrador de carga y reconfigúrelo con el nuevo nombre.
- 7 En DNS, suprima el registro DNS existente con el antiguo nombre de host.

Resultados

Si tiene problemas al cambiar un nombre de host, intente realizar los distintos procedimientos de la documentación de vRealize Automation 7.3.

Cambiar la dirección IP del dispositivo de vRealize Automation

Cuando se mantiene un entorno o una red, es posible que tenga que asignar una dirección IP diferente a un dispositivo de vRealize Automation existente.

Requisitos previos

- Como precaución, tome snapshots de los dispositivos de vRealize Automation y los servidores de IaaS.
- Desde una sesión de consola como raíz en los dispositivos de vRealize Automation, inspeccione las entradas del archivo `/etc/hosts`.

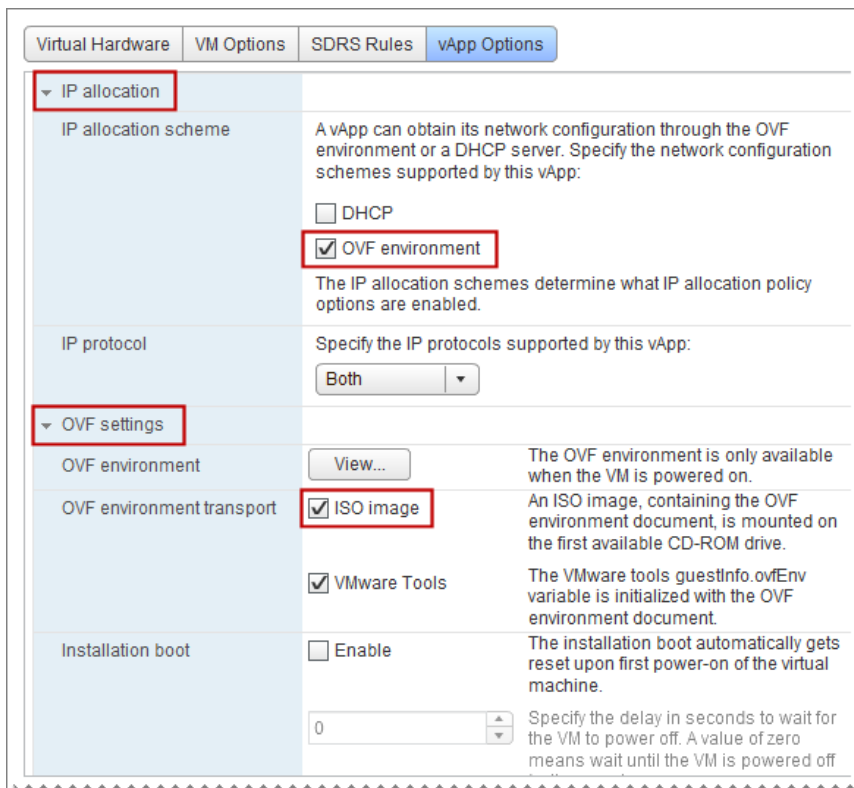
Busque las asignaciones de dirección que pueden entrar en conflicto con el nuevo plan de direcciones IP y haga los cambios que sean necesarios.

En todos los servidores de IaaS, repita el proceso para el archivo `Windows\system32\drivers\etc\hosts`.

- Apague todos los dispositivos de vRealize Automation.
- Detenga todos los servicios de vRealize Automation en los servidores de IaaS.

Procedimiento

- 1 En vSphere, busque el dispositivo de vRealize Automation que desee cambiar y seleccione **Acciones > Editar configuración**.
- 2 Haga clic en **Opciones de vApp**.
- 3 Expanda la **asignación de IP** y habilite la opción de **entorno de OVF**.
- 4 Expanda la **configuración de OVF** y habilite la opción de **imagen ISO**.



- 5 Haga clic en **Aceptar**.
- 6 Inicie el dispositivo de vRealize Automation que va a cambiar.
- 7 Inicie sesión como raíz en la interfaz de administración del dispositivo de vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 8 Haga clic en la pestaña **Red**.
- 9 Debajo de las pestañas, haga clic en **Dirección**.

- 10 Actualice la dirección IP.
- 11 En la parte superior derecha, haga clic en **Guardar configuración**.
- 12 Apague el dispositivo de vRealize Automation que va a cambiar.
- 13 En DNS, actualice las entradas que correspondan a las nuevas direcciones IP.

Actualice solo los registros de tipo A existentes. No cambie los FQDN.

Si utiliza un equilibrador de carga, actualice la configuración de la IP del equilibrador de carga para los nodos de back-end, los grupos de servicios y los servidores virtuales según sea necesario.
- 14 Espere que ocurra la replicación DNS y la distribución de zona.
- 15 Inicie todos los dispositivos de vRealize Automation.
- 16 Inicie los servicios de vRealize Automation en los servidores de IaaS.
- 17 Inicie sesión como raíz en la interfaz de administración del dispositivo de vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`
- 18 Compruebe el estado del dispositivo de vRealize Automation en las siguientes áreas.
 - Estado de la conexión de base de datos en **Clúster**
 - Estado de RabbitMQ en **vRA > Mensajes**
 - Estado de Xenon en **vRA > Xenon**
 - Todos los servicios que aparezcan como REGISTRADO en **Servicios**

Ajuste de la base de datos SQL para un nombre de host modificado

Debe revisar las opciones de configuración si mueve la base de datos SQL de IaaS de vRealize Automation a un nombre de host distinto.

En el mismo nombre de host, puede restaurar la base de datos SQL a partir de una copia de seguridad sin pasos adicionales requeridos. Si restaura a un nombre de host diferente, debe editar los archivos de configuración para realizar otros cambios.

Consulte [Artículo 2074607 de la base de conocimientos de VMware](#) para conocer los cambios que se deben realizar al mover la base de datos SQL a otro nombre de host.

Cambiar una dirección IP del servidor de IaaS

Cuando se mantiene un entorno o una red, es posible que tenga que asignar una dirección IP diferente a un servidor Windows de IaaS de vRealize Automation existente.

Requisitos previos

- Si tiene que cambiar la dirección IP del dispositivo de vRealize Automation, hágalo en primer lugar. Consulte [Cambiar la dirección IP del dispositivo de vRealize Automation](#).

- Como precaución, tome snapshots de los dispositivos de vRealize Automation y los servidores de IaaS.
- Desde una sesión de consola como raíz en el dispositivo de vRealize Automation, inspeccione las entradas del archivo `/etc/hosts`.

Busque las asignaciones de dirección que pueden entrar en conflicto con el nuevo plan de direcciones IP y haga los cambios que sean necesarios.

En todos los servidores de IaaS, repita el proceso para el archivo `Windows\system32\drivers\etc\hosts`.

- Apague el dispositivo de vRealize Automation.
- Detenga todos los servicios de vRealize Automation en los servidores de IaaS.

Procedimiento

- 1 Inicie sesión en el servidor de IaaS con una cuenta que tenga derechos de administrador.

- 2 En Windows, cambie la dirección IP.

Busque la dirección IP en la configuración del adaptador de red de Windows, en las propiedades del protocolo de Internet.

- 3 Actualice el DNS local con los cambios.

Al actualizar el DNS, se asegura de que los servidores Windows de IaaS se puedan encontrar entre sí y que podrá volver a conectarse a un servidor de Windows si se desconecta.

- 4 En el host de Manager Service, examine el siguiente archivo en un editor de texto.

carpeta de instalación\vCAC\Server\ManagerService.exe.config

La carpeta de instalación predeterminada es `C:\Archivos de programa (x86)\VMware`.

Compruebe las direcciones IP o los FQDN de los dispositivos de vRealize Automation y los servidores Windows de IaaS.

- 5 En todos los servidores Windows de IaaS, examine el siguiente archivo en un editor de texto.

carpeta de instalación\vCAC\Management Agent
\VMware.IaaS.Management.Agent.exe.Config

Compruebe la dirección IP o el FQDN del dispositivo de vRealize Automation.

- 6 Inicie sesión en el host de SQL Server.

- 7 Compruebe que la dirección de repositorio está configurada correctamente para utilizar el FQDN en la columna `ConnectionString`.

Por ejemplo, abra SQL Management Studio y ejecute la siguiente consulta.

```
"SELECT Name, ConnectionString FROM [nombre de base de datos].
[DynamicOps.RepositoryModel].[Models]"
```

- 8 Inicie el dispositivo de vRealize Automation.

- 9 Inicie los servicios de vRealize Automation en los servidores de IaaS.
- 10 Revise los archivos de log para comprobar que el agente, el trabajo de DEM, Manager Service y los servicios de host web se han iniciado correctamente.
- 11 Inicie sesión en vRealize Automation como usuario con la función de administrador de infraestructura.
- 12 Desplácese hasta **Infraestructura > Supervisión > Distributed Execution Status** (Estado de ejecución distribuida) y compruebe que todos los servicios se estén ejecutando.
- 13 Para probar que toda funciona correctamente, compruebe los servicios del dispositivo, realice pruebas de aprovisionamiento o utilice la herramienta de prueba de producción de vRealize.

Cambiar un nombre de host del servidor de IaaS

Cuando se mantiene un entorno o una red, es posible que tenga que asignar un nombre de host diferente a un servidor Windows de IaaS de vRealize Automation existente.

Procedimiento

- 1 Cree una snapshot del servidor de IaaS.
- 2 En el servidor de IaaS, utilice el Administrador de IIS para detener los grupos de aplicaciones de vRealize Automation: repositorio, VMware vRealize Automation y Wapi.
- 3 En el servidor de IaaS, utilice Herramientas administrativas > Servicios para detener todos los agentes, los DEM y los servicios de vRealize Automation.
- 4 Cree un registro adicional en el DNS con el nuevo nombre de host.
No suprima todavía el registro de DNS existente con el nombre de host antiguo.
- 5 Espere que ocurra la replicación DNS y la distribución de zona.
- 6 En el servidor de IaaS, cambie el nombre de host, pero no reinicie cuando se le solicite.
Busque el nombre de host en las propiedades del sistema Windows, en la configuración del nombre de equipo, el dominio y el grupo de trabajo.
Cuando se le pida que reinicie, haga clic en la opción para reiniciar más tarde.
- 7 Si ha usado el nombre de host antiguo para generar certificados, actualice los certificados.
Para obtener información sobre cómo actualizar certificados, consulte *Administración de vRealize Automation*.

- 8 Utilice un editor de texto para buscar y actualizar el nombre de host en los archivos de configuración.

Realice las actualizaciones en función del nombre de host del servidor de IaaS que haya cambiado. En una implementación distribuida de alta disponibilidad, podría necesitar acceder a más de un servidor. No hay ninguna actualización si cambia el nombre de host de un orquestador de DEM o un trabajo de DEM.

Nota Actualice únicamente el anterior nombre de host del servidor Windows. Si en su lugar encuentra un nombre del equilibrador de carga, conserve el nombre del equilibrador de carga.

Tabla 7-1. Archivos que se actualizan al cambiar el nombre de host de un nodo web

Servidor de IaaS	Ruta de acceso	Archivo
Nodos web	<i>carpeta-instalación</i> \Server\Website	Web.config
	<i>carpeta-instalación</i> \Server\Website\Cafe	Vcac-Config.exe.config
	<i>carpeta-instalación</i> \Web API	Web.config
	<i>carpeta-instalación</i> \Web API\ConfigTool	Vcac-Config.exe.config
Nodo con el componente de Model Manager instalado	<i>carpeta-instalación</i> \Server\Model Manager Data	Repoutil.exe.config
	<i>carpeta-instalación</i> \Server\Model Manager Data\Cafe	Vcac-Config.exe.config
Nodos de Manager Service	<i>carpeta-instalación</i> \Server	ManagerService.exe.config
Nodos del orquestador de DEM	<i>carpeta-instalación</i> \Distributed Execution Manager\dem	DynamicOps.DEM.exe.config
Nodos del trabajo de DEM	<i>carpeta-instalación</i> \Distributed Execution Manager\DEM-name	DynamicOps.DEM.exe.config
Nodos de agente	<i>carpeta-instalación</i> \Agents\agent-name	RepoUtil.exe.config
	<i>carpeta-instalación</i> \Agents\agent-name	VRMAgent.exe.config

Tabla 7-2. Archivos que se actualizan al cambiar el nombre de host de un nodo de Manager Service

Servidor de IaaS	Ruta de acceso	Archivo
Nodos del orquestador de DEM	<i>carpeta-instalación</i> \Distributed Execution Manager\ <i>DEM-name</i>	DynamicOps.DEM.exe.config
Nodos del trabajo de DEM	<i>carpeta-instalación</i> \Distributed Execution Manager\dem	DynamicOps.DEM.exe.config
Nodos de agente	<i>carpeta-instalación</i> \Agents\ <i>agent-name</i>	VRMAgent.exe.config

Tabla 7-3. Archivos que se actualizan al cambiar el nombre de host de un nodo de agente

Servidor de IaaS	Ruta de acceso	Archivo
Nodo de agente	<i>carpeta-instalación</i> \Agents\ <i>agent-name</i>	VRMAgent.exe.config

- 9 Reinicie el servidor de IaaS en el que ha cambiado el nombre de host.
- 10 Inicie los grupos de aplicaciones de vRealize Automation que detuvo anteriormente.
- 11 Inicie los DEM, los agentes y los servicios de vRealize Automation que detuvo anteriormente.
- 12 Si se ha utilizado el nombre anterior de host del servidor de IaaS con un equilibrador de carga en un entorno de alta disponibilidad, compruebe el equilibrador de carga y reconfigúrelo con el nuevo nombre.
- 13 En DNS, suprima el registro DNS existente con el antiguo nombre de host.
- 14 Espere que ocurra la replicación DNS y la distribución de zona.
- 15 Si ha cambiado el nombre de un host de Manager Service, realice los siguientes pasos adicionales.
 - a Actualice los agentes de software en las máquinas virtuales existentes.
 - b Recree los archivos ISO o las plantillas que contengan un agente invitado.

Pasos siguientes

Valide que vRealize Automation esté listo para su uso. Consulte la documentación de [Restauración y copia de seguridad de vRealize Suite](#).

Establecer la URL de inicio de sesión de vRealize Automation como un nombre personalizado

Si desea que los usuarios de vRealize Automation inicien sesión en un nombre de URL distinto del nombre del equilibrador de carga o del dispositivo de vRealize Automation, siga los pasos de personalización antes y después de la instalación.

Procedimiento

- 1 Antes de instalar, prepare un certificado que incluya la instancia de CNAME que desee, así como los nombres del equilibrador de carga y del dispositivo de vRealize Automation.
- 2 Instale vRealize Automation y escriba el nombre del equilibrador de carga o del dispositivo como de costumbre. Durante la instalación, importe el certificado personalizado.
- 3 Después de la instalación, en el DNS, cree un alias de CNAME de nombre común y apúntelo a la dirección VIP del equilibrador de carga o el dispositivo.
- 4 Inicie sesión en la interfaz de administrador del dispositivo de vRealize Automation como raíz.
`https://vrealize-automation-appliance-FQDN:5480`
- 5 En **vRA > Configuración del host**, cambie **Nombre del host** a la instancia de CNAME que haya elegido.

Eliminar un nodo de dispositivo de vRealize Automation

Durante el mantenimiento de un entorno de alta disponibilidad, es posible que se deba eliminar un nodo del dispositivo vRealize Automation con errores del clúster.

Para eliminar un nodo, siga las directrices del [artículo 2149866 de la Base de conocimientos de VMware](#).

Instalar el agente de vRealize Log Insight en servidores de IaaS

Los servidores Windows en una configuración IaaS de vRealize Automation no incluyen el agente de vRealize Log Insight de forma predeterminada.

vRealize Log Insight proporciona indexación y agregación de logs, y puede recopilar, importar y analizar logs para exponer problemas del sistema. Si quiere capturar y analizar logs desde los servidores de IaaS mediante vRealize Log Insight, debe instalar por separado el agente de vRealize Log Insight para Windows.

Para obtener más información, consulte la *guía de administración del agente de VMware vRealize Log Insight*.

Las unidades de Dispositivo de vRealize Automation incluyen el agente vRealize Log Insight de forma predeterminada.

Cambiar el puerto de proxy de VMware Remote Console

Si su sitio se bloquea o, por el contrario, reserva el puerto 8444, puede cambiar el puerto de proxy predeterminado utilizado por VMware Remote Console.

Procedimiento

- 1 Acceda al símbolo del sistema del dispositivo de vRealize Automation como raíz.

- 2 Abra el siguiente archivo en un editor de texto.

```
/etc/vcac/security.properties
```

- 3 Cambie `consoleproxy.service.port` de su valor predeterminado de 8444 a un puerto sin utilizar.
- 4 Guarde y cierre `security.properties`.
- 5 Reinicie el dispositivo de vRealize Automation.

Resultados

En un entorno de alta disponibilidad, realice el mismo cambio a todos los dispositivos de vRealize Automation.

Cambiar el FQDN del dispositivo de vRealize Automation por el FQDN original

En algunos casos, el FQDN de un dispositivo de vRealize Automation se puede cambiar si no lo quiere. Por ejemplo, el FQDN cambia si crea un directorio de autenticación integrada de Windows (IWA) para un dominio distinto al dominio en el que se encuentra el dispositivo.

Si crea un directorio de IWA para otro dominio, realice los siguientes pasos para cambiar el FQDN del dispositivo por el FQDN original.

Procedimiento

- 1 Inicie sesión en vRealize Automation y cree el directorio de IWA como lo haría normalmente. Consulte *Configuración de vRealize Automation*.

- 2 Si se trata de un entorno de HA, debe seguir también los pasos sobre la configuración de la administración de directorios para HA que se describen en *Configuración de vRealize Automation*.

- 3 Al crear un directorio de IWA para un dominio distinto al dominio en el que se encuentra un dispositivo en silencio, cambia el FQDN del dispositivo.

Por ejemplo, `va1.domain1.local` cambia a `va1.domain2.local` cuando se crea un directorio de IWA para `domain2.local`.

Puede deshacer el cambio si nombra de nuevo cada dispositivo como su FQDN original. Consulte el procedimiento asociado en [Cambiar nombres de host y direcciones IP](#).

- 4 Una vez que los dispositivos vuelvan a estar totalmente conectados con su FQDN original, inicie sesión en cada nodo de IaaS y realice los siguientes pasos.

- a Abra el siguiente archivo en un editor de texto.

```
C:\Program Files (x86)\VMware\VCAC\Management Agent
\VMware.IaaS.Management.Agent.exe.Config
```

- b Cambie cada FQDN de `endpoint address=` del dispositivo por el FQDN original.

Por ejemplo, de:

```
<endpoint address="https://va1.domain2.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain2.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

a:

```
<endpoint address="https://va1.domain1.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain1.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

c Guardar y cerrar VMware.IaaS.Management.Agent.exe.Config.

- 5 Inicie sesión como raíz en la interfaz de administración del dispositivo de vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`

- 6 Desplácese hasta **vRA > Mensajes** y haga clic en **Restablecer clúster RabbitMQ**.
- 7 Una vez que finalice el restablecimiento, inicie sesión en cada interfaz de administración de dispositivos.
- 8 Desplácese hasta **Clúster** y compruebe que todos los nodos están conectados al clúster.

Configurar grupo de disponibilidad AlwaysOn de SQL

Debe realizar cambios en la configuración si configura el grupo de disponibilidad AlwaysOn (AlwaysOn Availability Group, AAG) de SQL después de instalar vRealize Automation.

Si configura AAG de SQL después de la instalación, debe seguir los pasos que se indican en [Artículo 2074607 de la base de conocimientos de VMware](#) para configurar vRealize Automation con el FQDN del agente de escucha de AAG como el host de SQL Server.

Añadir controladores de interfaz de red después de instalar vRealize Automation

vRealize Automation admite varios controladores de interfaz de red (Network Interface Controller, NIC). Tras la instalación, puede añadir NIC al dispositivo de vRealize Automation o la instancia de Windows Server de IaaS.

Es posible que se necesiten varios NIC para algunas implementaciones de vRealize Automation, por ejemplo:

- Desea disponer de redes de infraestructura y de usuario distintas.
- Necesita un NIC adicional para que los servidores de IaaS puedan unirse a un dominio de Active Directory.

Para obtener más información sobre escenarios con varios NIC, consulte esta [publicación de blog de VMware Cloud Management](#).

Para tres o más NIC, tenga en cuenta las siguientes limitaciones.

- VIDM necesita acceder a la base de datos de Postgres y Active Directory.
- En un clúster de alta disponibilidad, VIDM necesita acceder a la URL del equilibrador de carga.
- Las conexiones de VIDM anteriores deben proceder de los dos primeros NIC.
- Los NIC que siguen al segundo NIC no deben utilizarse ni ser reconocidos por VIDM.
- Los NIC que siguen al segundo NIC no deben utilizarse para conectarse a Active Directory.

Utilice el primer o el segundo NIC al configurar un directorio en vRealize Automation.

Requisitos previos

Instale vRealize Automation por completo en el entorno de vCenter.

Procedimiento

- 1 En vCenter, agregue los NIC a cada dispositivo de vRealize Automation.
 - a Haga clic con el botón secundario en el dispositivo y seleccione **Editar configuración**.
 - b Agregue los NIC de VMXNETn.
 - c Si el dispositivo está encendido, reinícielo.

- 2 Inicie sesión en la interfaz de administración del dispositivo de vRealize Automation como raíz.

`https://vrealize-automation-appliance-FQDN:5480`

- 3 Seleccione **Red** y compruebe que haya varios NIC disponibles.
- 4 Seleccione **Dirección** y configure la dirección IP para los NIC.

Tabla 7-4. Ejemplo de configuración de NIC

Configuración	Valor
Tipo de dirección IPv4	Estático
Dirección IPv4	172.22.0.2
Máscara de red	255.255.255.0

- 5 Compruebe que todos los nodos de vRealize Automation pueden resolverse mutuamente por nombre de DNS.
- 6 Compruebe que todos los nodos de vRealize Automation pueden acceder a cualquier FQDN con equilibrio de carga para los componentes de vRealize Automation.

- 7 Si utiliza DNS de cerebro dividido, compruebe que todos los VIP y los nodos de vRealize Automation tengan el mismo FQDN en DNS para el VIP y la IP de cada nodo.
- 8 En vCenter, agregue los NIC a instancias de Windows Server de IaaS.
 - a Haga clic con el botón secundario en el servidor de IaaS y seleccione **Editar configuración**.
 - b Añada los NIC a la máquina virtual del servidor de IaaS.
- 9 En Windows, configure los NIC del servidor de IaaS agregado y sus direcciones IP. Si es necesario, consulte la documentación de Microsoft.

Pasos siguientes

(Opcional) Si necesita rutas estáticas, consulte [Configurar rutas estáticas](#).

Configurar rutas estáticas

Al añadir los NIC a una instalación de vRealize Automation, si necesita rutas estáticas, abra una sesión del símbolo del sistema para configurarlas.

Requisitos previos

Añada varios NIC a los dispositivos de vRealize Automation o las instancias de Windows Server de IaaS.

Procedimiento

- 1 Inicie sesión en la línea de comandos del dispositivo de vRealize Automation como raíz.
- 2 Abra el archivo de rutas en un editor de texto.

```
/etc/sysconfig/network/routes
```

- 3 Busque la línea default de la puerta de enlace predeterminada, pero no la modifique.

Nota Cuando sea necesario cambiar la puerta de enlace predeterminada, utilice la interfaz de administración de vRealize Automation.

- 4 Debajo de la línea default, añada nuevas líneas para las rutas estáticas. Por ejemplo:

```
default 10.10.10.1 - -
172.30.30.0 192.168.100.1 255.255.255.0 eth0
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

- 5 Guarde y cierre el archivo de rutas.
- 6 Reinicie el dispositivo.
- 7 En los clústeres de alta disponibilidad, repita el proceso para cada dispositivo.
- 8 Inicie sesión en la instancia de Windows Server de IaaS como administrador.
- 9 Abra un símbolo del sistema como administrador.

- 10 Para configurar una ruta estática, escriba el comando `route -p add`, donde `-p` conserva la ruta estática tras cada reinicio. Por ejemplo:

```
C:\Windows\system32> route -p add 172.30.30.0 mask 255.255.255.0 192.168.100.1 metric 1
OK!
```

Para obtener más información sobre la configuración de rutas estáticas en Windows, consulte la documentación de Microsoft.

Acceder a la administración de revisiones

Es posible que el soporte técnico para la instalación de vRealize Automation incluya una revisión de software que se instala o se quita mediante la interfaz de administración de dispositivos de vRealize Automation.

Puesto que se pueden producir problemas casi en tiempo real, se ofrecen revisiones, requisitos previos e instrucciones de instalación en [Base de conocimientos de VMware](#). Por ejemplo, se realiza un seguimiento del [artículo 70911 de la base de conocimientos de VMware](#) y se actualiza con la información de la revisión de vRealize Automation 7.6 más reciente.

La interfaz de revisiones no puede aplicar la revisión de los siguientes componentes de vRealize Automation.

- El agente de administración.
- Agentes que no sean de vSphere, como XenServer, VDI o Hyper-V.

Procedimiento

- 1 Inicie sesión en la interfaz de administración del dispositivo de vRealize Automation como raíz.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Haga clic en **vRA > Revisiones**.
- 3 En Administración de revisiones, haga clic en la opción que necesite y siga las indicaciones.

Opción	Descripción
Nueva revisión	Instala una nueva revisión que se ha descargado.
Revisiones instaladas	Añade la revisión instalada más reciente a los nodos del clúster recién añadidos.
Revertir	Quita la revisión instalada más reciente y revierte vRealize Automation al nivel de revisión anterior.
Historial	Permite examinar la lista de revisiones instaladas y quitadas.

Para habilitar o deshabilitar Administración de revisiones, inicie sesión en el símbolo del sistema del dispositivo de vRealize Automation como raíz y escriba uno de los siguientes comandos.

```
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh enable
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh disable
```

Configurar el acceso al tenant predeterminado

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 vRealize Automation como administrador del tenant predeterminado.
 - a Acceda a la interfaz del producto de vRealize Automation.
`https://vrealize-automation-FQDN/vcac`
 - 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**.

Pasos siguientes

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.

Solucionar problemas de instalación de vRealize Automation

8

En la solución 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 incluye los siguientes temas:

- [Revertir una instalación fallida](#)
- [Crear un paquete de soporte de vRealize Automation](#)
- [Solucionar problemas de instalación general](#)
- [Solucionar problemas del dispositivo vRealize Automation](#)
- [Solucionar problemas con componentes de IaaS](#)
- [Solucionar problemas de errores de inicio de sesión](#)

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.

Resultados

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 Revierta 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.

Resultados

Tabla 8-1. 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 de vRealize Automation

Puede crear un paquete de soporte de vRealize Automation mediante la interfaz de administración del dispositivo de vRealize Automation. Los paquetes de soporte recopilan logs, y le permiten a usted o al soporte técnico de VMware solucionar problemas de vRealize Automation.

Procedimiento

- 1 Inicie sesión en la interfaz de administración del dispositivo de vRealize Automation como raíz.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Haga clic en **vRA > Logs**.
- 3 Haga clic en **Crear paquete de soporte**.

4 Haga clic en **Descargar** y guarde el paquete de soporte en el sistema.

Resultados

Los paquetes de soporte incluyen información del dispositivo de vRealize Automation y de los servidores de Windows de IaaS. Si se pierde la conectividad entre los componentes del dispositivo de vRealize Automation e IaaS, puede que al paquete de soporte le falten los logs de componentes de IaaS.

Para ver qué archivos de logs se han recopilado, descomprima el paquete de soporte y abra el archivo `Environment.html` en un navegador web. Sin conectividad, los componentes de IaaS aparecerán en rojo en la tabla Nodos. Adicionalmente, los logs de IaaS podrían estar ausentes debido a que el servicio del agente de administración de vRealize Automation se ha detenido en los servidores de Windows de IaaS en color rojo.

Línea de comandos: para generar un paquete de soporte desde la línea de comandos del dispositivo de vRealize Automation como raíz, puede ejecutar `vcac-support` o `vcac-config log-bundle`.

Como alternativa, puede ejecutar el comando `log-bundle` completo como se muestra en el siguiente ejemplo. Consulte [vRealize Automation Principios básicos de la línea de comandos de instalación](#) para obtener información general sobre la ejecución de `vra-command`.

```
# vra-command execute --node cafe.node.497772175.21500 log-bundle --requestor va-1.mycompany.com

Parent command with id='981e3028-c99b-5c92-1bae-7d2bf5b6aaaa' was created.
Waiting for all child commands to complete...
...
Command execution result:
Command id: 3d64d122-0af1-28dd-b5a5-d932b78b3678
  Type: log-bundle
  Node id: cafe.node.497772175.21500
  Node host: va-1.mycompany.com
  Result: The command was successfully executed.
  Result description: {"path": "/opt/vmware/var/support-bundle/log/
va-1.mycompany.com_cafe.node.497772175.21500-VA.zip"}

Status: COMPLETED
```

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.

Causa

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.
- 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.

Causa

Es posible que los servidores horarios no estén sincronizados en todos los servidores.

Solución

Sincronice todos los dispositivos de vRealize Automation y las instancias de Windows Server de IaaS con el mismo origen de hora. No combine orígenes de hora dentro de una implementación de vRealize Automation.

- Establezca un origen de hora del dispositivo de vRealize Automation:
 - a Inicie sesión en la interfaz de administración del dispositivo de vRealize Automation como raíz.

`https://vrealize-automation-appliance-FQDN:5480`

- b Seleccione **Administración > Configuración horaria** y establezca el origen de sincronización de hora.

Opción	Descripción
Hora del host	Sincronización con el host ESXi del dispositivo de vRealize Automation.
Servidor de hora	Sincronización con un servidor externo de protocolo de hora de red (Network Time Protocol, NTP). Escriba el FQDN o la dirección IP del servidor NTP.

- Para las instancias de Windows Server de IaaS, consulte [Habilitar la sincronización de hora en el servidor de Windows](#).

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.

Requisitos previos

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**).

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

Causa

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

- 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 `vcac-config.exe.config` en un editor de texto y ubique la dirección del repositorio:
`<add key="repositoryAddress" value="https://IaaS-address:443/repository/" />`
- 2 Abra el navegador Internet Explorer con esta dirección.
- 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 del certificado.

Solución

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.

Requisitos previos

Solicítele al administrador de su sitio los nombres, números de puerto y credenciales del 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.

Causa

Su sitio se conecta a Internet mediante un servidor proxy.

Solución

- 1 Abra un navegador web en la dirección URL de la interfaz de administración del dispositivo de vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`

- 2 Inicie sesión como usuario raíz y haga clic en **Red**.
- 3 Escriba el FQDN, o dirección IP, y el número de puerto del servidor proxy de su sitio.
- 4 Si el servidor proxy requiere credenciales, introduzca el nombre de usuario y la contraseña.
- 5 Haga clic en **Guardar configuración**.

Pasos siguientes

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 proxy impide el inicio de sesión de un usuario de VMware Identity Manager](#).

Pasos de la consola para la configuración de contenido inicial

Existe una alternativa a usar la interfaz de instalación de vRealize Automation para crear la cuenta del administrador de configuración y el contenido inicial.

En lugar de utilizar la interfaz, introduzca los comandos de consola para crear el usuario configurationadmin y el contenido inicial. Tenga en cuenta que la interfaz podría fallar después de completar correctamente parte del proceso, por lo que podría necesitar tan solo algunos comandos.

Por ejemplo, podría inspeccionar logs y la ejecución del flujo de trabajo de vRealize Orchestrator y determinar que la configuración basada en la interfaz ha creado el usuario configurationadmin, pero no el contenido inicial. En ese caso, puede introducir los últimos dos comandos de consola para completar el proceso.

Problema

Como parte de la última fase de la instalación de vRealize Automation, siga el proceso para introducir una nueva contraseña, crear la cuenta de usuario local configurationadmin y crear el contenido inicial. Se produce un error y la interfaz entra en un estado irrecuperable.

Solución

- 1 Inicie sesión en la consola del dispositivo de vRealize Automation como raíz.
- 2 Importe el flujo de trabajo de vRealize Orchestrator con el siguiente comando:

```
/usr/sbin/vcac-config -e content-import --workflow /usr/lib/vcac/tools/initial-config/vra-
initial-config-bundle-workflow.package --user $SSO_ADMIN_USERNAME --password
$SSO_ADMIN_PASSWORD --tenant $TENANT
```

- 3 Ejecute el flujo de trabajo para crear el usuario configurationadmin:

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py
--host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD
--workflowid f2b3064a-75ca-4199-a824-1958d9c1efed --configurationAdminPassword
$CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```


- 4 Importe el blueprint de ASD con el siguiente comando:

```
/usr/sbin/vcac-config -e content-import --blueprint /usr/lib/vcac/tools/initial-config/
vra-initial-config-bundle-asd.zip --user $CONFIGURATIONADMIN_USERNAME --password
$CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 5 Ejecute el flujo de trabajo para configurar el contenido inicial:

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py
--host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD
--workflowid ef00fce2-80ef-4b48-96b5-fdee36981770 --configurationAdminPassword
$CONFIGURATIONADMIN_PASSWORD
```

No se pueden degradar licencias de vRealize Automation

Se produce un error al enviar la clave de licencia de una edición anterior del producto.

Problema

Se mostrará el siguiente mensaje cuando utilice la página Licencias de la interfaz de administración de vRealize Automation para enviar la clave de una edición de producto anterior a la actual. Por ejemplo, comienza con una licencia empresarial e intenta introducir una licencia avanzada.

```
Unable to downgrade existing license edition
```

Causa

Esta versión de vRealize Automation no admite la degradación de las licencias. Solo se pueden agregar las licencias de una edición igual o posterior.

Solución

Para cambiar a una edición anterior, vuelva a instalar vRealize Automation.

Solucionar problemas del dispositivo 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 del dispositivo de vRealize Automation.

Problema

Los instaladores no se descargan cuando se ejecuta `setup__vrealize-automation-appliance-FQDN@5480.exe`.

Causa

- Problemas de conectividad de red al conectarse a la máquina del dispositivo de vRealize Automation.
- No se puede establecer una conexión con la máquina del dispositivo de vRealize Automation porque no se puede acceder a la máquina o esta no responde antes de que se agote el tiempo de espera de la conexión.

Solución

- 1 Compruebe que puede conectarse a la URL de vRealize Automation en un navegador web.
`https://vrealize-automation-appliance-FQDN`
- 2 Consulte el resto de los temas de solución de problemas del dispositivo de vRealize Automation.
- 3 Descargue el archivo de instalación y vuelva a conectarse al 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.

Requisitos previos

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.

Problema

Inicia sesión en Dispositivo de vRealize Automation y se abre la página Tenants. Una vez que la página empieza a cargarse, aparece el mensaje Error del sistema.

Causa

El archivo Encryption.key tiene permisos incorrectos o el nivel de usuario de propietario o grupo está mal asignado.

Solución

- 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.

Pasos siguientes

Iniciar sesión en la página Tenants para constatar que puede hacerlo sin errores.

Identity Manager para la gestión de directorios no puede iniciarse tras el reinicio de Horizon-Workspace

En un entorno de alta disponibilidad de vRealize Automation, puede producirse un error de inicio de Identity Manager para la gestión de directorios 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 creating bean with name
'liquibase' defined in class path resource [spring/datastore-wireup.xml]:
Invocation of init method failed; nested exception is
liquibase.exception.LockException: Could not acquire change log lock. Currently
locked by fe80:0:0:0:250:56ff:fea8:7d0c%eth0
(fe80:0:0:0:250:56ff:fea8:7d0c%eth0) since 10/29/15
```

Causa

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 una sesión de consola en el dispositivo de vRealize Automation.
- 2 Detenga el servicio de Horizon-Workspace mediante el siguiente comando.

```
#service horizon-workspace stop
```

- 3 Abra el shell de Postgres como superusuario.

```
su postgres
```

- 4 Desplácese hasta el directorio bin correcto.

```
cd /opt/vmware/vpostgres/current/bin
```

- 5 Conéctese a la base de datos.

```
psql vcac
```

- 6 Desde saas.databaschangelock, ejecute la siguiente consulta SQL.

```
select * from databaschangelock;
```

Si el resultado muestra un valor "t" (por "true"), el bloqueo se debe liberar manualmente.

- 7 Si tiene que liberar el bloqueo de forma manual, ejecute la siguiente consulta SQL.

```
update saas.databaschangeloglock set locked=FALSE, lockgranted=NULL, lockedby=NULL where id=1;
```

- 8 Desde saas.databaschangeloglock, ejecute la siguiente consulta SQL.

```
select * from databaschangeloglock;
```

El resultado debe mostrar un valor "f" (por "false"), lo que indicará que está desbloqueado.

- 9 Salga de la base de datos de vcac de Postgres.

```
vcac=# \q
```

- 10 Cierre el shell de Postgres.

```
exit
```

- 11 Inicie el servicio de Horizon-Workspace.

```
#service horizon-workspace start
```

Asignaciones incorrectas de la función del dispositivo tras una conmutación por error

Tras una conmutación por error, puede que no se haya asignado la función correcta a los nodos del dispositivo de vRealize Automation principales y de réplica, lo cual afecta a todos los servicios que requieren acceso de escritura a la base de datos.

Problema

En un clúster de alta disponibilidad de dispositivos de vRealize Automation, debe desconectar o impedir el acceso al nodo principal de base de datos. La interfaz de administración se emplea en otro nodo para promocionar ese nodo como el nuevo elemento principal, lo que restaura el acceso de escritura a la base de datos de vRealize Automation.

Más adelante, se vuelve a conectar el nodo principal anterior, pero la pestaña Clúster de su interfaz de administración seguirá mostrando el nodo como nodo principal, incluso cuando no lo sea. Fallarán los intentos que se hagan para utilizar cualquier interfaz de administración de nodos para solucionar el problema promoviendo oficialmente el anterior nodo a principal.

Solución

Cuando se produzca una conmutación por error, siga estas directrices para configurar el nodo principal anterior frente al nuevo.

- Antes de promocionar otro nodo a nodo principal, quite el nodo principal anterior del grupo de equilibradores de carga de nodos del dispositivo de vRealize Automation.

- Para que vRealize Automation devuelva un nodo principal anterior al clúster, permita que la máquina anterior se vuelva a conectar. A continuación, abra la nueva interfaz de administración principal. Busque el nodo anterior que aparece como `invalid` en la pestaña Clúster y haga clic en su botón **Restablecer**.

Una vez que se haya restablecido correctamente, puede restaurar el nodo anterior en el grupo de equilibradores de carga de nodos del dispositivo de vRealize Automation.

- Para devolver un nodo principal anterior al clúster de forma manual, vuelva a conectar la máquina y únala al clúster como si fuese un nodo nuevo. Mientras se realiza esta unión, especifique que el nodo que se acaba de promocionar es el nodo principal.

Una vez que se haya realizado la unión correctamente, puede restaurar el nodo anterior en el grupo de equilibradores de carga de nodos del dispositivo de vRealize Automation.

- Hasta que restablezca un nodo principal anterior o vuelva a unirlo correctamente al clúster, no use su interfaz de administración para realizar operaciones de administración del clúster, incluso si el nodo se conecta de nuevo.
- Cuando el restablecimiento o la unión se realicen correctamente, podrá promocionar un nodo anterior como principal.

Problemas después de la promoción de los nodos de réplica y principales

Los problemas de espacio en el disco, junto con la promoción de nodos de la base de datos del dispositivo de vRealize Automation de réplica y principales, podrían causar problemas de aprovisionamiento.

Problema

El nodo principal se queda sin espacio en el disco. Inicia sesión en la página Base de datos de su interfaz de administración y realiza la promoción de un nodo de réplica con suficiente espacio en el disco como para convertirse en el nuevo nodo principal. La promoción parece realizarse con éxito cuando actualiza la página de la interfaz de administración, aunque aparece un mensaje de error.

Después, libera espacio en el disco del antiguo nodo principal. Sin embargo, después de volver a promover el nodo a principal, se produce un error en las operaciones de aprovisionamiento que se muestran como `IN_PROGRESS`.

Causa

vRealize Automation no puede actualizar correctamente la configuración del antiguo nodo principal si el problema es la falta de espacio.

Solución

Si la interfaz de administración muestra errores durante la promoción, excluya temporalmente el nodo del equilibrador de carga. Corrija el problema del nodo, por ejemplo, añadiendo espacio en el disco, antes de volver a incluirlo en el equilibrador de carga. A continuación, actualice la página Base de datos de la interfaz de administración y compruebe que los nodos principal y de réplica son correctos.

Registros de servicios de componentes de vRealize Automation incorrectos

La interfaz de administración del dispositivo de vRealize Automation puede ayudarle a resolver problemas de registro con los servicios de componentes de vRealize Automation.

Problema

Con un funcionamiento normal, todos los servicios de componentes de vRealize Automation deben ser únicos y tener el estado REGISTRADO. Cualquier otro grupo de condiciones podría hacer que vRealize Automation tuviera un comportamiento impredecible.

Causa

A continuación se muestran ejemplos de problemas que se podrían producir con los servicios de componentes de vRealize Automation.

- Un servicio se ha desactivado.
- La configuración del servidor ha causado que un servicio deje de tener el estado REGISTRADO.
- Una dependencia de otro servicio ha causado que un servicio deje de tener el estado REGISTRADO.
- Es posible que el servicio SQL no se esté ejecutando.

Solución

Vuelva a registrar los servicios de componentes que parecen tener problemas.

- 1 Cree una snapshot snapshot del dispositivo de vRealize Automation.
Es posible que tenga que volver a la snapshot snapshot si prueba distintos cambios en los servicios, y que el dispositivo termine en un estado impredecible.
- 2 Inicie sesión en la interfaz de administración del dispositivo de vRealize Automation como raíz.
`https://vrealize-automation-appliance-FQDN:5480`
- 3 Haga clic en **Servicios**.
- 4 En la lista de servicios, busque un servicio cuyo estado no sea correcto o tenga algún otro problema.

- 5 Si `iaas-service` es un servicio defectuoso, vaya al paso siguiente.

De lo contrario, para que vRealize Automation vuelva a registrar el servicio, inicie una sesión en la consola en el dispositivo de vRealize Automation como raíz y reinicie vRealize Automation escribiendo el siguiente comando.

```
service vcac-server restart
```

Si hay servicios asociados con la instancia de vRealize Orchestrator integrada, escriba el siguiente comando adicional.

```
service vco-restart restart
```

- 6 Si un servicio con problemas es `iaas-service`, realice los siguientes pasos para volver a registrarlo.
 - a No elimine del registro el servicio.
 - b En el servidor web de IaaS principal, inicie sesión con una cuenta que tenga derechos de administrador.
 - c Abra un símbolo del sistema como administrador.
 - d Ejecute el siguiente comando.

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterSolutionUser -url https://appliance-or-load-balancer-IP-or-FQDN/ -t
vsphere.local -cu administrator -cp password -f "C:\Program Files (x86)\VMware\VCAC
\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

La contraseña es la contraseña de `administrator@vsphere.local`.

- e Ejecute un comando para actualizar la información de registro en la base de datos de IaaS.

SQL Server con autenticación de Windows:

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
MoveRegistrationDataToDb -s IaaS-SQL-server-IP-or-FQDN -d SQL-database-name -f
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

SQL Server con autenticación de SQL nativa:

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
MoveRegistrationDataToDb -s SQL-server-IP-or-FQDN -d SQL-database-name -su SQL-user -
sp SQL-user-password -f "C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data
\Cafe\Vcac-Config.data" -v
```

Para buscar el servidor o el nombre de la base de datos, inspeccione el siguiente archivo en un editor de texto y busque `repository`. Los valores de origen de datos y catálogo inicial revelan la dirección del servidor y el nombre de la base de datos, respectivamente.

```
C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
```

El usuario SQL debe tener privilegios DBO para la base de datos.

- f Registre los endpoints mediante los siguientes comandos:

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /vcac
--Endpoint ui -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /WAPI
--Endpoint wapi -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /
repository --Endpoint repo -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /
WAPI/api/status --Endpoint status -v
```

- g Registre los elementos del catálogo mediante la ejecución del siguiente comando:

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterCatalogTypesAsync -v
```

- h Reinicie IIS.

```
iisreset
```

- i Inicie sesión en el host principal de Manager Service de IaaS.

- j Reinicie el servicio de Windows de vRealize Automation.

```
VMware vCloud Automation Center Service
```

- 7 Para volver a registrar cualquier servicio asociado con un sistema externo, como una instancia de vRealize Orchestrator externa, inicie sesión en el sistema externo y vuelva a iniciar los servicios ahí.

Una NIC adicional provoca errores en la interfaz de administración

Cuando agrega una segunda tarjeta de interfaz de red (NIC) a un dispositivo de vRealize Automation, se producen errores en algunas páginas de la interfaz de administración de vRealize Automation y no se cargan correctamente.

Problema

Agrega una segunda NIC mediante vCenter correctamente y las siguientes páginas de la interfaz de administración de vRealize Automation muestran errores en lugar de la carga.

- La página **Red > Estado** muestra un error relacionado con un script que no responde.
- La página **Red > Dirección** muestra un error relacionado con la imposibilidad de leer la información de la interfaz de red.

Causa

Desde la versión 7.3, el dispositivo de vRealize Automation admite dobles NIC. Sin embargo, la plantilla de ingeniería en el que se basa el dispositivo impide que la interfaz de administración funcione correctamente hasta que se aplique la solución.

Solución

Después de agregar una NIC adicional, reinicie el dispositivo de vRealize Automation.

No se puede promocionar un dispositivo virtual secundario a principal

En vRealize Automation, si la memoria del dispositivo virtual es reducida, podrían impedirse las promociones de dispositivos virtuales en el clúster.

Problema

Al nodo principal se le agota la memoria. Inicia sesión en la página base de datos de su interfaz de administración e intenta promover un nodo secundario para que se convierta en el nuevo nodo principal. Se produce el siguiente error.

```
Fail to execute on Node node-name, host is master-FQDN
because of: Could not read remote lock command result for node: node-name
on address: master-FQDN, reason is: 500 Internal Server Error
```

Causa

La promoción solo se realiza correctamente cuando todos los nodos pueden confirmar la reconfiguración de un nodo principal promocionado recientemente. La falta de memoria impide que el nodo principal anterior confirme, a pesar de que sea posible acceder a todos los nodos.

Solución

Desconecte el nodo principal que tiene poca memoria. Inicie sesión en la página de la base de datos de la interfaz de administración del nodo secundario y promueva el nodo secundario.

El tiempo de retención del log de sincronización de Active Directory es demasiado corto

En vRealize Automation, los logs de sincronización de Active Directory solo abarcan un par de días.

Problema

Después de dos días, los logs de sincronización de Active Directory desaparecen de la interfaz de administración. Las carpetas de los logs también desaparecen del siguiente directorio del dispositivo de vRealize Automation.

`/db/elasticsearch/horizon/nodes/0/indices`

Causa

Para ahorrar espacio, vRealize Automation define el tiempo máximo de retención de logs de sincronización de Active Directory en tres días.

Solución

- 1 Inicie una sesión de consola en el dispositivo de vRealize Automation como raíz.
- 2 Abra el siguiente archivo en un editor de texto.
`/usr/local/horizon/conf/runtime-config.properties`
- 3 Incremente la propiedad `analytics.maxQueryDays`.
- 4 Guarde y cierre `runtime-config.properties`.
- 5 Reinicie los servicios de búsqueda elástica y Identity Manager.

```
service horizon-workspace restart
service elasticsearch restart
```

RabbitMQ no puede resolver nombres de host

De forma predeterminada, RabbitMQ utiliza nombres de host cortos para los dispositivos de vRealize Automation, lo que puede impedir que los nodos se resuelvan entre sí.

Problema

Al intentar unir otro dispositivo de vRealize Automation al clúster, se produce un error similar al siguiente.

```
Clustering node 'rabbit@sc2-rdops-vm01-dhcp-62-2' with rabbit@company ...
Error: unable to connect to nodes [rabbit@company]: nodedown

DIAGNOSTICS
=====

attempted to contact: [rabbit@company]

rabbit@company:
  * unable to connect to epmd (port 4369) on company: nxdomain (non-existing domain)

current node details:
- node name: 'rabbitmq-cli-11@sc2-rdops-vm01-dhcp-62-2'
- home dir: /var/lib/rabbitmq
- cookie hash: 4+kP1tKnxGYaGjrPL2C8bQ==

[2017-09-01 14:58:04] [root] [INFO] RabbitMQ join failed with exit code: 69, see RabbitMQ logs for
details.
```

Causa

La configuración de red no permite que los dispositivos de vRealize Automation se resuelvan entre sí por nombre de host corto.

Solución

- 1 Para todos los dispositivos de vRealize Automation en la implementación, inicie sesión como raíz en una sesión de consola.

- 2 Detenga el servicio de RabbitMQ.

```
service rabbitmq-server stop
```

- 3 Abra el siguiente archivo en un editor de texto.

```
/etc/rabbitmq/rabbitmq-env.conf
```

- 4 Establezca la siguiente propiedad en true.

```
USE_LONGNAME=true
```

- 5 Guarde y cierre `rabbitmq-env.conf`.

- 6 Restablezca RabbitMQ.

```
vcac-vami rabbitmq-cluster-config reset-rabbitmq-node
```

- 7 Ejecute el siguiente script en un solo nodo de dispositivo de vRealize Automation.

```
vcac-config cluster-config-ping-nodes --services rabbitmq-server
```

- 8 En todos los nodos, compruebe que se haya iniciado el servicio de RabbitMQ.

```
vcac-vami rabbitmq-cluster-config get-rabbitmq-status
```

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.

Se rechazan las conexiones del coordinador de transacciones distribuidas

La configuración de llamada a procedimiento remoto (Remote Procedure Call, RPC) de Microsoft puede afectar al Coordinador de transacciones distribuidas (Distributed Transaction Coordinator, DTC) en vRealize Automation.

Problema

Se producen errores que indican que se rechazan las conexiones del DTC entre los servidores de Windows IaaS o el servidor de base de datos SQL de vRealize Automation.

Causa

Un ajuste de conexión de RPC restringe el acceso y debe deshabilitarse.

Solución

En todos los servidores de Windows de IaaS y el servidor de base de datos SQL de vRealize Automation, elimine la siguiente clave de registro o establézcala en cero.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC\RestrictRemoteClients

Los servidores de IaaS parecen estar desconectados

Los problemas de los contadores de rendimiento de Windows pueden provocar que se informe de que los servidores de IaaS están desconectados.

Problema

Después de instalar o actualizar el agente de administración, el servidor de IaaS envía pings al dispositivo de vRealize Automation. El problema se produce cuando ocurre un error en los pings, lo que provoca que el servidor de IaaS en la pestaña Clúster de la interfaz de administración de dispositivos de vRealize Automation tenga el estado No conectado.

En el servidor de IaaS, aparece un error similar al siguiente en el archivo All.log del agente de administración.

```
[UTC:2019-05-25 16:09:37 Local:2019-05-25 18:09:37] [Error]: [sub-thread-Id="4" context="" token=""]
System.InvalidOperationException: Category does not exist.
at System.Diagnostics.PerformanceCounterLib.CounterExists(String machine, String category, String
counter)
at System.Diagnostics.PerformanceCounter.InitializeImpl()
at System.Diagnostics.PerformanceCounter.NextSample()
at System.Diagnostics.PerformanceCounter.NextValue()
at VMware.IaaS.Component.Metrics.MetricsUtility.CalculateMachineProcessorMeasure(Int32
samplePeriodMilliseconds)
at VMware.IaaS.Management.Agent.ManagementEndpointService.CollectEnvironmentInfo()
at VMware.IaaS.Management.Agent.ManagementEndpointService.<PingAsync>d__0.MoveNext()
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.CompilerServices.TaskAwaiter.ThrowForNonSuccess(Task task)
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at System.Runtime.CompilerServices.ConfiguredTaskAwaitable`1.ConfiguredTaskAwaiter.GetResult()
at VMware.IaaS.Management.Agent.ManagementAgent.<<PingManagementEndpointAsync>b__1f>d__23.MoveNext()
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.CompilerServices.TaskAwaiter.ThrowForNonSuccess(Task task)
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at VMware.IaaS.Management.Agent.ManagementAgent.<ExecutePeriodicAction>d__8.MoveNext()
```

Causa

Existe un problema conocido por el cual los contadores de rendimiento de Windows se dañan con el transcurso del tiempo, lo que provoca el error.

Solución

Vuelva a generar todos los contadores de rendimiento, incluidos los contadores extensibles y de terceros.

- 1 En el servidor de IaaS, abra una línea de comandos como administrador.
- 2 Vuelva a generar los contadores:


```
cd C:\Windows\system32

lodctr /R

cd C:\Windows\syswow64

lodctr /R
```
- 3 Vuelva a sincronizar los contadores con el Instrumental de administración de Windows (Windows Management Instrumentation, WMI):


```
WINMGMT.EXE /RESYNCPERF
```
- 4 Detenga y reinicie el servicio de registros y alertas de rendimiento.
- 5 Detenga y reinicie el servicio de Instrumental de administración de Windows.

Pasos siguientes

Si los pasos anteriores no resuelven el problema, consulte el [artículo 300956 de soporte técnico de Microsoft](#) o el [artículo 2554336 de soporte técnico de Microsoft](#). En los artículos, se describe cómo restablecer manualmente los elementos asociados del Registro. Se recomienda realizar primero una copia de seguridad del Registro.

El Comprobador de requisitos previos no puede instalar funciones .NET

La opción **Reparar** del comprobador de requisitos previos de vRealize Automation da error y muestra mensajes donde se indica que no se encuentra el origen de instalación de .NET 3.5.1.

Problema

El Comprobador de requisitos previos tiene que verificar que esté instalado .NET 3.5.1 para poder cumplir los requisitos de los sistemas Windows Server 2008 R2 con IIS 7.5 y los sistemas Windows Server 2012 R2 con IIS 8.

Causa

En el caso de Windows Server 2012 R2, el hecho de que no sea posible conectarse a Internet podría ser un impedimento para la instalación automática de .NET. Algunas actualizaciones de Windows 2012 R2 también pueden evitar que se realice la instalación. El problema se genera porque la versión de Windows carece de una copia local del origen de instalación de .NET Framework 3.5.

Solución

Proporcione manualmente un origen de instalación de .NET Framework 3.5.

- 1 En el host de Windows, monte una imagen ISO de los medios de instalación de Windows Server 2012 R2.
- 2 En el Administrador de servidores, habilite .NET Framework 3.5 mediante el Asistente para agregar roles y características.
- 3 Mientras se está ejecutando el asistente, acceda a la ruta de instalación de .NET Framework 3.5 en los medios ISO.
- 4 Después de agregar .NET Framework 3.5, vuelva a ejecutar el Comprobador de requisitos previos de vRealize Automation.

Validar certificados de servidor para IaaS

Puede utilizar el comando `vcac-Config.exe` para comprobar que un servidor de IaaS acepte certificados del dispositivo de vRealize Automation y de dispositivos SSO.

Problema

Aparecen errores de autorización al utilizar las funciones de IaaS.

Causa

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` en `vra-installation-dir\Server\Model Manager Data\Cafe`, que suele estar 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`.

Causa

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.

Causa

Este mensaje puede aparecer por error cuando hay problemas de comunicación o de red.

Solución

Ignórelo 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 del 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 del dispositivo de vRealize Automation porque los parámetros de `msiexec` no son válidos.

Causa

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

Puede que se produzca un error en la instalación de vRealize Automation si el instalador de IaaS no puede guardar el componente Model Manager Data ni el componente web.

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.

Causa

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 la URL de vRealize Automation en un navegador web.

`https://vrealize-automation-appliance-FQDN`

◆ 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 web, compruebe el estado del servicio MetaModel y asegúrese de que no se producen errores de certificado:

`https://FQDN-or-IP/repository/data/MetaModel.svc`

◆ 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 web, compruebe el estado del servicio MetaModel:
`https://FQDN-or-IP/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.

Los servidores de IaaS de Windows no admiten FIPS

Una instalación no se puede realizar correctamente si el Estándar federal de procesamiento de información (Federal Information Processing Standard, FIPS) está habilitado.

Problema

La instalación muestra el siguiente error al instalar el componente web de IaaS.

Esta implementación no forma parte de los algoritmos criptográficos validados por Windows Platform FIPS.

Causa

vRealize Automation IaaS está integrado en Microsoft Windows Communication Foundation (WCF), que no es compatible con FIPS.

Solución

En el servidor de IaaS de Windows, deshabilite la política de FIPS.

- 1 Vaya a **Inicio > Panel de control > Herramientas administrativas > Política de seguridad local**.
- 2 En el cuadro de diálogo Política de grupo, bajo **Políticas locales**, seleccione **Opciones de seguridad**.
- 3 Encuentre y deshabilite la siguiente entrada.

Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash.

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, `c0DDOC01`.
- 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
```

Causa

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 [Artículo 2564571 de Microsoft Knowledge Base](#).

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.

Causa

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, desplácese hasta **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 la interfaz de producto de vRealize Automation.
<https://vrealize-automation-appliance-FQDN/vcac/org/tenant-name>
 - 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 servidores de IaaS clonados a partir de una plantilla donde ya está instalado el DTC contienen identificadores de DTC duplicados que impiden la comunicación entre los nodos.

Problema

Se produce un error en IaaS Manager Service y el siguiente mensaje de error se registra 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.
```

Causa

Cuando se clona un servidor de IaaS que ya tiene el DTC instalado, el clon contiene el mismo identificador único de DTC que el elemento principal, con lo cual las dos máquinas no pueden comunicarse.

Solución

- 1 En el clon, abra un símbolo del sistema como administrador.
- 2 Ejecute el siguiente comando.
`msdtc -uninstall`
- 3 Reinicie el clon.
- 4 Abra otro símbolo del sistema y ejecute el siguiente comando.
`msdtc -install manager-service-host-FQDN`

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 `@sudominio` del nombre de usuario, se cerrará la sesión de SSO de forma inmediata y se redireccionará a la página de inicio de sesión sin ninguna explicación.

Causa

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`.

Errores de inicio de sesión con alta disponibilidad

Cuando tiene más de un dispositivo de vRealize Automation, los dispositivos deben poder identificarse mutuamente mediante el nombre de host corto. De lo contrario, no podrá iniciar sesión.

Para permitir que un clúster de dispositivos de vRealize Automation de alta disponibilidad resuelva nombres de host cortos, elija uno de los siguientes enfoques. Debe modificar todos los dispositivos del clúster.

Problema

vRealize Automation se configura para la alta disponibilidad instalando un dispositivo de vRealize Automation adicional. Cuando intente iniciar sesión en vRealize Automation, aparecerá un mensaje sobre una licencia no válida. El mensaje es incorrecto sin embargo, porque determinó que su licencia era válida.

Causa

Los nodos del dispositivo de vRealize Automation no crearán un clúster de alta disponibilidad de forma correcta hasta que puedan resolver los nombres de host cortos de los nodos del clúster.

Solución

- ◆ Edite o cree una línea de búsqueda en `/etc/resolv.conf`. La línea debe incluir dominios que contengan dispositivos de vRealize Automation. Separe los dominios con espacios. Por ejemplo:

```
search sales.mycompany.com support.mycompany.com
```

- ◆ Edite o cree líneas de dominio en `/etc/resolv.conf`. Cada debe incluir un dominio que contenga dispositivos de vRealize Automation. Por ejemplo:

```
domain support.mycompany.com
```

- ◆ Añada líneas al archivo `/etc/hosts` para que cada nombre corto del dispositivo de vRealize Automation se asigne a su nombre de dominio completo. Por ejemplo:

```
node1    node1.support.mycompany.com
node2    node2.support.mycompany.com
```

El proxy impide el inicio de sesión de un usuario de VMware Identity Manager

Configurar el uso de un proxy puede impedir el inicio de sesión de los usuarios de VMware Identity Manager.

Requisitos previos

Configure vRealize Automation para acceder a la red a través de un servidor proxy. Consulte [Conectarse a la red mediante un servidor proxy](#).

Problema

Si configura vRealize Automation para acceder a la red a través de un servidor proxy, los usuarios de VMware Identity Manager verán el siguiente error cuando intenten iniciar sesión.

Error Unable to get metadata

Solución

- 1 Inicie sesión en la consola del dispositivo de vRealize Automation como usuario 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=vrealize-automation-hostname
```

Por ejemplo, NO_PROXY="localhost, 127.0.0.1, automation.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
```