

Instalar y actualizar vRealize Automation

5 de octubre de 2018
vRealize Automation 7.4



vmware®

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

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

El sitio web de VMware también ofrece las actualizaciones de producto más recientes.

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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 © 2017–2018 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y marca comercial.](#)

Contenido

| | | |
|----------|---|----------|
| 1 | Instalar o actualizar vRealize Automation | 4 |
| | Arquitectura de referencia de vRealize Automation | 4 |
| | Recomendaciones de configuración e implementación inicial | 4 |
| | Implementación de vRealize Automation | 5 |
| | Consideraciones sobre la implementación de vRealize Business for Cloud | 7 |
| | Escalabilidad de vRealize Automation | 8 |
| | Escalabilidad de vRealize Business for Cloud | 11 |
| | Consideraciones sobre configuración de alta disponibilidad de vRealize Automation | 11 |
| | Consideraciones sobre alta disponibilidad de vRealize Business for Cloud | 13 |
| | Especificaciones del hardware y valores máximos de capacidad de vRealize Automation | 14 |
| | Requisitos de implementaciones pequeñas de vRealize Automation | 16 |
| | Requisitos de implementaciones medianas de vRealize Automation | 21 |
| | Requisitos de implementaciones grandes de vRealize Automation | 27 |
| | Implementaciones de datos de centros de multidados de vRealize Automation | 33 |
| | Configuración segura de vRealize Automation | 34 |
| | Descripción general de la línea de base segura de vRealize Automation | 35 |
| | Comprobar la integridad de los medios de instalación | 36 |
| | Proteger la infraestructura de software del sistema de VMware | 36 |
| | Revisar el software instalado | 38 |
| | Avisos de seguridad y revisiones de VMware | 38 |
| | Configuración segura | 38 |
| | Configurar la seguridad de la red del host | 73 |
| | Auditoría y registro | 88 |
| | Instalar vRealize Automation | 89 |
| | Descripción general de la instalación de vRealize Automation | 89 |
| | Preparar la instalación de vRealize Automation | 98 |
| | Implementar el dispositivo de vRealize Automation | 114 |
| | Instalar vRealize Automation con el Asistente de instalación | 121 |
| | Las interfaces estándar de instalación de vRealize Automation | 149 |
| | Instalación silenciosa de vRealize Automation | 230 |
| | Tareas posteriores a la instalación de vRealize Automation | 237 |
| | Solucionar problemas de instalación de vRealize Automation | 256 |
| | Actualizar vRealize Automation | 284 |
| | Actualizar de vRealize Automation 7.1 o posterior a 7.4 | 287 |
| | Actualizar de vRealize Automation 6.2.5 a 7.4 | 359 |
| | Migrar a vRealize Automation 7.4 | 446 |

Instalar o actualizar vRealize Automation

1

Puede instalar vRealize Automation por primera vez o puede actualizar el entorno actual a la versión más reciente.

Este capítulo incluye los siguientes temas:

- [Arquitectura de referencia de vRealize Automation](#)
- [Configuración segura de vRealize Automation](#)
- [Instalar vRealize Automation](#)
- [Actualizar vRealize Automation](#)

Arquitectura de referencia de vRealize Automation

La arquitectura de referencia describe la estructura y la configuración de implementaciones típicas de vRealize Automation. Además, ofrece información sobre alta disponibilidad, escalabilidad y perfiles de implementación.

La arquitectura de referencia incluye información sobre los siguientes componentes:

- VMware vRealize Automation
- VMware vRealize Business for Cloud

Para conocer los requisitos de software, las instalaciones y las plataformas compatibles, consulte la documentación de cada producto.

Recomendaciones de configuración e implementación inicial

Implemente y configure todos los componentes de VMware vRealize Automation de acuerdo con las recomendaciones de VMware.

Mantenga vRealize Automation, vRealize Business for Cloud y vRealize Orchestrator en la misma zona horaria con los relojes sincronizados.

Instale vRealize Automation, vRealize Business for Cloud y vRealize Orchestrator en el mismo clúster de administración. Aprovechne máquinas a un clúster que esté separado del clúster de administración para que la carga de trabajo del usuario y la de servidor puedan aislarse.

Implemente agentes de proxy en el mismo centro de datos que el extremo con el que se comunicarán. VMware no recomienda colocar los trabajos de DEM en centros de datos remotos a menos que exista un caso de uso basado en una habilidad de flujo de trabajo exprese que lo requiera. Todos los componentes excepto los agentes de proxy y los trabajos de DEM deben implementarse en el mismo centro de datos o en los mismos centros de datos dentro de una red de área metropolitana. La latencia debe ser menor a 5 milisegundos, y el ancho de banda no debe ser menor a 1 GB entre los centros de datos y la red de área metropolitana.

Para obtener más información, incluida una declaración de compatibilidad, consulte el artículo de la Base de conocimientos de VMware *Instalar VMware vRealize Automation en una instancia distribuida en varios emplazamientos*, disponible en

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2134842.

Implementación de vRealize Automation

Utilice las recomendaciones de recursos de VMware como punto de partida para planear la implementación de vRealize Automation.

Después de realizar las pruebas iniciales y la implementación para producción, siga supervisando el rendimiento y asigne recursos adicionales si es necesario, tal y como se describe en [Escalabilidad de vRealize Automation](#).

Autenticación

Cuando configure vRealize Automation, puede usar el conector de administración de directorios para la autenticación de los usuarios, o puede especificar un proveedor de identidad preexistente basada en SAML para admitir una experiencia de inicio de sesión único.

Si se requiere una autenticación de dos factores, vRealize Automation admite la integración con RSA SecurID. Cuando se configura este punto de integración, se pide a los usuarios que indiquen su ID de usuario y su contraseña.

Consideraciones sobre el equilibrador de carga

Utilice el menor tiempo de respuesta o un método round robin para equilibrar el tráfico a los dispositivos de vRealize Automation y los servidores web de infraestructura. Habilite la función de afinidad de sesión para que las solicitudes siguientes procedentes de cada sesión única se dirijan al mismo servidor web en el grupo de equilibradores de carga.

Puede usar el equilibrador de carga para administrar la conmutación por error para Manager Service, pero no use un algoritmo de equilibrio de carga porque solo hay un Manager Service activo a la vez. Tampoco use la afinidad de sesiones cuando administre la conmutación por error con un equilibrador de carga.

Use los puertos 443 y 8444 cuando equilibre la carga del dispositivo de vRealize Automation. Para el sitio web de infraestructura e Infrastructure Manager Service, solo se debe equilibrar la carga del puerto 443.

Aunque puede usar otros equilibradores de carga, se recomienda usar NSX, F5 BIG-IP y F5 BIG-IP Virtual Edition, ya que han sido probados.

Consulte la documentación de vRealize Automation para obtener información más detallada sobre la configuración de equilibradores de carga.

Implementación de base de datos

En las versiones 7.0 y posteriores, vRealize Automation agrupa automáticamente la base de datos del dispositivo en clústeres. Todas las implementaciones nuevas de la versión 7.0 y posteriores deben usar la base de datos interna del dispositivo. Las instancias de vRealize Automation que se actualizan a la versión 7.1 o posterior deben combinar sus bases de datos externas con la base de datos del dispositivo. Consulte la documentación del producto de vRealize Automation para obtener más información sobre el proceso de actualización.

Para las implementaciones de producción de los componentes de infraestructura, utilice un servidor de base de datos dedicado para hospedar las bases de datos de Microsoft SQL Server (MSSQL). vRealize Automation requiere que las máquinas que se comunican con el servidor de base de datos se configuren para usar Microsoft DTC (Coordinador de transacciones distribuidas). De manera predeterminada, Microsoft DTC requiere los puertos 135 y 1024 a través de 65535.

Para obtener más información sobre el cambio de los puertos predeterminados de MSDTC, consulte el artículo de la Base de conocimientos relativo a la Configuración de Microsoft Distributed Transaction Coordinator (DTC) para trabajar a través de un firewall, disponible en <https://support.microsoft.com/es-es/KB/250367>.

El host de IaaS Manager Service debe poder resolver el nombre de NETBIOS del host de base de datos de SQL Server de IaaS. Si no se puede resolver el nombre de NETBIOS, agregue el nombre de NETBIOS de SQL Server al archivo `/etc/hosts` de la máquina de Manager Service y reinicie Manager Service.

vRealize Automation solo admite grupos de SQL AlwaysON con Microsoft SQL Server 2016. Al instalar SQL Server 2016, la base de datos debe crearse en el modo 100. Si utiliza una versión anterior de Microsoft SQL Server, utilice una instancia de clúster de conmutación por error con discos compartidos. Para obtener más información sobre la configuración de grupos SQL AlwaysOn con MSDTC, consulte <https://msdn.microsoft.com/es-es/library/ms366279.aspx>.

Configuración de recopilación de datos

La configuración predeterminada de recopilación de datos es un buen punto de partida para la mayoría de las implementaciones. Después de implementar en el entorno de producción, siga supervisando el rendimiento de la recopilación de datos para determinar si debe realizar algún ajuste.

Agentes de proxy

Para obtener el máximo rendimiento, implemente los agentes del mismo centro de datos como el endpoint al que están asociados. También puede instalar agentes adicionales para aumentar el rendimiento y la simultaneidad del sistema. Las implementaciones distribuidas pueden tener varios servidores de agente distribuidos por todo el mundo.

Cuando los agentes se instalan en el mismo centro de datos como su endpoint asociado, puede apreciarse que el rendimiento de la recopilación de datos aumenta un 200% de media. El tiempo de recopilación medido incluye solo el tiempo dedicado a transferir los datos entre el agente de proxy y el servicio de administrador. No incluye el tiempo que Manager Service tarda en procesar los datos.

Por ejemplo, actualmente está implementando el producto en un centro de datos en Palo Alto (EE. UU.) y tiene endpoints de vSphere en Palo Alto (EE. UU.), Boston (EE. UU.) y Londres (Reino Unido). En esta configuración, los agentes de proxy de vSphere se implementan en Palo Alto, Boston y Londres para sus respectivos endpoints. Si, por el contrario, los agentes se implementan solo en Palo Alto, puede que se produzca un incremento del 200 % en el tiempo de recopilación de datos para Boston y Londres.

Configuración de Distributed Execution Manager

En general, se recomienda ubicar las instancias de Distributed Execution Manager (DEM) lo más cerca posible al host de Model Manager. El orquestador de DEM debe tener una fuerte conectividad de red a Model Manager en todo momento. El instalador coloca los orquestadores de DEM junto con Manager Service de forma predeterminada. Cree dos instancias del orquestador de DEM: una para la conmutación por error y dos instancias de trabajo de DEM en el centro de datos principal.

Si una instancia de trabajo de DEM debe ejecutar un flujo de trabajo específico de la ubicación, instale la instancia en esta ubicación.

Asigne aptitudes a los flujos de trabajo y los DEM relevantes para que DEM siempre ejecute esos flujos de trabajo en la ubicación correcta. Para obtener información sobre la asignación de aptitudes a flujos de trabajo y DEM mediante la consola de vRealize Automation Designer, consulte la documentación sobre extensibilidad de vRealize Automation.

Para obtener el mejor rendimiento, instale los DEM y los agentes en máquinas distintas. Para obtener información adicional sobre la instalación de agentes de vRealize Automation, consulte [Instalar agentes](#).

vRealize Orchestrator

Utilice la instancia interna de vRealize Orchestrator para todas las nuevas implementaciones. Si es necesario, las implementaciones heredadas pueden continuar utilizando un vRealize Orchestrator externo. Consulte https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2147109 para conocer el procedimiento que debe seguirse para aumentar la memoria asignada a la instancia interna de vRealize Orchestrator.

Para obtener el mejor rendimiento del producto, revise e implemente las directrices de configuración descritas en la *guía de diseño de codificación de vRealize Orchestrator* antes de importar el contenido de vRealize Orchestrator a las implementaciones de producción.

Consideraciones sobre la implementación de vRealize Business for Cloud

Implemente vRealize Business for Cloud, antes conocido como vRealize Business Standard Edition, de conformidad con las directrices de VMware.

Consideraciones sobre el equilibrador de carga

No se admite el equilibrio de carga para conexiones de recopilación de datos. Para obtener más información, consulte [Escalabilidad de vRealize Automation](#). En el dispositivo de vRealize Business for Cloud para conexiones del cliente de API y de interfaz de usuario, puede usar el equilibrador de carga de vRealize Automation.

Escalabilidad de vRealize Automation

Tenga en cuenta todos los factores de escalabilidad aplicables al configurar el sistema de vRealize Automation.

Usuarios

El Dispositivo de vRealize Automation está configurado para sincronizar menos de 100.000 usuarios. Si su sistema contiene varios usuarios, es posible que deba añadir memoria a Administración de directorios de vRealize Automation. Para obtener información más detallada sobre cómo añadir memoria en Administración de directorios, consulte [Add Memory to Directories Management](#) (Añadir memoria en Administración de directorios).

Escalabilidad de aprovisionamientos simultáneos

De manera predeterminada, vRealize Automation solo procesa ocho aprovisionamientos simultáneos por endpoint. Para obtener información sobre cómo aumentar este límite, consulte [Configurar el aprovisionamiento de máquinas simultáneas](#).

VMware recomienda que todas las implementaciones comiencen con al menos dos trabajos de DEM. En la versión 6.x, cada trabajo de DEM podría procesar 15 flujos de trabajo simultáneamente. Esta cifra se aumentó a 30 para vRealize Automation 7.0 y posterior.

Si las máquinas se van a personalizar a través de Workflow Stubs, debe tener 1 trabajo de DEM por 20 máquinas que se aprovisionarán simultáneamente. Por ejemplo, un sistema que admiten 100 aprovisionamientos simultáneos debe tener como mínimo 5 trabajos de DEM.

Para obtener más información sobre los trabajos de DEM y escalabilidad, consulte [Afinación y análisis del rendimiento de Distributed Execution Manager](#)

Escalabilidad de recopilación de datos

El tiempo que tarda en completarse la recopilación de datos depende de la capacidad de recursos informáticos, el número de máquinas en el endpoint o el recurso informático, el sistema actual y la carga de red, entre otras variables. El rendimiento se escala a una velocidad diferente según los distintos tipos de recopilación de datos.

Cada tipo de recopilación de datos tiene un intervalo predeterminado que puede reemplazar o modificar. Los administradores de infraestructura pueden iniciar manualmente la recopilación de datos para los endpoints del origen de la infraestructura. Los administradores de infraestructura pueden iniciar manualmente la recopilación de datos para los endpoints de recursos informáticos. Los siguientes valores son los intervalos predeterminados para la recopilación de datos.

Tabla 1-1. Intervalos predeterminados para la recopilación de datos

| Tipo de recopilación de datos | Intervalo predeterminado |
|-------------------------------|--------------------------|
| Inventario | Cada 24 horas (diario) |
| Estado | Cada 15 minutos |
| Rendimiento | Cada 24 horas (diario) |

Ajuste y análisis de rendimiento

A medida que aumenta el número de recursos que recopila datos, es posible que el tiempo que se tarda en completar la recopilación de datos sea mayor que el tiempo entre los intervalos de recopilación de datos, concretamente para la recopilación de datos de estado. Para determinar si la recopilación de datos de un endpoint o un recurso informático se va a completar a tiempo o se va a poner en cola, consulte la página Recopilación de datos. El valor del campo Última vez completada podría mostrar En cola o En curso en lugar de una marca de hora que indica cuándo se completó la recopilación de datos. Si se produce este problema, puede aumentar el intervalo entre recopilaciones de datos para reducir la frecuencia de recopilación de datos.

Si lo prefiere, puede aumentar el límite de recopilación de datos simultánea por agente. De manera predeterminada, vRealize Automation limita las actividades de recopilación de datos simultáneas a dos por agente y pone en cola las solicitudes que superen ese límite. Este límite permite que las actividades de recopilación de datos terminen rápidamente sin afectar al rendimiento general. Puede aumentar el límite para aprovechar la recopilación de datos simultáneos, pero debe sopesar esta opción con respecto a la degradación del rendimiento general.

Si aumenta el límite por agente configurado en vRealize Automation, puede interesarle aumentar uno o varios de estos intervalos de tiempo de espera de ejecución. Para obtener más información sobre cómo configurar la recopilación de datos simultánea y los intervalos de tiempo de espera, consulte la documentación sobre administración del sistema de vRealize Automation. La recopilación de datos de Manager Service hace un uso intensivo de la CPU. Si aumenta la capacidad de procesamiento del host de Manager Service, se reduce el tiempo necesario para la recopilación de datos total.

La recopilación de datos para Amazon Elastic Compute Cloud (Amazon AWS), concretamente, puede hacer un uso intensivo de la CPU, sobre todo si el sistema recopila datos en varias regiones simultáneamente y si los datos no se recopilaron con anterioridad en esas regiones. Este tipo de recopilación de datos puede provocar una degradación general en el rendimiento del sitio web. Reduzca la frecuencia de la recopilación de datos de inventario de Amazon AWS si está afectando de manera apreciable al rendimiento.

Escalabilidad del procesamiento del flujo de trabajo

El tiempo medio de procesamiento del flujo de trabajo, desde que el orquestador de DEM inicia el preprocesamiento del flujo de trabajo hasta que este termina de ejecutarse, aumenta con el número de flujos de trabajo simultáneos. El volumen del flujo de trabajo es una función de la cantidad de actividad de vRealize Automation, incluidas las solicitudes de máquinas y algunas actividades de recopilación de datos.

Configurar el servicio de administrador para volumen de datos altos

Si espera usar un clúster de VMware vSphere que contenga una gran cantidad de objetos, por ejemplo, 3.000 o más máquinas virtuales, modifique el archivo de config. del servicio de administrador con volúmenes más grandes. Si no modifica esta configuración, es probable que grandes recopilaciones de datos del inventario presenten errores.

Modifique el valor predeterminado de los parámetros `ProxyAgentServiceBinding` y `maxStringContentLength` en el archivo `ManagerService.exe.config`.

Procedimiento

- 1 Abra el archivo `ManagerService.exe.config` en un editor de texto.

Generalmente, este archivo se encuentra en `C:\Archivos de programa (x86)\VMware\VCAC\Server`.

- 2 Encuentre las líneas `binding name` y `readerQuotas` en el archivo.

```
<binding name="ProxyAgentServiceBinding" maxReceivedMessageSize="13107200">  
  <readerQuotas maxStringContentLength="13107200" />
```

Nota No confunda estas dos líneas con las líneas similares que contienen la siguiente cadena:
`binding name = "ProvisionServiceBinding"`.

- 3 Reemplace los valores de número asignados a los atributos `maxReceivedMessageSize` y `maxStringContentLength` con un volumen más grande.

El tamaño óptimo depende de cuántos objetos más espera que su clúster de VMware vSphere contenga en el futuro. Por ejemplo, puede aumentar estos números multiplicándolos por diez para fines de prueba.

- 4 Guarde los cambios y cierre el archivo.
- 5 Reinicie el servicio de administrador de vRealize Automation.

Afinación y análisis del rendimiento de Distributed Execution Manager

Puede ver el número total de los flujos de trabajo en curso o pendientes en cualquier momento en la página Estado de ejecución distribuida, y puede usar la página Historial del flujo de trabajo para determinar cuánto tiempo demanda ejecutar un flujo de trabajo dado.

Si tiene un gran número de flujos de trabajo pendientes o si los flujos de trabajo demoran más de lo esperado en terminarse, agregue más instancias de trabajo de Distributed Execution Manager (DEM) para elegir los flujos de trabajo. Cada instancia de trabajo de DEM puede procesar 30 flujos de trabajo simultáneos. Los flujos de trabajo en exceso se colocan en cola para su ejecución.

Puede ajustar los programas de flujos de trabajo para minimizar el número de flujos de trabajo que se inician al mismo tiempo. Por ejemplo, en lugar de programar todos flujos de trabajo por hora para que se ejecuten al comienzo de la hora, puede escalonar los tiempos de ejecución para que no compitan por los recursos de DEM. Para obtener más información sobre los flujos de trabajo, consulte la documentación sobre la extensibilidad de vRealize Automation.

Algunos flujos de trabajo, en especial ciertos flujos de trabajo personalizados, pueden hacer un uso intensivo de la CPU. Si la carga de la CPU en las máquinas de trabajo de DEM es alta, analice la posibilidad de aumentar la energía de procesamiento de la máquina de DEM o agregar más máquinas de esta a su entorno.

Escalabilidad de vRealize Business for Cloud

Configure la instalación de vRealize Business for Cloud para la escalabilidad siguiendo las directrices de VMware.

vRealize Business for Cloud puede escalar verticalmente hasta 20.000 máquinas virtuales en diez instancias de VMware vCenter Server. La primera sincronización de la colección de datos del inventario tarda tres horas aproximadamente en sincronizar 20.000 máquinas virtuales en todas las instancias de VMware vCenter Server. La sincronización de estadísticas de VMware vCenter Server tarda una hora aproximadamente para 20.000 máquinas virtuales. De manera predeterminada, el trabajo de cálculo de costes se ejecuta todos los días y tarda aproximadamente dos horas para cada ejecución para 20.000 máquinas virtuales.

Nota En vRealize Business for Cloud 1.0, la configuración del dispositivo virtual predeterminado puede admitir hasta 20.000 máquinas virtuales. Si aumenta los límites del dispositivo virtual más allá de su configuración predeterminada, no aumentará el número de máquinas virtuales que puede admitir.

Consideraciones sobre configuración de alta disponibilidad de vRealize Automation

Si necesita que el sistema sea lo más robusto posible, configure el sistema vRealize Automation para alta disponibilidad siguiendo las directrices de VMware.

Dispositivo de vRealize Automation

Dispositivo de vRealize Automation admite una alta disponibilidad activa-activa para todos los componentes salvo la base de datos del dispositivo. A partir de la versión 7.3, la conmutación por error de base de datos es automática si se implementan tres nodos y dos de ellos tienen configurada la replicación sincrónica entre ellos. Cuando el Dispositivo de vRealize Automation detecta errores de base de datos, promueve un servidor de base de datos adecuado para que sea el nodo principal. Puede supervisar y administrar la base de datos de dispositivo en la pestaña **Configuración de vRA > Base de datos** de la consola de administración del dispositivo virtual.

Para habilitar la alta disponibilidad para estos dispositivos, ubíquelos bajo un equilibrador de carga. Para obtener más información, consulte [Configurar el equilibrador de carga](#). A partir de la versión 7.0, la base de datos de dispositivos y vRealize Orchestrator se agruparán en clúster automáticamente y estarán disponibles para su uso.

Administración de directorios de vRealize Automation

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. No importa qué conector elija para usar como conector de sincronización. Para admitir la alta disponibilidad de la administración de directorios, es necesario configurar un segundo conector que corresponda al segundo dispositivo de vRealize Automation, el cual se conecta con el proveedor de identidades y apunta a la misma instancia de Active Directory. Con esta configuración, si se produce un error en un dispositivo, el otro se encarga de administrar la autenticación de usuarios.

En un entorno de alta disponibilidad, todos los nodos deben prestar servicio al mismo conjunto de directorios de Active Directory, usuarios, métodos de autenticación, etc. El método más directo para lograr esto es promocionar el proveedor de identidades en el clúster estableciendo el host del equilibrador de carga como el host del proveedor de identidades. Con esta configuración, todas las solicitudes de autenticación se dirigen al equilibrador de carga, que reenvía la solicitud al conector que corresponda.

Para obtener más información acerca de cómo configurar la administración de directorios para alta disponibilidad, consulte la sección [Configure Directories Management for High Availability](#).

Servidor de Infraestructura Web

Todos los componentes del servidor web de infraestructura admiten alta disponibilidad activa-activa. Para habilitar la alta disponibilidad para estos componentes, ubíquelos bajo un equilibrador de carga.

Manager Service de infraestructura

El componente Manager Service admite alta disponibilidad activa-pasiva. Para habilitar la alta disponibilidad para este componente, ubique dos instancias de Manager Service bajo un equilibrador de carga. En vRealize Automation 7.3 y versiones posteriores, la conmutación por error es automática.

Si se produce un error en la instancia activa de Manager Service, detenga el servicio de Windows si aún no se ha detenido bajo el equilibrador de carga. Habilite la instancia pasiva de Manager Service y reinicie el servicio de Windows bajo el equilibrador de carga. Consulte [Instalar el Manager Service activo](#).

Agentes

Los agentes admiten alta disponibilidad activa-activa. Para obtener información sobre cómo configurar agentes para alta disponibilidad, consulte la documentación sobre configuración de vRealize Automation. Compruebe la alta disponibilidad del servicio de destino.

Trabajo de Distributed Execution Manager

Un Distributed Execution Manager (DEM) que se ejecuta bajo el rol Trabajo admite alta disponibilidad activa-activa. Si se produce un error en una instancia de trabajo de DEM, el orquestador de DEM detecta el error y cancela los flujos de trabajo que se están ejecutando en la instancia de trabajo de DEM.

Cuando la instancia de trabajo de DEM vuelve a estar en línea, detecta que el orquestador de DEM ha cancelado los flujos de trabajo de la instancia y detiene su ejecución. Para evitar que los flujos de trabajo se cancelen prematuramente, deje una instancia de trabajo de DEM sin conexión durante varios minutos antes de cancelar sus flujos de trabajo.

Orquestador de Distributed Execution Manager

Los DEM que se ejecutan bajo el rol Orquestador admiten alta disponibilidad activa-activa. Cuando se inicia un orquestador de DEM, este busca otro orquestador de DEM que se esté ejecutando.

- Si no encuentra ninguna instancia de orquestador de DEM en ejecución, empieza a ejecutarse como el orquestador de DEM principal.
- Si no encuentra ningún otro orquestador de DEM en ejecución, supervisa los otros orquestadores de DEM principales para detectar una interrupción.
- Si detecta una, se encarga de ella como instancia principal.

Cuando la instancia principal anterior vuelve a estar en línea, esta detecta que otra instancia de orquestador de DEM se ha encargado de su rol como instancia principal y supervisa la instancia de orquestador principal en busca de errores.

Servidor de base de datos de MSSQL para componentes de infraestructura

vRealize Automation solo admite grupos de SQL AlwaysON con Microsoft SQL Server 2016. Al instalar SQL Server 2016, la base de datos debe crearse en el modo 100. Si utiliza una versión anterior de Microsoft SQL Server, utilice una instancia de clúster de conmutación por error con discos compartidos. Para obtener más información sobre cómo configurar grupos de SQL AlwaysOn con MSDTC, consulte el artículo de Microsoft <https://msdn.microsoft.com/en-us/library/ms366279.aspx>.

vRealize Orchestrator

Se suministra una instancia de alta disponibilidad interna de vRealize Orchestrator como parte del dispositivo de vRealize Automation.

Consideraciones sobre alta disponibilidad de vRealize Business for Cloud

Use la característica VMware vSphere HA para el dispositivo de vRealize Business for Cloud Edition.

Para configurar la función VMware vSphere HA en el host de VMware ESXi, consulte la documentación sobre administración de vCenter Server y host.

Especificaciones del hardware y valores máximos de capacidad de vRealize Automation

Instale los componentes adecuados según sus necesidades de configuración y capacidad en cada perfil de servidor de vRealize Automation del entorno.

| Función de servidor | Componentes | Especificaciones de hardware necesario | Especificaciones de hardware recomendado |
|---------------------------------------|---|---|--|
| Dispositivo de vRealize Automation | vRealize Automation Services, vRealize Orchestrator y base de datos de dispositivo de vRealize Automation | CPU: 4 vCPU RAM: 18 GB (consulte Escalabilidad de vRealize Automation para más información). Disco: 140 GB Red: 1 GB/s | Igual que las especificaciones de hardware necesario. |
| Servidor principal de infraestructura | Sitio web, Manager Service, orquestador de DEM, trabajo de DEM, agente proxy | CPU: 4 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s | Igual que las especificaciones de hardware necesario. |
| Servidor de Infrastructure Web | Sitio web | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s |
| Servidor de Infrastructure Manager | Manager Service, orquestador de DEM | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s |
| Infrastructure Web/Manager Server | Infrastructure Web/Manager Server | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s |
| Servidor de Infrastructure DEM | (Uno o varios) trabajos de DEM | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s por trabajo de DEM | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s por trabajo de DEM |
| Servidor de Infrastructure Agent | (Uno o varios) agentes proxy | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s |

| Función de servidor | Componentes | Especificaciones de hardware necesario | Especificaciones de hardware recomendado |
|--|--|---|--|
| Base de datos de MSSQL | Base de datos de infraestructura | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Red: 1 GB/s | CPU: 8 vCPU RAM: 16 GB Disco: 80 GB Red: 1 GB/s |
| Dispositivo de vRealize Business for Cloud | Servicios del dispositivo de vRealize Business for Cloud Servidor de base de datos de vRealize Business for Cloud | CPU: 2 vCPU RAM: 4 GB Disco: 50 GB Red: 1 GB/s | Igual que las especificaciones de hardware necesario |

Valores máximos de capacidad recomendados de vRealize Automation

Los siguientes valores máximos de capacidad de recursos son válidos para un perfil de implementación a gran escala de vRealize Automation.

Tabla 1-2. Valores máximos de capacidad de recursos de vRealize Automation

| Parámetro | Valor máximo | |
|---|---|--------|
| Tenant | 100 | |
| Endpoints de vSphere | 20 | |
| Recursos informáticos | 200 | |
| Máquinas administradas | 75.000 | |
| Máximo de solicitudes simultáneas | | |
| | constantes | 50 |
| | por ráfagas | 250 |
| Máximo de solicitudes por hora | 400 | |
| Grupos empresariales | 3000 (con 10 usuarios únicos por cada grupo empresarial y sin ningún usuario miembro de más de 50 grupos empresariales) | |
| Reservas | 9.000 (con 3 reservas por grupo empresarial) | |
| Blueprints | | |
| | solo CBP | 6.000 |
| | CBP+XaaS | 8.000 |
| Elementos del catálogo | | |
| | en todos los tenants | 4.000 |
| | en un único tenant | 6.000 |
| Sincronización de usuario/grupo con 18 GB de memoria predeterminada | | |
| | número de usuarios | 95.027 |

Tabla 1-2. Valores máximos de capacidad de recursos de vRealize Automation (Continuación)

| Parámetro | Valor máximo |
|---|---|
| número de grupos | 20.403 (cada grupo contiene 4 usuarios, incluido un nivel de anidamiento) |
| Usuario/grupo con un aumento a 30 GB de memoria | |
| número de usuarios | 100.000 |
| número de grupos | 750 (cada grupo contiene 4.000 usuarios y cada usuario se encuentra en 30 grupos) |

Requisitos de implementaciones pequeñas de vRealize Automation

Una implementación pequeña de vRealize Automation incluye sistemas de 10.000 máquinas administradas o menos, además de las máquinas virtuales, los equilibradores de carga y las configuraciones de puertos correspondientes. La implementación pequeña sirve como punto de partida para una implementación de vRealize Automation que pueda escalarse, de manera compatible, a una implementación mediana o grande.

Al implementar vRealize Automation, use el proceso de implementación empresarial para proporcionar un sitio web de infraestructura y una dirección de Manager Service que sean independientes.

Compatibilidad

Una implementación pequeña puede admitir lo siguiente.

- 10.000 máquinas administradas
- 500 elementos del catálogo
- 10 aprovisionamientos de máquinas simultáneos

Requisitos

Una implementación pequeña debe configurarse con los componentes adecuados.

- Dispositivo de vRealize Automation: vrava-1.ra.local
- Servidor principal de infraestructura: inf-1.ra.local.
- Servidor de bases de datos MSSQL: mssql.ra.local
- Dispositivo de vRealize Business for Cloud: vrb.ra.local

Entradas de DNS

| Entrada de DNS | Apunta a |
|------------------|------------------|
| vrava.ra.local | vrava-1.ra.local |
| web.ra.local | inf.ra.local |
| manager.ra.local | inf.ra.local |

Certificados

Los nombres de host usados en esta tabla son solamente ejemplos.

| Función de servidor | CN o SAN |
|---|---|
| Dispositivo de vRealize Automation | SAN contiene vra.va.sqa.local y vra.va-1.sqa.local |
| Servidor principal de infraestructura | SAN contiene web.ra.local, managers.ra.local y inf-1.ra.local |
| Servidor de vRealize Business for Cloud | CN = vrb.ra.local |

Puertos

Los usuarios requieren acceso a ciertos puertos. Todos los puertos que figuran son puertos predeterminados.

| Función de servidor | Puerto |
|------------------------------------|---|
| Dispositivo de vRealize Automation | 443, 8444. Se requiere el puerto 8444 para Virtual Machine Remote Console. Se requiere el puerto 8283 para acceder al centro de control de vRealize Orchestrator. |

Los administradores requieren de acceso a ciertos puertos, además de los puertos que los usuarios requieren.

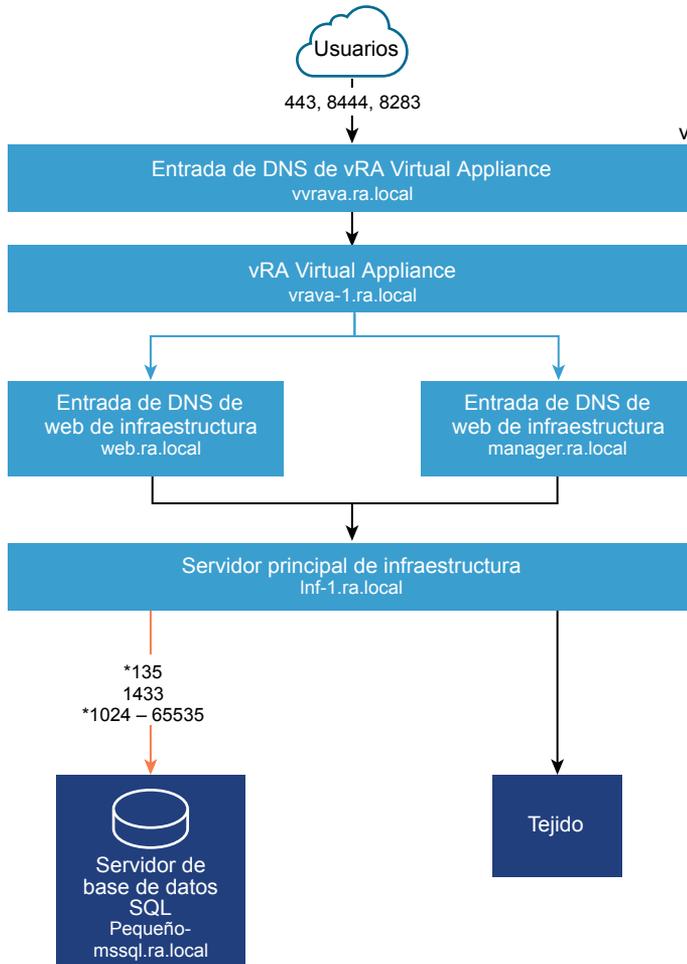
| Función de servidor | Puerto |
|------------------------------------|--|
| Dispositivo de vRealize Automation | 5480, 8443. El puerto 8443 se usa para configuración de administración de identidad avanzada. VMware Identity Manager para Active Directory: 389, 636, 3268, 3269 VMware Identity Manager para el controlador de dominio: 88, 464, 135 |
| vRealize Business for Cloud | 5480 |

| Función de servidor | Puertos entrantes | Puertos de salida del servicio/sistema |
|---------------------------------------|--|---|
| Dispositivo de vRealize Automation | HTTPS: 443 Configuración de adaptador: 8443 Proxy de Remote Console: 8444 SSH: 22 Consola de administración de dispositivo virtual: 5480 | LDAP: 389 LDAPS:636 El servidor principal de infraestructura de VMware ESXi: 902 necesita acceder al puerto de endpoint de vSphere 443 para obtener un ticket para VMware Remote Console. El dispositivo de vRealize Automation necesita acceder al puerto 902 del host de ESXi para autorizar el tráfico al usuario. Servidor principal de infraestructura: 443 Autenticación Kerberos: 88 Renovación de la contraseña de objetos de equipo: 464 |
| Servidor principal de infraestructura | HTTPS: 443 MSDTC: 135, 1024 - 65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation . | Dispositivo virtual de vRealize Automation: 443, 5480 El servidor principal de infraestructura del endpoint de vSphere: 443 necesita acceder al puerto de endpoint de vSphere 443 para obtener un ticket para VMware Remote Console. El dispositivo de vRealize Automation necesita acceder al puerto 902 del host de ESXi para autorizar el tráfico al usuario. MSSQL: 135, 1433, 1024-65535 MSDTC: 135, 1024 - 65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de |

| Función de servidor | Puertos entrantes | Puertos de salida del servicio/sistema |
|--|---|--|
| | | implementación de bases de datos de Implementación de vRealize Automation . |
| Base de datos de MSSQL | MSSQL: 1433 MSDTC: 135, 1024 - 65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation . | Servidor principal de infraestructura: 135, 1024 a 65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation . MSDTC: 135, 1024 - 65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation . |
| Dispositivo de vRealize Business for Cloud | HTTPS: 443 SSH: 22 Consola de administración de dispositivo virtual: 5480 | Dispositivo virtual de vRealize Automation: 443 Servidor principal de infraestructura: 443 |
| Catálogo global | | Catálogo global: 3268, 3269 |

Espacios físicos mínimos

Figura 1-1. Espacio físico mínimo de una configuración pequeña de vRealize Automation



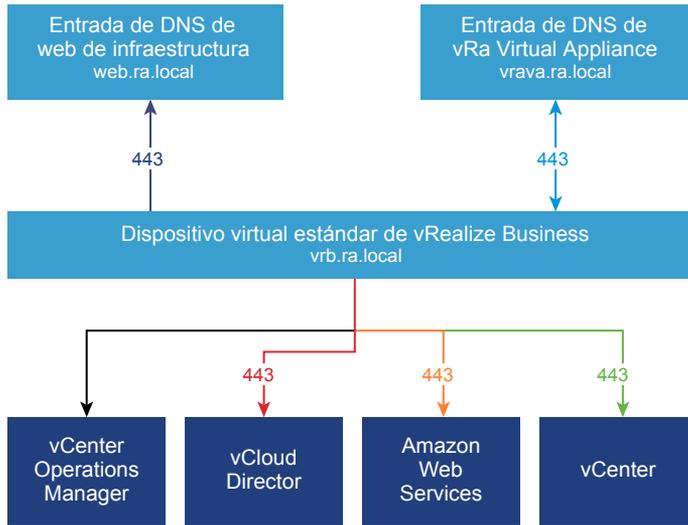
No se muestra:
 todos los sistemas de infraestructura requieren acceso al puerto 5480 de todas las instancias de vRealize Appliance para la recopilación de logs (Configuración de vRA > Clúster > Recopilar logs en el dispositivo virtual:5480) para que funcionen.

Para la consola remota de máquina virtual, vRealize Appliance requiere acceso al puerto 902 de VMware ESXi y el servidor de Infrastructure Core requiere acceso al puerto 443 del endpoint de vSphere.

* Consulte la sección de implementación de la base de datos para obtener información sobre cómo restringir este intervalo.

Además, se requiere una comunicación bidireccional.

Figura 1-2. Espacio físico mínimo de una configuración pequeña de vRealize Business for Cloud



Requisitos de implementaciones medianas de vRealize Automation

Una implementación mediana de vRealize Automation se compone de sistemas de 30.000 máquinas administradas o menos, e incluye las configuraciones de puerto, los equilibradores de carga y las máquinas virtuales apropiadas.

Compatibilidad

Una implementación mediana puede admitir los siguientes elementos.

- 30.000 máquinas administradas
- 1.000 elementos del catálogo
- 50 aprovisionamientos de máquinas

Requisitos

Una implementación mediana debe cumplir con los requisitos de configuración del sistema apropiados.

Dispositivos virtuales

- Dispositivo de vRealize Automation 1: vrava-1.ra.local
- Dispositivo de vRealize Automation 2: vrava-2.ra.local
- Dispositivo de vRealize Automation 3: vrava-3.ra.local
- Dispositivo de vRealize Business for Cloud: vrb.ra.local

Máquinas virtuales de Windows Server

- Servidor de Infraestructura Web/Manager 1 (Active Web o DEM-O, Active Manager): inf-1.ra.local

- Servidor de Infrastructure Web/Manager 2 (Active Web o DEM-O, Active Manager): inf-2.ra.local
- Servidor de Infrastructure DEM 1: dem-1.ra.local
- Servidor de Infrastructure DEM 2: dem-2.ra.local
- Servidor de Infrastructure Agent 1: agent-1.ra.local
- Servidor de Infrastructure Agent 2: agent-2.ra.local

Servidores de base de datos

- Instancia de clúster de conmutación por error de MSSQL: mssql.ra.local

Equilibradores de carga

- Equilibrador de carga de Dispositivo de vRealize Automation: med-vrava.ra.local
- Equilibrador de carga de Infrastructure Web: med-web.ra.local
- Equilibrador de carga de Infrastructure Manager Service: med-manager.ra.local

Certificados

Los nombres de hosts que se usan en esta tabla son solo ejemplos.

| Función de servidor | CN o SAN |
|--|---|
| Dispositivo de vRealize Automation | SAN contiene los siguientes nombres de host: <ul style="list-style-type: none"> ▪ vrava.ra.local ▪ vrava-1.ra.local ▪ vrava-2.ra.local |
| Infrastructure Web o Manager Server | SAN contiene los siguientes nombres de host: <ul style="list-style-type: none"> ▪ web.ra.local ▪ manager.ra.local ▪ inf-1.ra.local ▪ inf-2.ra.local |
| Dispositivo de vRealize Business for Cloud | CN = vrb.ra.local |

Puertos

Los usuarios requieren acceso a ciertos puertos. Todos los puertos que figuran son puertos predeterminados.

| Función de servidor | Puerto |
|---|--|
| Equilibrador de carga de Dispositivo de vRealize Automation | 443, 8444. Se requiere el puerto 8444 para Virtual Machine Remote Console. |

Los administradores requieren de acceso a ciertos puertos, además de los puertos que los usuarios requieren.

| Función de servidor | Puerto |
|--|--|
| Dispositivo de vRealize Automation fVAMI | 5480, 8443. El puerto 8443 está destinado a la configuración de administración de identidad avanzada. VMware Identity Manager para Active Directory: 389, 636, 3268, 3269 VMware Identity Manager para el controlador de dominio: 88, 464, 135 |
| Centro de control de vRealize Appliance Orchestrator | 8283 |
| Servidor de vRealize Business for Cloud | 5480 |

En la siguiente tabla se muestran las comunicaciones entre aplicaciones.

| Función de servidor | Puertos entrantes | Puertos salientes para servicio o sistema |
|------------------------------------|--|---|
| Dispositivo de vRealize Automation | HTTPS: Configuración de adaptador: 8443 Proxy de Remote Console: 8444 Postgres: 5432 RabbitMQ: 4369, 25672, 5671, 5672 ElasticSearch: 9300, 40002, 40003 Stomp: 61613 SSH: 22 | LDAP: 389 LDAPS: 636 Dispositivo de vRealize Automation (todos los demás): 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003 Equilibrador de carga de Infrastructure Web de vRealize Automation: 443 VMware ESXi: 902 Infrastructure Web o Manager requiere acceso al puerto de endpoint de vSphere443 para obtener un ticket para Virtual Machine Remote Console. Dispositivo de vRealize Automation requiere acceso al puerto host ESXi 902 para enviar mediante proxy datos de la consola al usuario. Autenticación Kerberos: 88 Renovación de la contraseña de objetos de equipo: 464 |
| Infrastructure Web/Manager Server | HTTPS: 443 MSDTC: 135, 1024-65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation . | Equilibrador de carga de Dispositivo de vRealize Automation: 443 Equilibrador de carga de Infrastructure Web de vRealize Automation: 443 Dispositivo de vRealize Automation(VA): 5480. Endpoint de vSphere: 443. Infrastructure Web o Manager requiere acceso al puerto de endpoint de vSphere443 para obtener un ticket para Virtual Machine Remote Console. Dispositivo de vRealize Automation requiere acceso al puerto host ESXi 902 para enviar mediante proxy datos de la consola al usuario. MSSQL: 135, 1433, 1024 a 65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation . |
| Servidor de Infrastructure DEM | No corresponde | Equilibrador de carga del dispositivo de vRealize Automation: 443 Equilibrador de carga de Infrastructure Web de vRealize Automation: 443 Equilibrador de carga de Infrastructure Manager de vRealize Automation: 443 Dispositivo de vRealize Automation(VA): 5480. |

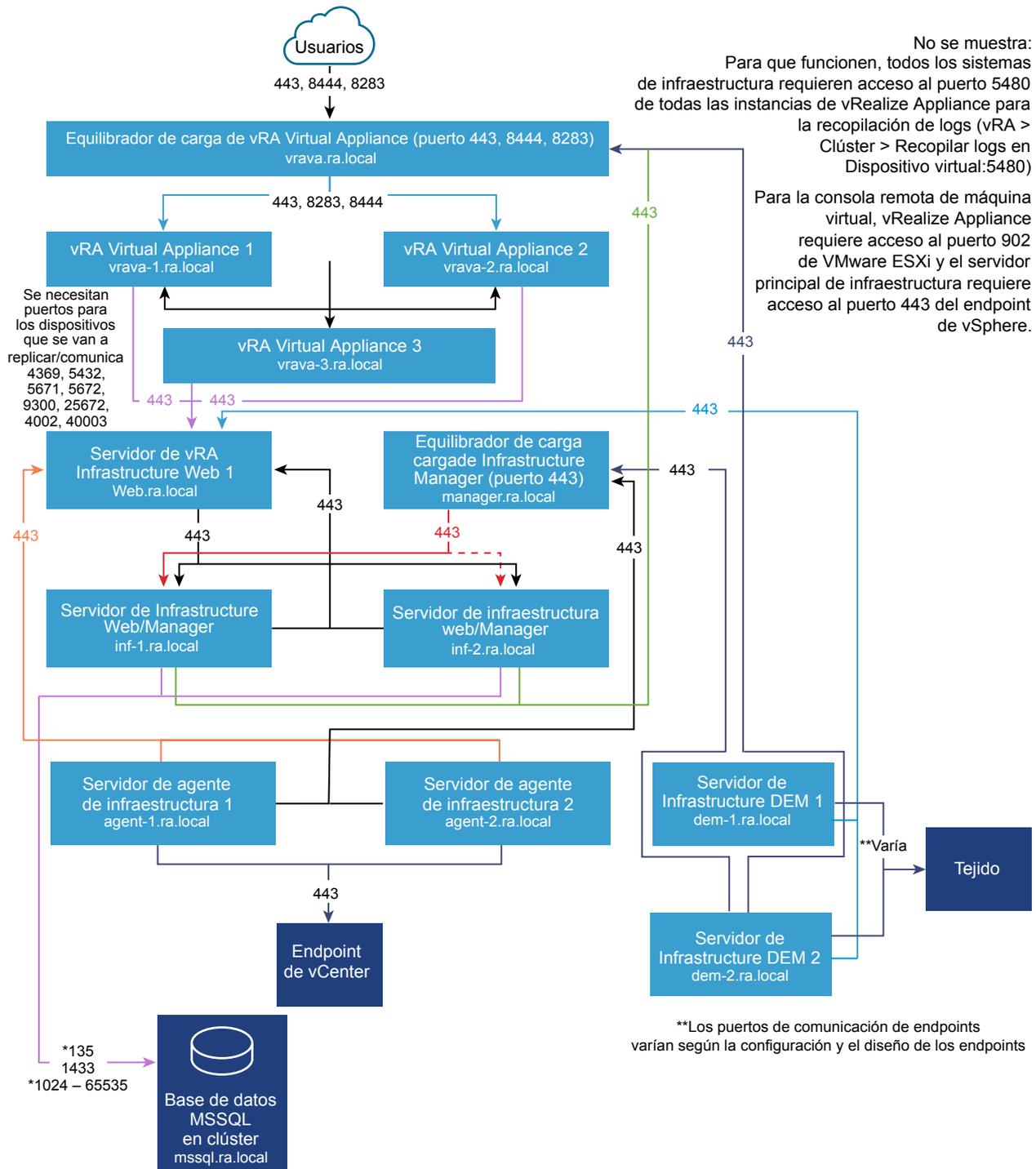
| Función de servidor | Puertos entrantes | Puertos salientes para servicio o sistema |
|---|---|--|
| Servidor de Infrastructure Agent | No corresponde | Equilibrador de carga de Infrastructure Web de vRealize Automation: 443 Equilibrador de carga de Infrastructure Manager de vRealize Automation: 443 Dispositivo de vRealize Automation(VA): 5480. |
| Base de datos de MSSQL | MSSQL: 1433 MSDTC: 135, 1024 - 65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation . | Infrastructure Web/Manager Server: 135, 1024 - 65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation . |
| Servidor de vRealize Business for Cloud | HTTPS: 443 SSH: 22 Consola de administración de dispositivo virtual: 5480 | Equilibrador de carga del dispositivo de vRealize Automation: 443 Equilibrador de carga de Infrastructure Web de vRealize Automation: 443 |
| Catálogo global | | Catálogo global: 3268, 3269 |

Los equilibradores de carga requieren de acceso a través de los siguientes puertos.

| Equilibrador de carga | Puertos equilibrados |
|--|----------------------|
| Equilibrador de carga de Dispositivo de vRealize Automation | 443, 8444 |
| Equilibrador de carga de Infrastructure Web de vRealize Automation | 443 |
| Equilibrador de carga de Infrastructure Manager Service de vRealize Automation | 443 |

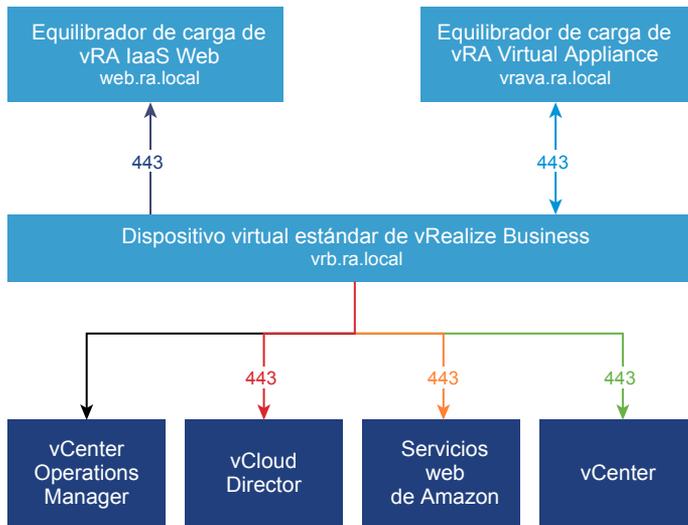
Gráficos

Figura 1-3. Huella mínima para configuración mediana de vRealize Automation



* Consulte la sección de implementación de la base de datos para obtener información sobre cómo restringir este intervalo. Además, se requiere una comunicación bidireccional.

Figura 1-4. Huella mínima para implementación mediana de vRealize Business for Cloud



Requisitos de implementaciones grandes de vRealize Automation

Una implementación mayor de vRealize Automation se compone de sistemas de 50.000 máquinas administradas o menos, e incluye las configuraciones de puerto, los equilibradores de carga y las máquinas virtuales apropiadas.

Compatibilidad

Una implementación mayor puede admitir los siguientes elementos.

- 50.000 máquinas administradas
- 2.500 elementos del catálogo
- 100 aprovisionamientos de máquinas simultáneas

Requisitos

Una implementación mayor debe cumplir con los requisitos de configuración del sistema apropiados.

Dispositivos virtuales

- Dispositivo de vRealize Automation 1: vrava-1.ra.local
- Dispositivo de vRealize Automation 2: vrava-2.ra.local
- Dispositivo de vRealize Automation 2: vrava-3.ra.local
- Dispositivo de vRealize Automation: vrb.ra.local

Máquinas virtuales de Windows Server

- Servidor de Infrastructure Web 1: web-1.ra.local
- Servidor de Infrastructure Web 2: web-2.ra.local

- Servidor de Infrastructure Manager 1: manager-1.ra.local
- Servidor de Infrastructure Manager 2: manager-2.ra.local
- Servidor de Infrastructure DEM 1: dem-1.ra.local
- Servidor de Infrastructure DEM 2: dem-2.ra.local
- Servidor de Infrastructure Agent 1: agent-1.ra.local
- Servidor de Infrastructure Agent 2: agent-2.ra.local
- Base de datos de MSSQL en clúster: mssql.ra.local

Equilibradores de carga

- Equilibrador de carga del dispositivo de vRealize Automation: vrava.ra.local
- Equilibrador de carga de Infrastructure Web: web.ra.local
- Equilibrador de carga de Infrastructure Manager Service: manager.ra.local

Certificados

Los nombres de host usados en esta tabla son solamente ejemplos.

| Función de servidor | CN o SAN |
|--|---|
| Dispositivo de vRealize Automation | SAN contiene los siguientes nombres de host: <ul style="list-style-type: none"> ▪ vrava.ra.local ▪ vrava-1.ra.local ▪ vrava-2.ra.local |
| Servidor de Infrastructure Web | SAN contiene los siguientes nombres de host: <ul style="list-style-type: none"> ▪ web.ra.local ▪ web-1.ra.local ▪ web-2.ra.local |
| Servidor de Infrastructure Manager | SAN contiene los siguientes nombres de host: <ul style="list-style-type: none"> ▪ manager.ra.local ▪ manager-1.ra.local ▪ manager-2.ra.local |
| Dispositivo de vRealize Business for Cloud | CN = vrb.ra.local |

Puertos

Los usuarios requieren acceso a ciertos puertos. Todos los puertos que figuran son puertos predeterminados.

| Función de servidor | Puerto |
|--|--|
| Equilibrador de carga del dispositivo de vRealize Automation | 443, 8444. El puerto 88444 es necesario para la VMware Remote Console. |

Los administradores requieren de acceso a ciertos puertos, además de los puertos que los usuarios requieren.

| Función de servidor | Puerto |
|---|--|
| Dispositivo de vRealize Automation | 5480, 8443. El puerto 8443 se usa para configuración de administración de identidad avanzada. VMware Identity Manager para Active Directory: 389, 636, 3268, 3269 VMware Identity Manager para el controlador de dominio: 88, 464, 135 |
| Servidor de vRealize Business for Cloud | 5480 |

El sistema debe admitir las comunicaciones apropiadas internas de la aplicación.

| Función de servidor | Puertos entrantes | Puertos salientes para servicio o sistema |
|------------------------------------|---|--|
| vRealize Automation | | |
| Dispositivo de vRealize Automation | HTTPS: 443 Configuración de adaptador: 8443 Proxy de Remote Console: 8444 Postgres: 5432 Rabbit MQ: 4369, 25672, 5671, 5672 ElasticSearch: 9300, 40002, 40003 Stomp: 61613 SSH: 22 Control-Center: 8283 | LDAP: 389 LDAPS: 636 Dispositivo de vRealize Automation: 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003. Equilibrador de carga de Infrastructure Web de vRealize Automation: 443 VMware ESXi: 902 Infrastructure Web necesita acceder al puerto de endpoint de vSphere 443 para obtener un ticket para VMware Remote Console. Dispositivo de vRealize Automation requiere acceso al puerto host ESXi 902 para enviar mediante proxy datos de la consola al usuario. Autenticación Kerberos: 88 Renovación de la contraseña de objetos de equipo: 464 |

| Función de servidor | Puertos entrantes | Puertos salientes para servicio o sistema |
|------------------------------------|---|--|
| Servidor de Infrastructure Web | <p>HTTPS: 443</p> <p>MSDTC: 443, 1024-65535.</p> <p>Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation.</p> | <p>Equilibrador de carga del dispositivo de vRealize Automation: 443</p> <p>Dispositivo virtual del dispositivo de vRealize Automation: 5480.</p> <p>Endpoint de vSphere: 443.</p> <p>Infrastructure Web necesita acceder al puerto de endpoint de vSphere 443 para obtener un ticket para VMware Remote Console. El dispositivo de vRealize Automation necesita acceder al puerto de host ESXi 902 para enviar datos de la consola al usuario mediante proxy.</p> <p>MSSQL: 135, 1433, 1024 a 65535.</p> <p>Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation.</p> |
| Servidor de Infrastructure Manager | <p>HTTPS: 443</p> <p>MSDTC: 135,1024-65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation.</p> | <p>Equilibrador de carga del dispositivo de vRealize Automation: 443</p> <p>Equilibrador de carga de Infrastructure Web de vRealize Automation: 443</p> <p>Dispositivo de vRealize Automation: 443, 5480</p> <p>MSSQL: 135, 1433, 1024 a 65535.</p> <p>Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation.</p> |
| Servidor de Infrastructure DEM | No corresponde | <p>Equilibrador de carga del dispositivo de vRealize Automation: 443</p> <p>Equilibrador de carga de Infrastructure Web de vRealize Automation: 443</p> <p>Equilibrador de carga de Infrastructure Manager de vRealize Automation: 443</p> <p>Equilibrador de carga de vRealize Orchestrator: 8281</p> <p>Dispositivo de vRealize Automation: 5480.</p> |

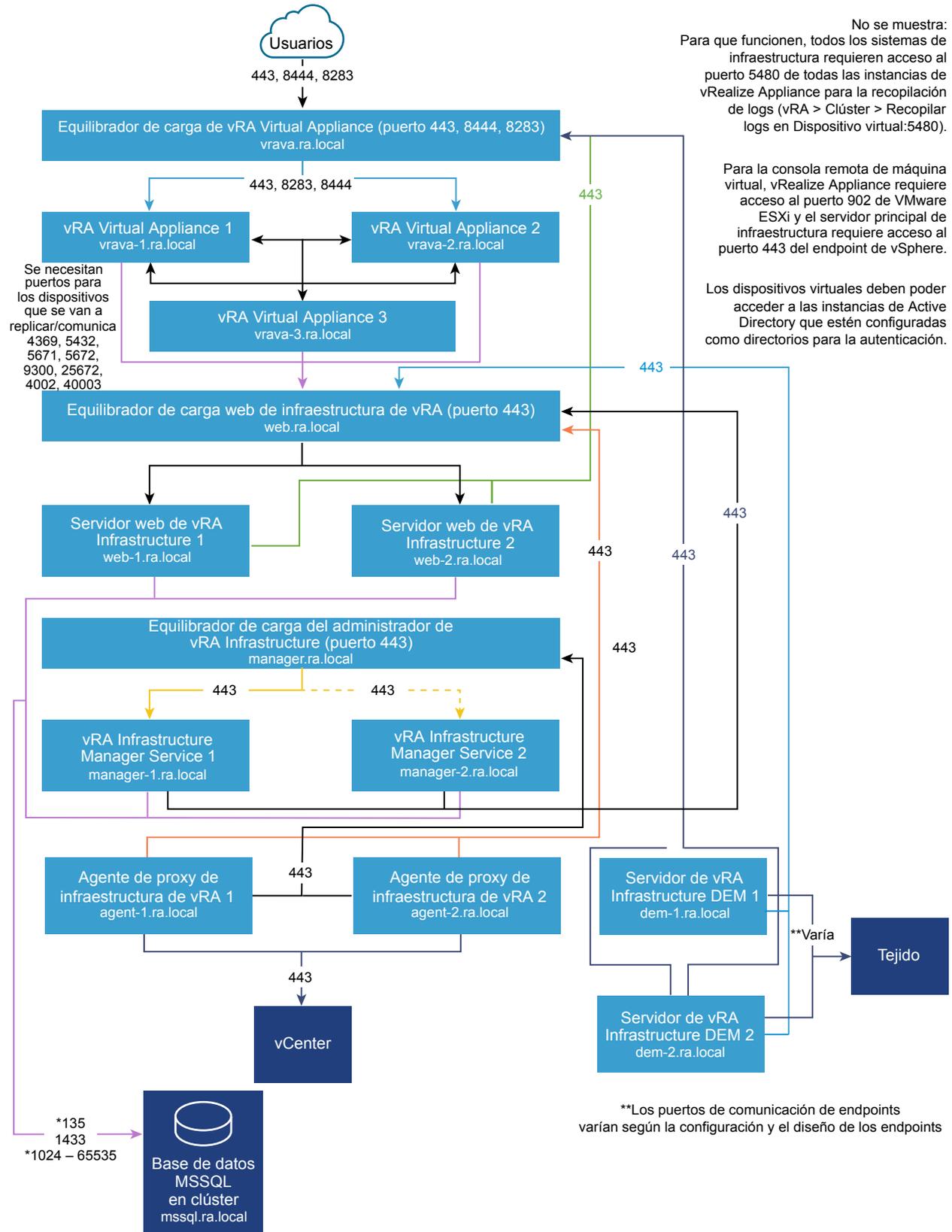
| Función de servidor | Puertos entrantes | Puertos salientes para servicio o sistema |
|---|--|--|
| Servidor de Infrastructure Agent | No corresponde | Equilibrador de carga de Infrastructure Web de vRealize Automation: 443 Equilibrador de carga de Infrastructure Manager de vRealize Automation: 443 Dispositivo de vRealize Automation: 5480. |
| Base de datos de MSSQL | MSSQL: 1433 MSDTC: 135, 1024-65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation . | Servidor de Infrastructure Web: 135, 1024-65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation . Servidor de Infrastructure Manager: 135, 1024-65535. Para obtener información acerca de cómo reducir este rango, consulte la sección de implementación de bases de datos de Implementación de vRealize Automation . |
| Servidor de vRealize Business for Cloud | HTTPS: 443 SSH: 22 Consola de administración de dispositivo virtual: 5480 | Equilibrador de carga del dispositivo de vRealize Automation: 443 Equilibrador de carga de Infrastructure Web de vRealize Automation: 443 |
| Catálogo global | | Catálogo global: 3268, 3269 |

Los equilibradores de carga requieren de acceso a través de los siguientes puertos.

| Equilibrador de carga | Puertos equilibrados |
|--|----------------------|
| Equilibrador de carga del dispositivo de vRealize Automation | 443, 8444 |
| Equilibrador de carga de Infrastructure Web de vRealize Automation | 443 |
| Equilibrador de carga de Manager Server de vRealize Automation | 443 |

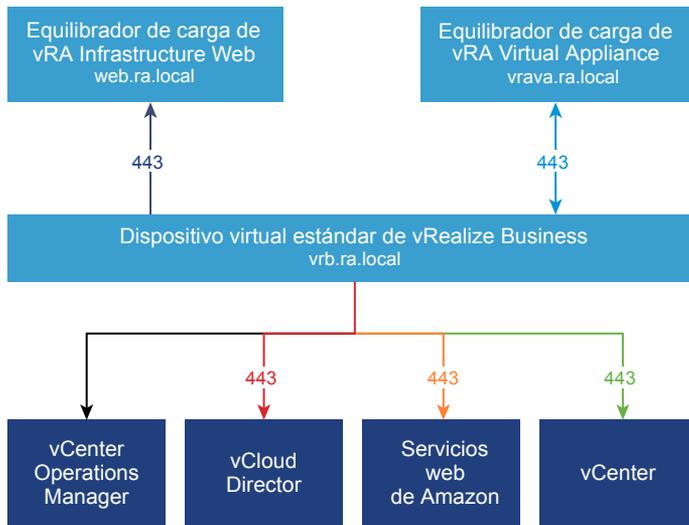
Gráficos

Figura 1-5. Huella mínima para configuración mayor de vRealize Automation



* Consulte la sección de implementación de la base de datos para obtener información sobre cómo restringir este intervalo. Además, se requiere una comunicación bidireccional. VMware, Inc.

Figura 1-6. Huella mínima para configuración mayor de vRealize Business for Cloud



Implementaciones de datos de centros de multidados de vRealize Automation

vRealize Automation admite la administración de recursos en centros de datos remotos.

Para administrar los recursos de Xen, HyperV o vSphere en centros de datos remotos, implemente el agente de proxy en una máquina virtual del centro de datos remoto.

Nota En el siguiente diagrama se muestra una implementación de vSphere. Otros endpoints no requieren que se configuren otra vez.

Debido a que los flujos de trabajo de vRealize Orchestrator se comunican potencialmente a través de una WAN, siga las prácticas recomendadas tal como se especifican en la *vRealize Orchestrator guía de diseño de codificación de* .

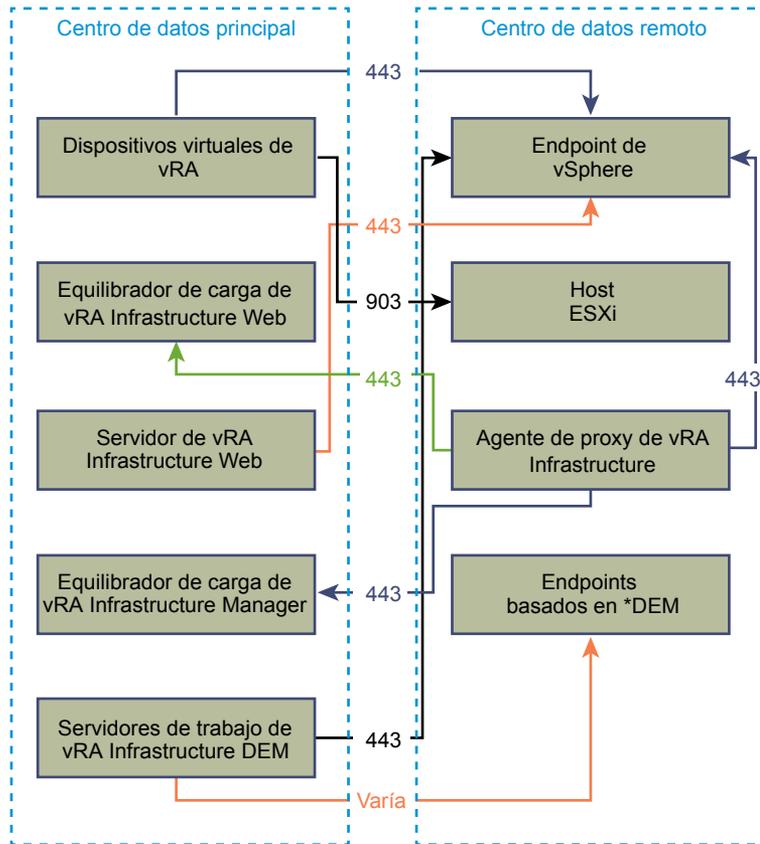
Tabla 1-3. Puertos necesarios para la comunicación WAN

| Función | Puertos entrantes | Puertos de salida del servicio/sistema |
|--|---|---|
| Dispositivo de vRealize Automation - incluidos vRealize Orchestrator integrado | No corresponde | Endpoint de vSphere: 443 Hosts ESXi: 903 |
| Equilibrador de carga de Infrastructure de vRealize Automation | Agente de proxy de Infrastructure de vRealize Automation: 443 | No corresponde |
| Servidor de Infrastructure Web de vRealize Automation | No corresponde | Endpoint de vSphere: 443 |
| Equilibrador de carga de Infrastructure Manager de vRealize Automation | Agente de proxy de Infrastructure de vRealize Automation: 443 | No corresponde |
| Servidores de trabajo de Infrastructure DEM de vRealize Automation | No corresponde | Endpoint: ** varía |

* Si los trabajos de DEM se instalan en la máquina de Manager Service o en otro servidor, estos puertos deben estar abiertos entre dicha máquina y el endpoint de destino.

** El puerto que se requiere para comunicarse con un endpoint externo varía según el endpoint. De forma predeterminada, para vSphere es el puerto 443.

Figura 1-7. Configuración de varios sitios de vRealize Automation



Configuración segura de vRealize Automation

La configuración segura describe cómo comprobar, configurar y actualizar el perfil de seguridad de una implementación de vRealize Automation según las directrices de VMware.

La configuración segura abarca los siguientes temas:

- Seguridad de la infraestructura de software
- Seguridad de la configuración implementada
- Seguridad de la red de host

Descripción general de la línea de base segura de vRealize Automation

VMware proporciona recomendaciones integrales para permitirle comprobar y configurar una línea de base segura para el sistema de vRealize Automation.

Utilice las herramientas y los procedimientos adecuados, según lo especifica VMware, para comprobar y mantener una configuración de línea de base segura y protegida para el sistema de vRealize Automation. Algunos componentes de vRealize Automation están instalados en un estado protegido o parcialmente protegido, pero debería verificar la configuración de cada componente en función de las recomendaciones de seguridad de VMware, las políticas de seguridad de la empresa y las amenazas conocidas.

Posición de seguridad de vRealize Automation

La posición de seguridad de vRealize Automation supone un entorno seguro en general, con base en la configuración del sistema y la red, las políticas de seguridad de la organización y los procedimientos recomendados de seguridad.

Al comprobar y configurar la protección de un sistema de vRealize Automation, tenga en cuenta cada una de las siguientes áreas de acuerdo con las recomendaciones de protección de VMware.

- Implementación segura
- Configuración segura
- Seguridad de red

Para asegurarse de que su sistema está realmente protegido, tenga en cuenta las recomendaciones de VMware y las políticas de seguridad locales que se relacionan con cada una de estas áreas conceptuales.

Componentes del sistema

Al pensar en la protección y en la configuración segura del sistema de vRealize Automation, asegúrese de que conoce todos los componentes y comprende cómo funcionan juntos para respaldar la funcionalidad del sistema.

Tenga en cuenta los siguientes componentes al planificar e implementar un sistema seguro.

- Dispositivo de vRealize Automation
- Componente de IaaS

Para familiarizarse con vRealize Automation y saber cómo se complementan los componentes, consulte [Fundamentos y conceptos](#) en el centro de documentación de vRealize Automation de VMware. Para obtener información sobre las implementaciones y la arquitectura típicas de vRealize Automation, consulte [Arquitectura de referencia de vRealize Automation](#).

Comprobar la integridad de los medios de instalación

Los usuarios siempre deben comprobar la integridad de los medios de instalación antes de instalar un producto de VMware.

Revise siempre el hash SHA1 después de descargar una ISO, un paquete sin conexión o una revisión para garantizar la integridad y la autenticidad de los archivos descargados. Si obtiene los soportes físicos de VMware y el sello de seguridad está roto, devuelva el software a VMware para su reemplazo.

Después de descargar los medios, utilice el valor de suma MD5/SHA1 para comprobar la integridad de la descarga. Compare la salida del hash MD5/SHA1 con el valor publicado en el sitio web de VMware. El hash SHA1 o MD5 debe coincidir.

Para obtener más información acerca de cómo comprobar la integridad de los medios de instalación, consulte <http://kb.vmware.com/kb/1537>.

Proteger la infraestructura de software del sistema de VMware

Como parte del proceso de protección, evalúe la infraestructura de software implementada que admite el sistema de VMware y compruebe que cumpla con las directrices de protección de VMware.

Antes de proteger el sistema de VMware, revise y solucione las deficiencias de seguridad en la infraestructura del software de apoyo para crear un entorno totalmente protegido. Los elementos de la infraestructura de software que se deben considerar incluyen componentes del sistema operativo, software de apoyo y software de base de datos. Solucione los problemas de seguridad en estos y en otros componentes de acuerdo con las recomendaciones del fabricante y otros protocolos de seguridad pertinentes.

Proteger el entorno de VMware vSphere[®]

Evalúe el entorno de VMware vSphere[®] y compruebe que se aplique y se mantenga el nivel apropiado de instrucciones de protección de vSphere.

Para obtener más instrucciones relacionadas con la protección, consulte <http://www.vmware.com/security/hardening-guides.html>.

Como parte de un entorno totalmente protegido, la infraestructura de VMware vSphere[®] debe cumplir con las directrices de seguridad que VMware define.

Proteger el host de infraestructura como servicio

Compruebe que la máquina host de Microsoft Windows de infraestructura como servicio esté protegida según las directrices de VMware.

Revise las recomendaciones establecidas en las directrices apropiadas de procedimientos recomendados seguros y de protección de Microsoft Windows, y asegúrese de que el host de Windows Server esté protegido correctamente. Si no se siguen las recomendaciones de protección, puede quedar expuesto a vulnerabilidades de seguridad conocidas de los componentes inseguros de las versiones de Windows.

Para comprobar que la versión es compatible, consulte la [matriz de soporte de vRealize Automation](#).

Pregunte a su proveedor de Microsoft acerca de las directrices correctas de los procedimientos de protección de los productos de Microsoft.

Proteger Microsoft SQL Server

Compruebe que la base de datos de Microsoft SQL Server cumpla con las directrices de seguridad establecidas por Microsoft y VMware.

Revise las recomendaciones establecidas en las directrices apropiadas de procedimientos recomendados seguros y de protección de Microsoft SQL Server. Revise todos los boletines de seguridad de Microsoft con respecto a la versión instalada de Microsoft SQL Server. Si no sigue las recomendaciones de protección, puede quedar expuesto a vulnerabilidades de seguridad conocidas de los componentes inseguros de las versiones de Microsoft SQL Server.

Para comprobar que se admite la versión de Microsoft SQL Server, consulte la [matriz de soporte de vRealize Automation](#).

Póngase en contacto con el proveedor de Microsoft para obtener consejos sobre la prácticas de protección de los productos de Microsoft.

Proteger Microsoft .NET

Como parte de un entorno totalmente protegido, Microsoft .NET debe cumplir con las directrices de seguridad establecidas por Microsoft y VMware.

Revise las recomendaciones establecidas en las directrices apropiadas de procedimientos recomendados seguros y de protección de .NET. Además, revise todos los boletines de seguridad de Microsoft sobre la versión de Microsoft SQL Server que está utilizando. Si no se siguen las recomendaciones de protección, puede quedar expuesto a vulnerabilidades de seguridad conocidas de los componentes inseguros de Microsoft.NET.

Para comprobar que su versión de Microsoft.NET es compatible, consulte la [matriz de soporte de vRealize Automation](#).

Póngase en contacto con su proveedor de Microsoft para obtener consejos sobre las prácticas de protección de los productos de Microsoft.

Proteger Microsoft Internet Information Services (IIS)

Compruebe que Microsoft Internet Information Services (IIS) cumpla con todas las directrices de seguridad de Microsoft y de VMware.

Revise las recomendaciones establecidas en las directrices apropiadas de procedimientos recomendados seguros y de protección de Microsoft IIS. Además, revise todos los boletines de seguridad de Microsoft sobre la versión de IIS que está utilizando. Si no se siguen las recomendaciones de protección, puede quedar expuesto a vulnerabilidades de seguridad conocidas.

Para comprobar que la versión es compatible, consulte la [matriz de soporte de vRealize Automation](#).

Póngase en contacto con su proveedor de Microsoft para obtener consejos sobre las prácticas de protección de los productos de Microsoft.

Revisar el software instalado

Debido a que las vulnerabilidades del software de terceros y del software no utilizado aumentan el riesgo de accesos no autorizados al sistema y de interrupciones de disponibilidad, es importante revisar todo el software instalado en las máquinas host de VMware y evaluar su uso.

No instale ningún software que no sea necesario para el funcionamiento seguro del sistema en las máquinas host de VMware. Desinstale el software irrelevante o que no se utiliza.

Realizar un inventario del software instalado no compatible

Evalúe la implementación de VMware y realice un inventario de los productos instalados para asegurarse de que no se haya instalado ningún software irrelevante y no compatible.

Para obtener más información acerca de las políticas de soporte para productos de terceros, consulte el artículo de soporte de VMware, en <https://www.vmware.com/support/policies/thirdparty.html>.

Comprobar el software de terceros

VMware no admite ni recomienda la instalación de software de terceros que no se haya probado y verificado. El software de terceros no seguro, no revisado o sin autenticar que se instale en las máquinas host de VMware puede causar accesos no autorizados e interrupción de la disponibilidad. Si debe usar software de terceros no compatible, pida al proveedor externo la configuración segura y los requisitos de revisiones.

Avisos de seguridad y revisiones de VMware

Para mantener la máxima seguridad en el sistema, siga los avisos de seguridad de VMware y aplique todas las revisiones correspondientes.

VMware publica avisos de seguridad relacionados con los productos. Supervise estos avisos para asegurarse de que su producto está protegido contra las amenazas conocidas.

Evalúe la instalación, las revisiones y el historial de actualizaciones de vRealize Automation, y compruebe que los avisos de seguridad de VMware publicados se sigan y se apliquen.

Para obtener más información sobre los avisos de seguridad de VMware actuales, consulte <http://www.vmware.com/security/advisories/>.

Configuración segura

Compruebe y actualice la configuración de seguridad de los dispositivos virtuales de vRealize Automation y del componente de infraestructura como servicio según corresponda para la configuración del sistema. Asimismo, compruebe y actualice la configuración de otros componentes y aplicaciones.

La configuración segura de una instalación de vRealize Automation implica abordar la configuración de cada componente de forma individual y cuando están trabajando juntos. Considere la configuración de los componentes de todos los sistemas en conjunto para lograr una línea de base razonablemente segura.

Proteger el dispositivo de vRealize Automation

Compruebe y actualice la configuración de seguridad del dispositivo de vRealize Automation como corresponda para la configuración del sistema.

Configure los ajustes de seguridad para los dispositivos virtuales y sus sistemas operativos host. Además, establezca o compruebe la configuración de aplicaciones y componentes relacionados adicionales. En algunos casos, debe comprobar la configuración existente, mientras que en otros casos debe cambiar o agregar valores para realizar la configuración de forma adecuada.

Cambiar la contraseña raíz

Puede cambiar la contraseña raíz para que Dispositivo de vRealize Automation cumpla con los requisitos de seguridad correspondientes.

Cambie la contraseña raíz en el Dispositivo de vRealize Automation mediante la interfaz de administración de dispositivos virtuales. Compruebe que la contraseña raíz cumpla con los requisitos de complejidad de contraseña corporativa de la organización.

Procedimiento

- 1 Abra la interfaz de administración de dispositivos virtuales de Dispositivo de vRealize Automation.
<https://vRealizeAppliance-url:5480>
- 2 Seleccione la pestaña **Administración** en la interfaz de administración de dispositivos virtuales.
- 3 Seleccione el submenú **Administración**.
- 4 Introduzca la contraseña existente en el cuadro de texto **Contraseña de administrador actual**.
- 5 Introduzca la nueva contraseña en el cuadro de texto **Contraseña de administrador nueva**.
- 6 Introduzca la nueva contraseña en el cuadro de texto **Volver a escribir la nueva contraseña de administrador**.
- 7 Haga clic en **Guardar configuración** para guardar los cambios.

Comprobar la complejidad y el hash de la contraseña raíz

Compruebe que la contraseña raíz cumpla con los requisitos de complejidad de contraseña corporativa de la organización.

Es necesario validar la complejidad de la contraseña raíz debido a que el usuario raíz sortea la comprobación de complejidad de la contraseña del módulo pam_cracklib que se aplica a las cuentas de usuario.

La contraseña de la cuenta debe comenzar con \$6\$, lo que indica un hash sha512. Este es el hash estándar para todos los dispositivos protegidos.

Procedimiento

- 1 Para comprobar el hash de la contraseña raíz, inicie sesión como usuario raíz y ejecute el comando `# more /etc/shadow`.

Se muestra la información del hash.

Figura 1-8. Resultados del hash de la contraseña

```
vcac148-084-111:~ $ more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870:::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870:::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KezK4SS44UEHPfAtgsP/16346:0:365:7:::
```

- 2 Si la contraseña raíz no contiene un hash sha512, ejecute el comando `passwd` para cambiarla.

Todos los dispositivos protegidos habilitan `enforce_for_root` en el módulo `pw_history`, que se encuentra en el archivo `etc/pam.d/common-password`. El sistema recuerda las últimas cinco contraseñas de forma predeterminada. Las contraseñas antiguas de cada usuario se almacenan en el archivo `/etc/securetty/passwd`.

Comprobar historial de contraseñas raíz

Compruebe que el historial de contraseñas se aplique a la cuenta raíz.

Todos los dispositivos protegidos habilitan `enforce_for_root` en el módulo `pw_history`, que se encuentra en el archivo `etc/pam.d/common-password`. El sistema recuerda las últimas cinco contraseñas de forma predeterminada. Las contraseñas antiguas de cada usuario se almacenan en el archivo `/etc/securetty/passwd`.

Procedimiento

- 1 Ejecute el siguiente comando:

```
cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so
```

- 2 Asegúrese de que `enforce_for_root` aparezca en los resultados devueltos.

```
password required pam_pwhistory.so enforce_for_root remember=5 retry=3
```

Administrar la caducidad de las contraseñas

Configure la caducidad de todas las contraseñas de cuenta en conformidad con las políticas de seguridad de la organización.

De forma predeterminada, todas las cuentas del dispositivo virtual protegido de VMware definen la caducidad de contraseña en 60 días. En la mayoría de los dispositivos protegidos, la caducidad de la contraseña de la cuenta raíz es de 365 días. Se recomienda comprobar que la fecha de caducidad de todas las cuentas cumpla con los estándares de requisitos de seguridad y funcionamiento.

Si la contraseña raíz caduca, no podrá reactivarla. Debe implementar políticas específicas de sitio para evitar que las contraseñas administrativas y de usuario raíz caduquen.

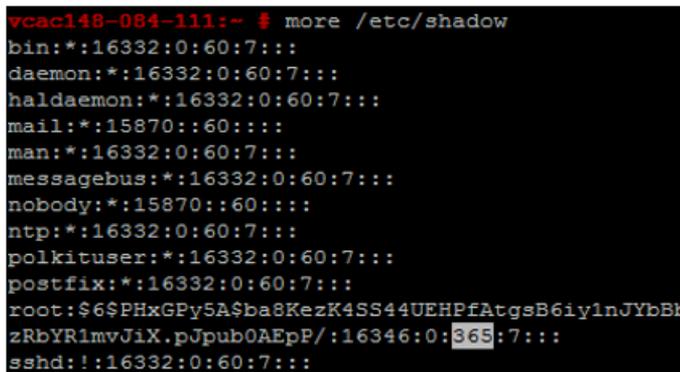
Procedimiento

- 1 Inicie sesión en las máquinas del dispositivo virtual como usuario raíz y ejecute el siguiente comando para comprobar la caducidad de contraseña en todas las cuentas.

```
# cat /etc/shadow
```

La caducidad de contraseña es el quinto campo del archivo de sombra (los campos están separados por dos puntos). La caducidad de la raíz se establece en días.

Figura 1-9. Campo de caducidad de contraseña



```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KezK4SS44UEHPfAtgsB6iy1nJYbBk
zRbYR1mvJiX.pJpub0AEpP/:16346:0:365:7:::
sshd:!:16332:0:60:7:::
```

- 2 Para modificar la caducidad de la cuenta raíz, ejecute un comando con el siguiente formato.

```
# passwd -x 365 root
```

En este comando, 365 especifica el número de días que deben transcurrir antes de que caduque la contraseña. Puede utilizar el mismo comando para modificar cualquier usuario. Tan solo debe sustituir "root" por la cuenta específica y reemplazar el número de días para cumplir con los estándares de caducidad de la organización.

Administrar Secure Shell y cuentas administrativas

Para las conexiones remotas, todos los dispositivos protegidos incluyen el protocolo Secure Shell (SSH). Utilice SSH solo cuando sea necesario y adminístrelo correctamente para mantener la seguridad del sistema.

SSH es un entorno de línea de comandos interactivo que admite conexiones remotas con los dispositivos virtuales de VMware. De forma predeterminada, el acceso a SSH requiere credenciales de cuenta de usuario con privilegios elevados. Por lo general, las actividades de SSH del usuario raíz sortean el control de acceso basado en funciones (role-based access control, RBAC) y los controles de auditoría de los dispositivos virtuales.

Se recomienda deshabilitar SSH en un entorno de producción y habilitarlo solo para solucionar los problemas que no se puedan resolver por otros medios. Manténgalo habilitado solo mientras sea necesario para un propósito específico y en conformidad con las políticas de seguridad de la organización. En el dispositivo de vRealize Automation, SSH está deshabilitado de forma predeterminada. En función de la configuración de vSphere, puede habilitar o deshabilitar SSH al implementar la plantilla de Open Virtualization Format (OVF).

Para determinar de manera sencilla si SSH está habilitado en una máquina, intente abrir una conexión mediante SSH. Si la conexión se abre y se solicitan credenciales, SSH está habilitado y disponible para las conexiones.

Cuenta de usuario raíz de Secure Shell

Debido a que los dispositivos de VMware no incluyen cuentas de usuario preconfiguradas, la cuenta raíz puede usar SSH para iniciar sesión directamente de forma predeterminada. Deshabilite SSH como usuario raíz tan pronto como sea posible.

Para cumplir con los estándares de cumplimiento de manera que no haya rechazo, el servidor SSH de todos los dispositivos protegidos está preconfigurado con la entrada de `wheel AllowGroups` para restringir el acceso SSH al `wheel` del grupo secundario. Para separar las obligaciones, puede modificar la entrada de `wheel AllowGroups` en el archivo `/etc/ssh/sshd_config` para usar otro grupo, como `sshd`.

El grupo `wheel` está habilitado con el módulo `pam_wheel` para acceso de superusuarios, de modo que los miembros de grupo `wheel` puedan usar el comando `su-root`, en el que se requiere la contraseña raíz. La separación de grupos permite a los usuarios utilizar SSH en el dispositivo, pero no el comando `su to root`. Para garantizar el correcto funcionamiento del dispositivo, no quite ni modifique otras entradas del campo `AllowGroups`. Después de realizar un cambio, debe reiniciar el daemon SSH ejecutando el comando `# service sshd restart`.

Habilitar o deshabilitar Secure Shell en los dispositivos de vRealize Automation

Habilite Secure Shell (SSH) en el dispositivo de vRealize Automation solo para solucionar problemas. Deshabilite SSH en estos componentes durante la operación normal de producción.

Puede habilitar o deshabilitar SSH en el dispositivo de vRealize Automation mediante la consola de administración de dispositivos virtuales.

Procedimiento

- 1 Desplácese hasta la consola de administración de dispositivos virtuales del dispositivo de vRealize Automation.
`: https://vRealizeAppliance url:5480`
- 2 Haga clic en la pestaña **Administración**.
- 3 Haga clic en el submenú **Administración**.
- 4 Active la casilla de verificación **Habilitar servicio SSH** para habilitar SSH o desactívela para deshabilitar SSH.
- 5 Haga clic en **Guardar configuración** para guardar los cambios.

Crear una cuenta de administrador local para Secure Shell

Como procedimiento de seguridad recomendado, cree y configure cuentas administrativas locales de Secure Shell (SSH) en las máquinas host del dispositivo virtual. Además, también se recomienda quitar el acceso SSH raíz después de crear las cuentas apropiadas.

Cree cuentas administrativas locales para SSH o miembros del grupo wheel secundario, o ambos. Antes de deshabilitar el acceso directo a la raíz, compruebe que los administradores autorizados puedan acceder a SSH usando AllowGroups y que puedan recurrir a su to root utilizando el grupo wheel.

Procedimiento

- 1 Inicie sesión en el dispositivo virtual como usuario raíz y ejecute los siguientes comandos con el nombre de usuario adecuado.

```
# useradd -g users <username> -G wheel -m -d /home/username
# passwd username
```

Wheel es el grupo especificado en AllowGroups para el acceso a SSH. Para agregar varios grupos secundarios, utilice `-G wheel,sshd`.

- 2 Cambie al usuario y proporcione una contraseña nueva para aplicar la comprobación de complejidad de contraseña.

```
# su -username
# username@hostname:~>passwd
```

Si se cumple con la complejidad de contraseña, la contraseña se actualiza. Si no se cumple con la complejidad de contraseña, se revierte a la contraseña original, y debe volver a ejecutar el comando de contraseña.

- 3 Para quitar el inicio de sesión directo en SSH, modifique el archivo `/etc/ssh/sshd_config` reemplazando `(#)PermitRootLogin yes` por `PermitRootLogin no`.

Opcionalmente, se puede habilitar o deshabilitar SSH en la interfaz de administración de dispositivos virtuales (VAMI) activando o desactivando la casilla de verificación **Inicio de sesión de SSH de administrador habilitado** en la pestaña **Administración**.

Pasos siguientes

Deshabilite los inicios de sesión directos como raíz. De forma predeterminada, los dispositivos protegidos permiten realizar el inicio de sesión directo como raíz mediante la consola. Después de crear cuentas administrativas de manera que no haya rechazo y de probarlas para el acceso de wheel de su-root, deshabilite los inicios de sesión raíz directos editando el archivo `/etc/security` como usuario raíz y reemplazando la entrada `tty1` por `console`.

- 1 Abra el archivo `/etc/security` en un editor de texto.
- 2 Busque `tty1` y reemplácelo por `console`.

3 Guarde el archivo y ciérrelo.

Proteger la configuración del servidor de Secure Shell

Siempre que sea posible, todos los dispositivos de VMware tienen una configuración de protección predeterminada. Los usuarios pueden comprobar si su configuración está protegida adecuadamente examinando la configuración del servicio del cliente y el servidor en la sección de opciones globales del archivo de configuración.

Procedimiento

1 Abra el archivo de configuración del servidor `/etc/ssh/sshd_config` en el dispositivo de VMware y compruebe que la configuración sea correcta.

| Configuración | Estado |
|---|--|
| Protocolo de daemon de servidor | Protocol 2 |
| Cifrados de CBC | aes256-ctr y aes128-ctr |
| Reenvío de TCP | AllowTCPForwarding no |
| Puertos de puerta de enlace de servidor | Gateway Ports no |
| Reenvío de X11 | X11Forwarding no |
| Servicio SSH | Utilice el campo AllowGroups y especifique un acceso de grupo permitido. Agregue los miembros adecuados a este grupo. |
| Autenticación de GSSAPI | GSSAPIAuthentication no, si no se utiliza. |
| Autenticación Kerberos | KeberosAuthentication no, si no se utiliza. |
| Variables locales (opción AcceptEnv global) | Establecido como desactivado por conversión a comentario o habilitado para las variables LC_* o LANG. |
| Configuración de túnel | PermitTunnel no |
| Sesiones de red | MaxSessions 1 |
| Conexiones simultáneas de usuario | Establecido como 1 para raíz y cualquier otro usuario. El archivo <code>/etc/security/limits.conf</code> también debe configurarse con los mismos ajustes. |
| Comprobación en modo estricto | Strict Modes yes |
| Separación de privilegios | UsePrivilegeSeparation yes |
| Autenticación RSA de rhosts | RhostsESAAuthentication no |
| Compresión | Compression delayed o Compression no |
| Código de autenticación de mensaje | MACs hmac-sha1 |
| Restricción de acceso de usuario | PermitUserEnvironment no |

2 Guarde los cambios y cierre el archivo.

Proteger la configuración del cliente de Secure Shell

Como parte del proceso de protección del sistema, compruebe la protección del cliente de SSH examinando el archivo de configuración del cliente de SSH en las máquinas host del dispositivo virtual para asegurarse de que esté configurado según las directrices de VMware.

Procedimiento

- 1 Abra el archivo de configuración del cliente de SSH, `/etc/ssh/ssh_config`, y compruebe que la configuración en la sección de opciones globales sea correcta.

| Configuración | Estado |
|--|---|
| Protocolo de cliente | Protocol 2 |
| Puertos de puerta de enlace de cliente | Gateway Ports no |
| Autenticación de GSSAPI | GSSAPIAuthentication no |
| Variables locales (opción <code>SendEnv</code> global) | Proporcionar solo las variables <code>LC_*</code> o <code>LANG</code> |
| Cifrados de CBC | Solo <code>aes256-ctr</code> y <code>aes128-ctr</code> |
| Códigos de autenticación de mensaje | Solo en la entrada <code>MACs</code> <code>hmac-sha1</code> |

- 2 Guarde los cambios y cierre el archivo.

Comprobar los permisos de archivo de claves de shell seguro

Para minimizar la posibilidad de ataques malintencionados, mantenga los permisos de archivo de claves SSH críticos en las máquinas host del dispositivo virtual.

Después de ajustar o actualizar la configuración de SSH, asegúrese de comprobar que los siguientes permisos de archivo de claves de SSH no hayan cambiado.

- Los archivos de claves de host público ubicados en `/etc/ssh/*key.pub` son propiedad del usuario raíz y tienen los permisos establecidos en `0644 (-rw-r--r--)`.
- Los archivos de claves de host privado ubicados en `/etc/ssh/*key` son propiedad del usuario raíz y tienen los permisos establecidos en `0600 (-rw-----)`.

Comprobar los permisos de archivo de clave SSH

Compruebe que se aplican permisos de SSH a los archivos de clave tanto pública como privada.

Procedimiento

- 1 Ejecute el siguiente comando para comprobar los archivos de clave pública SSH: `ls -l /etc/ssh/*key.pub`
- 2 Compruebe que el propietario es `root`, que el propietario del grupo es `root` y que los archivos tienen los permisos establecidos en `0644 (-rw-r--r--)`.
- 3 Ejecute los siguientes comandos para resolver los problemas que haya.
`chown root /etc/ssh/*key.pub`

```
chgrp root /etc/ssh/*key.pub
```

```
chmod 644 /etc/ssh/*key.pub
```

- 4 Ejecute el siguiente comando para comprobar los archivos de clave privada SSH: `ls -l /etc/ssh/*key`

- 5 Ejecute los siguientes comandos para resolver los problemas que haya.

```
chown root /etc/ssh/*key
```

```
chgrp root /etc/ssh/*key
```

```
chmod 644 /etc/ssh/*key
```

Cambiar el usuario de la interfaz de administración de dispositivos virtuales

Puede añadir y eliminar usuarios en la interfaz de administración de dispositivos virtuales para lograr el nivel de seguridad adecuado.

La cuenta de usuario raíz de la interfaz de administración de dispositivos virtuales utiliza PAM para la autenticación, por lo que también se usan los niveles de recorte establecidos por PAM. Si la interfaz de administración de dispositivos virtuales no se ha aislado correctamente, podría producirse un bloqueo de la cuenta raíz del sistema en caso de que un atacante trate de iniciar sesión mediante fuerza bruta. Además, cuando la cuenta raíz no sea suficiente para que no haya rechazo a través más de una persona de la organización, habrá que cambiar el usuario administrador de la interfaz de administración.

Requisitos previos

Procedimiento

- 1 Ejecute el siguiente comando para crear un usuario y añadirlo al grupo de interfaz de administración de dispositivos virtuales.

```
useradd -G vami,root usuario
```

- 2 Cree una contraseña para el usuario.

```
passwd usuario
```

- 3 (opcional) Ejecute el siguiente comando para deshabilitar el acceso raíz en la interfaz de administración de dispositivos virtuales.

```
usermod -R vami root
```

Nota Cuando se deshabilita el acceso raíz en la interfaz de administración de dispositivos virtuales, también se deshabilita la posibilidad de actualizar la contraseña del administrador (o raíz) en la pestaña Administración.

Configurar la autenticación del cargador de arranque

Para proporcionar un nivel de seguridad adecuado, configure la autenticación del cargador de arranque en los dispositivos virtuales de VMware.

Si el cargador de arranque del sistema no requiere autenticación, los usuarios con acceso a la consola del sistema pueden modificar la configuración de arranque del sistema o arrancar el sistema en el modo de usuario único o de mantenimiento, lo que puede provocar la denegación de servicio o el acceso no autorizado al sistema. Debido a que la autenticación del cargador de arranque no se establece de forma predeterminada en los dispositivos virtuales de VMware, debe crear una contraseña GRUB para configurarla.

Procedimiento

- 1 Para comprobar si existe una contraseña de arranque, busque la línea `password --md5 <password-hash>` en el archivo `/boot/grub/menu.lst` en los dispositivos virtuales.
- 2 Si no existe ninguna contraseña, ejecute el comando `# /usr/sbin/grub-md5-crypt` en el dispositivo virtual.

Se genera una contraseña MD5 y el comando proporciona la salida del hash md5.
- 3 Añada la contraseña al archivo `menu.lst`; para ello, ejecute el comando `# password --md5 <hash from grub-md5-crypt>`.

Configurar NTP

Para el aprovisionamiento de tiempo crítico, deshabilite la sincronización de hora del host y utilice el protocolo de tiempo de redes (Network Time Protocol, NTP) en el dispositivo de vRealize Automation.

El daemon de NTP en el dispositivo de vRealize Automation proporciona servicios de hora sincronizada. De forma predeterminada, NTP está deshabilitado, por lo que deberá configurarlo manualmente. Si es posible, utilice NTP en entornos de producción para realizar un seguimiento de las acciones del usuario y detectar posibles intrusiones y ataques malintencionados mediante la auditoría y la generación de logs precisas. Para obtener información sobre los avisos de seguridad de NTP, consulte el sitio web de NTP.

El archivo de configuración de NTP se encuentra en la carpeta `/etc/` de cada dispositivo. Puede habilitar el servicio de NTP para el dispositivo de vRealize Automation y añadir servidores horarios en la pestaña **Administración** de la interfaz de administración de dispositivos virtuales.

Procedimiento

- 1 Abra el archivo de configuración `/etc/ntp.conf` en un editor de texto de la máquina host del dispositivo virtual.
- 2 Establezca la propiedad del archivo en **root:root**.
- 3 Establezca los permisos en **0640**.
- 4 Para reducir el riesgo de un ataque de amplificación por denegación de servicio en el servicio NTP, abra el archivo `/etc/ntp.conf` y asegúrese de que las líneas de restricción aparezcan en el archivo.

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

- 5 Guarde los cambios y cierre los archivos.

Configurar TLS para datos en tránsito del dispositivo de vRealize Automation

Asegúrese de que la implementación de vRealize Automation use protocolos TLS seguros para proteger los canales de transmisión de los componentes del dispositivo de vRealize Automation.

Por motivos de rendimiento, no se habilita TLS para las conexiones de localhost entre algunos servicios de aplicación. Cuando una defensa más robusta sea una preocupación, habilite TLS en todas las comunicaciones de localhost.

Importante Al finalizar TLS en el equilibrador de carga, deshabilite protocolos no seguros (como SSLv2, SSLv3 y TLS 1.0) en todos los equilibradores de carga.

Habilitar TLS en la configuración de localhost

De manera predeterminada, algunas comunicaciones de localhost no utilizan TLS. Puede habilitar TLS en todas las conexiones de localhost para proporcionar una mayor seguridad.

Procedimiento

- 1 Conéctese con el Dispositivo de vRealize Automation mediante SSH.
- 2 Defina permisos para el almacén de claves de vCAC mediante la ejecución de los siguientes comandos.

```
usermod -A vco,coredump,pivotal vco
chown vcac.pivotal /etc/vcac/vcac.keystore
chmod 640 /etc/vcac/vcac.keystore
```

- 3 Actualice la configuración de HAProxy.
 - a Abra el archivo de configuración de HAProxy ubicado en `/etc/haproxy/conf.d` y elija el servicio `20-vcac.cfg`.
 - b Busque las líneas que contengan la siguiente cadena:

```
server local 127.0.0.1... y añada lo siguiente al final de estas líneas: ssl verify none
```

Esta sección contiene otras líneas como la siguiente:

```
backend-horizon    backend-vro
backend-vra        backend-artifactory
backend-vra-health
```

- c Cambie el puerto de `backend-horizon` de 8080 a 8443.

4 Obtenga la contraseña de keystorePass.

- a Busque la propiedad `certificate.store.password` en el archivo `/etc/vcac/security.properties`.

Por ejemplo, `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

- b Descifre el valor con el siguiente comando:

```
vcac-config prop-util -d --p VALUE
```

Por ejemplo, `vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

5 Configure el servicio de vRealize Automation.

- a Abra el archivo `/etc/vcac/server.xml`.
- b Agregue el siguiente atributo a la etiqueta `Connector`, reemplazando `certificate.store.password` con el valor de contraseña del almacén de certificados que se encuentra en `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"
keystorePass="certificate.store.password"
```

6 Configure el servicio de vRealize Orchestrator.

- a Abra el archivo `/etc/vco/app-server.xml`.
- b Agregue el siguiente atributo a la etiqueta `Connector`, reemplazando `certificate.store.password` con el valor de contraseña del almacén de certificados que se encuentra en `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"
keystorePass="certificate.store.password"
```

7 Reinicie los servicios de HAProxy, de vRealize Orchestrator y de vRealize Automation.

```
service vcac-server restart
service vco-server restart
service haproxy restart
```

Nota Si `vco-server` no se reinicia, reinicie el equipo host.

8 Configure la interfaz de administración de dispositivos virtuales.

- a Abra el archivo `/opt/vmware/share/htdocs/service/café-services/services.py`.
- b Para aumentar la seguridad, cambie la línea `conn = httpLib.HTTP()` por `conn = httpLib.HTTPS()`.

Habilitar el cumplimiento con el Estándar federal de procesamiento de información (Federal Information Processing Standard, FIPS) 140-2

El dispositivo de vRealize Automation ahora utiliza la versión de OpenSSL certificada por el FIPS 140-2 para los datos en tránsito en TLS en todo el tráfico de red entrante y saliente.

Puede habilitar o deshabilitar el modo FIPS en la interfaz de administración del dispositivo de vRealize Automation. También puede configurar el FIPS desde la línea de comandos después de iniciar sesión como raíz con los siguientes comandos:

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

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

Nota Actualmente, vRealize Automation solo habilita parcialmente el cumplimiento del estándar FIPS porque algunos componentes internos no utilizan todavía módulos criptográficos certificados. En los casos en los que todavía no se hayan implementado módulos certificados, el cifrado basado en AES-256 se utiliza en todos los algoritmos criptográficos.

Nota Con el siguiente procedimiento se reiniciará la máquina física cuando la configuración se altere.

Procedimiento

- 1 Inicie sesión como raíz en la interfaz de administración del dispositivo de vRealize Automation.
`https:// vrealize-automation-appliance-FQDN:5480`
- 2 Seleccione **Configuración de vRA > Configuración del host**.
- 3 Para habilitar o deshabilitar FIPS, haga clic en el botón que se encuentra debajo del encabezado Acciones en la parte superior derecha.
- 4 Haga clic en **Sí** para reiniciar el dispositivo de vRealize Automation.

Comprobar que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados

Como parte del proceso de protección, asegúrese de que la instancia implementada de Dispositivo de vRealize Automation utiliza canales de transmisión seguros.

Nota No se puede ejecutar la operación Unirse a un clúster después de deshabilitar TLS 1.0/1.1 y habilitar TLS 1.2

Requisitos previos

Complete el procedimiento [Habilitar TLS en la configuración de localhost](#).

Procedimiento

- 1 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados en los controladores https de HAProxy en Dispositivo de vRealize Automation.

| Revisar este archivo | Asegurarse de que lo siguiente esté presente | Asegurarse de que esté en la línea adecuada tal como se muestra |
|---------------------------------------|--|---|
| /etc/haproxy/conf.d/20-vcac.cfg | no-sslv3 no-tlsv10 no-tls11 force-tls12 | bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11 |
| /etc/haproxy/conf.d/30-vro-config.cfg | no-sslv3 no-tlsv10 no-tls11 force-tls12 | bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11 |

- 2 Reinicie el servicio.

```
service haproxy restart
```

- 3 Abra el archivo /opt/vmware/etc/lighttpd/lighttpd.conf y compruebe que aparezcan las entradas de deshabilitación correctas.

Nota No hay ninguna directiva para deshabilitar TLS 1.0 o TLS 1.1 en Lighttpd. La restricción en el uso de TLS 1.0 y TLS 1.1 puede mitigarse parcialmente aplicando OpenSSL para que no utilice los conjuntos de cifrado de TLS 1.0 y TLS 1.1.

```
ssl.use-ssl2 = "disable"  
ssl.use-ssl3 = "disable"
```

- 4 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados para el proxy de la consola en Dispositivo de vRealize Automation.
 - a Edite el archivo /etc/vcac/security.properties mediante la adición o la modificación de la siguiente línea:

```
consoleproxy.ssl.server.protocols = TLSv1.2
```
 - b Reinicie el servidor ejecutando el siguiente comando:

```
service vcac-server restart
```

5 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados para el servicio vCO.

- a Busque la etiqueta <Connector> en el archivo /etc/vco/app-server/server.xml y agregue el siguiente atributo:

```
sslEnabledProtocols = "TLSv1.2"
```

- b Ejecute el siguiente comando para reiniciar el servicio vCO.

```
service vco-server restart
```

6 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados para el servicio vRealize Automation.

- a Añada los siguientes atributos a la etiqueta <Connector> en el archivo /etc/vcac/server.xml:

```
sslEnabledProtocols = "TLSv1.2"
```

- b Ejecute el siguiente comando para reiniciar el servicio vRealize Automation:

```
service vcac-server restart
```

7 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados para RabbitMQ.

Abra el archivo /etc/rabbitmq/rabbitmq.config y compruebe que {versions, ['tlsv1.2', 'tlsv1.1']} aparezca en las secciones ssl y ssl_options.

```
[
  {ssl, [
    {versions, ['tlsv1.2', 'tlsv1.1']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]},
    {frame_max, 262144},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
      {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
      {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
      {versions, ['tlsv1.2', 'tlsv1.1']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]},
      {verify, verify_peer},
      {fail_if_no_peer_cert, false}
    ]},
    {mnesia_table_loading_timeout, 600000},
    {cluster_partition_handling, autoheal},
    {heartbeat, 600}
  ]},
  {kernel, [{net_ticktime, 120}]}
].
```

8 Reinicie el servidor de RabbitMQ.

```
# service rabbitmq-server restart
```

- 9 Compruebe que SSLv3, TLS 1.0 y TLS 1.1 estén deshabilitados para el servicio vIDM.

Abra el archivo `opt/vmware/horizon/workspace/conf/server.xml` para cada instancia del conector que contenga `SSLEnabled="true"` y asegúrese de que la siguiente línea esté presente.

```
sslEnabledProtocols="TLSv1.2"
```

Configurar conjuntos de cifrados TLS para los componentes de vRealize Automation

Para lograr la máxima seguridad, debe configurar los componentes de vRealize Automation para que utilicen cifrados seguros.

Los cifrados que se negocian entre el servidor y el navegador determinan el nivel de cifrado que se utiliza durante una sesión de TLS.

Para asegurarse de que se seleccionen solo cifrados seguros, deshabilite los cifrados no seguros en los componentes de vRealize Automation. Configure el servidor para que admita solo cifrados seguros y para que utilice tamaños de clave lo suficientemente grandes. Además, configure todos los cifrados en un orden adecuado.

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4. Asegúrese también de que el conjunto de cifrados que usa el intercambio de claves Diffie-Hellman (DHE) está deshabilitado

Deshabilitar cifrados no seguros en HAProxy

Compare los cifrados del servicio HAProxy del dispositivo de vRealize Automation con la lista cifrados aceptados y deshabilite todos los que no considere seguros.

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4.

Procedimiento

- 1 Revise la entrada de cifrados del archivo `/etc/haproxy/conf.d/20-vcac.cfg` de la directiva de enlace y deshabilite aquellos que no considere seguros.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH
+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-
tls10 no-tls11
```

- 2 Revise la entrada de cifrados del archivo `/etc/haproxy/conf.d/30-vro-config.cfg` de la directiva de enlace y deshabilite aquellos que no considere seguros.

```
bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!
eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH
no-ssl3 no-tls10 no-tls11
```

Deshabilitar cifrados no seguros del servicio de proxy de la consola del dispositivo de Dispositivo de vRealize Automation

Compare los cifrados del servicio de proxy de la consola del dispositivo de vRealize Automation con la lista cifrados aceptados y deshabilite todos los que no considere seguros.

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4.

Procedimiento

- 1 Abra el archivo `/etc/vcac/security.properties` en un editor de texto.
- 2 Agregue una línea al archivo para deshabilitar los conjuntos de cifrados no deseados.

Utilice una variación de la siguiente línea:

```
consoleproxy.ssl.ciphers.disallowed=cipher_suite_1, cipher_suite_2, etc.
```

Por ejemplo, para deshabilitar los conjuntos de claves de cifrado AES 128 y AES 256, añada la siguiente línea:

```
consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,  
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,  
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,  
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

- 3 Reinicie el servidor mediante el siguiente comando.

```
service vcac-server restart
```

Deshabilitar cifrados no seguros en el servicio vCO de Dispositivo de vRealize Automation

Compare los cifrados del servicio vCO de Dispositivo de vRealize Automation con la lista de cifrados aceptados y deshabilite todos los que se consideren no seguros.

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4.

Procedimiento

- 1 Busque la etiqueta `<Connector>` en el archivo `/etc/vco/app/server/server.xml`.

2 Edite o añada el atributo de cifrado para utilizar los conjuntos de claves cifrado deseados.

Consulte el siguiente ejemplo:

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

Deshabilitar cifrados no seguros en el servicio RabbitMQ de Dispositivo de vRealize Automation

Compare los cifrados del servicio RabbitMQ de Dispositivo de vRealize Automation con la lista de cifrados aceptados y deshabilite todos los que considere no seguros.

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4.

Procedimiento

- 1 Para analizar los conjuntos de cifrados compatibles, ejecute el comando `# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites()'`.

Los cifrados que se devuelven en el siguiente ejemplo representan solo los cifrados compatibles. El servidor de RabbitMQ no utiliza ni anuncia estos cifrados, a menos que esté configurado para hacerlo en el archivo `rabbitmq.config`.

```
["ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384",
 "ECDHE-ECDSA-AES256-SHA384", "ECDHE-RSA-AES256-SHA384",
 "ECDH-ECDSA-AES256-GCM-SHA384", "ECDH-RSA-AES256-GCM-SHA384",
 "ECDH-ECDSA-AES256-SHA384", "ECDH-RSA-AES256-SHA384",
 "DHE-RSA-AES256-GCM-SHA384", "DHE-DSS-AES256-GCM-SHA384",
 "DHE-RSA-AES256-SHA256", "DHE-DSS-AES256-SHA256", "AES256-GCM-SHA384",
 "AES256-SHA256", "ECDHE-ECDSA-AES128-GCM-SHA256",
 "ECDHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES128-SHA256",
 "ECDHE-RSA-AES128-SHA256", "ECDH-ECDSA-AES128-GCM-SHA256",
 "ECDH-RSA-AES128-GCM-SHA256", "ECDH-ECDSA-AES128-SHA256",
 "ECDH-RSA-AES128-SHA256", "DHE-RSA-AES128-GCM-SHA256",
 "DHE-DSS-AES128-GCM-SHA256", "DHE-RSA-AES128-SHA256", "DHE-DSS-AES128-SHA256",
 "AES128-GCM-SHA256", "AES128-SHA256", "ECDHE-ECDSA-AES256-SHA",
 "ECDHE-RSA-AES256-SHA", "DHE-RSA-AES256-SHA", "DHE-DSS-AES256-SHA",
 "ECDH-ECDSA-AES256-SHA", "ECDH-RSA-AES256-SHA", "AES256-SHA",
 "ECDHE-ECDSA-DES-CBC3-SHA", "ECDHE-RSA-DES-CBC3-SHA", "EDH-RSA-DES-CBC3-SHA",
 "EDH-DSS-DES-CBC3-SHA", "ECDH-ECDSA-DES-CBC3-SHA", "ECDH-RSA-DES-CBC3-SHA",
 "DES-CBC3-SHA", "ECDHE-ECDSA-AES128-SHA", "ECDHE-RSA-AES128-SHA",
 "DHE-RSA-AES128-SHA", "DHE-DSS-AES128-SHA", "ECDH-ECDSA-AES128-SHA",
 "ECDH-RSA-AES128-SHA", "AES128-SHA"]
```

- 2 Seleccione los cifrados compatibles que cumplan con los requisitos de seguridad de su organización.

Por ejemplo, para permitir solo ECDHE–ECDSA–AES128–GCM–SHA256 & ECDHE–ECDSA–AES256–GCM–SHA384, revise el archivo `/etc/rabbitmq/rabbitmq.config` y agregue la siguiente línea a `ssl` y `ssl_options`.

```
{ciphers, ["ECDHE–ECDSA–AES128–GCM–SHA256", "ECDHE–ECDSA–AES256–GCM–SHA384"]}
```

- 3 Reinicie el servidor de RabbitMQ con el siguiente comando.

```
service rabbitmq-server restart
```

Comprobar la seguridad de datos en reposo

Compruebe la seguridad de los usuarios y las cuentas de la base de datos con vRealize Automation.

Usuario de Postgres

La cuenta de usuario de Postgres Linux está vinculada a la función de cuenta de superusuario de la base de datos de Postgres, la cual es una cuenta bloqueada de forma predeterminada. Esta es la configuración más segura para este usuario, ya que solo es accesible desde la cuenta de usuario raíz. No desbloquee esta cuenta de usuario.

Funciones de cuenta de usuario de base de datos

Las funciones predeterminadas de la cuenta de usuario de Postgres no deben utilizarse al margen de la funcionalidad de la aplicación. Para poder admitir actividades de generación de informes o revisión de base de datos no predeterminadas, debe crearse una cuenta adicional que esté protegida con una contraseña apropiada.

Ejecute el siguiente script en la línea de comandos:

```
vcac-vami add-db-user newUsername newPassword
```

Esto agregará un nuevo usuario y una contraseña proporcionada por el usuario.

Nota Este script debe ejecutarse en la base de datos de Postgres principal en los casos donde existe una configuración de Postgres de HA principal-esclavo.

Configurar autenticación de cliente de PostgreSQL

Asegúrese de que la autenticación de confianza local no esté configurada en la base de datos PostgreSQL del dispositivo de vRealize Automation. Esta configuración permite que cualquier usuario local, incluido el superusuario de base de datos, se conecte como cualquier usuario de PostgreSQL sin una contraseña.

Nota La cuenta de superusuario de Postgres debe permanecer como de confianza local.

Se recomienda el método de autenticación md5, ya que envía contraseñas cifradas.

La configuración de autenticación de cliente se encuentra en el archivo `/storage/db/pgdata/pg_hba.conf`.

```
# TYPE DATABASE USER ADDRESS METHOD

# "local" is for Unix domain socket connections only
local all postgres trust
# IPv4 local connections:
#host all all 127.0.0.1/32 md5
hostssl all all 127.0.0.1/32 md5
# IPv6 local connections:
#host all all ::1/128 md5
hostssl all all ::1/128 md5

# Allow remote connections for VCAC user.
#host vcac vcac 0.0.0.0/0 md5
hostssl vcac vcac 0.0.0.0/0 md5
hostssl vcac vcac ::0/0 md5
# Allow remote connections for VCAC replication user.
#host vcac vcac_replication 0.0.0.0/0 md5
hostssl vcac vcac_replication 0.0.0.0/0 md5
hostssl vcac vcac_replication ::0/0 md5
# Allow replication connections by a user with the replication privilege.
#host replication vcac_replication 0.0.0.0/0 md5
hostssl replication vcac_replication 0.0.0.0/0 md5
hostssl replication vcac_replication ::0/0 md5
```

Si edita el archivo `pg_hba.conf`, debe reiniciar el servidor de Postgres ejecutando los siguientes comandos para que los cambios surtan efecto.

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

Configurar recursos de aplicación de vRealize Automation

Revise los recursos de aplicación de vRealize Automation y restrinja los permisos de archivo.

Procedimiento

- 1 Ejecute el siguiente comando para comprobar que los archivos con bits SUID y GUID estén definidos correctamente.

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

Debería aparecer la siguiente lista.

```
2197357 24 -rwsr-xr-x 1 polkituser root 23176 Mar 31 2015 /usr/lib/PolicyKit/polkit-
set-default-helper
2197354 16 -rwxr-sr-x 1 root polkituser 14856 Mar 31 2015 /usr/lib/PolicyKit/polkit-
read-auth-helper
2197353 12 -rwsr-x--- 1 root polkituser 10744 Mar 31 2015 /usr/lib/PolicyKit/polkit-
grant-helper-pam
2197352 20 -rwxr-sr-x 1 root polkituser 19208 Mar 31 2015 /usr/lib/PolicyKit/polkit-
```

```

grant-helper
2197351 20 -rwxr-sr-x 1 root polkituser 19008 Mar 31 2015 /usr/lib/PolicyKit/polkit-
explicit-grant-helper
2197356 24 -rwxr-sr-x 1 root polkituser 23160 Mar 31 2015 /usr/lib/PolicyKit/polkit-
revoke-helper
2188203 460 -rws--x--x 1 root root 465364 Apr 21 22:38 /usr/lib64/ssh/ssh-keysign
2138858 12 -rwxr-sr-x 1 root tty 10680 May 10 2010 /usr/sbin/utempter
2142482 144 -rwsr-xr-x 1 root root 142890 Sep 15 2015 /usr/bin/passwd
2142477 164 -rwsr-xr-x 1 root shadow 161782 Sep 15 2015 /usr/bin/chage
2142467 156 -rwsr-xr-x 1 root shadow 152850 Sep 15 2015 /usr/bin/chfn
1458298 364 -rwsr-xr-x 1 root root 365787 Jul 22 2015 /usr/bin/sudo
2142481 64 -rwsr-xr-x 1 root root 57776 Sep 15 2015 /usr/bin/newgrp
1458249 40 -rwsr-x--- 1 root trusted 40432 Mar 18 2015 /usr/bin/crontab
2142478 148 -rwsr-xr-x 1 root shadow 146459 Sep 15 2015 /usr/bin/chsh
2142480 156 -rwsr-xr-x 1 root shadow 152387 Sep 15 2015 /usr/bin/gpasswd
2142479 48 -rwsr-xr-x 1 root shadow 46967 Sep 15 2015 /usr/bin/expiry
311484 48 -rwsr-x--- 1 root messagebus 47912 Sep 16 2014 /lib64/dbus-1/dbus-daemon-
launch-helper
876574 36 -rwsr-xr-x 1 root shadow 35688 Apr 10 2014 /sbin/unix_chkpwd
876648 12 -rwsr-xr-x 1 root shadow 10736 Dec 16 2011 /sbin/unix2_chkpwd
49308 68 -rwsr-xr-x 1 root root 63376 May 27 2015 /opt/likewise/bin/ksu
1130552 40 -rwsr-xr-x 1 root root 40016 Apr 16 2015 /bin/su
1130511 40 -rwsr-xr-x 1 root root 40048 Apr 15 2011 /bin/ping
1130600 100 -rwsr-xr-x 1 root root 94808 Mar 11 2015 /bin/mount
1130601 72 -rwsr-xr-x 1 root root 69240 Mar 11 2015 /bin/umount
1130512 36 -rwsr-xr-x 1 root root 35792 Apr 15 2011 /bin/ping6
2012 /lib64/dbus-1/dbus-daemon-launch-helper

```

- 2 Ejecute el siguiente comando para comprobar que todos los archivos del dispositivo virtual tienen un propietario.

```
find / -path /proc -prune -o -nouser -o -nogroup
```

- 3 Ejecute el siguiente comando para verificar los permisos de todos los archivos en el dispositivo virtual para comprobar que ninguno de ellos puede ser modificado por cualquier usuario.

```
find / -name ".*" -type f -perm -a+w | xargs ls -ldb
```

- 4 Ejecute el siguiente comando para comprobar que solo el usuario vcac es el propietario de los archivos correctos.

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep -v -e "*/vmware-vcac/*"
```

Si se devuelve ningún resultado, todos los archivos correctos son propiedad exclusiva del usuario vcac.

- 5 Compruebe que solo el usuario vcac tenga permiso para escribir en los siguientes archivos.

```

/etc/vcac/vcac/security.properties
/etc/vcac/vcac/solution-users.properties
/etc/vcac/vcac/sso-admin.properties
/etc/vcac/vcac/vcac.keystore

```

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

Compruebe también los siguientes archivos y sus subdirectorios:

```
/var/log/vcac/*
```

```
/var/lib/vcac/*
```

```
/var/cache/vcac/*
```

- 6 Compruebe que solo el usuario raíz o el usuario vcac pueden leer los archivos correctos en los siguientes directorios y sus subdirectorios.

```
/etc/vcac/*
```

```
/var/log/vcac/*
```

```
/var/lib/vcac/*
```

```
/var/cache/vcac/*
```

- 7 Compruebe que los archivos correctos son propiedad exclusiva del usuario raíz o el usuario vco, como se muestra en los siguientes directorios y sus subdirectorios.

```
/etc/vco/*
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

- 8 Compruebe que solo el usuario raíz o el usuario vco pueden escribir en los archivos correctos, como se muestra en los siguientes directorios y sus subdirectorios.

```
/etc/vco/*
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

- 9 Compruebe que solo el usuario raíz o el usuario vco pueden leer los archivos correctos, como se muestra en los siguientes directorios y sus subdirectorios.

```
/etc/vco/*
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

Personalizar configuración de proxy de la consola

Puede personalizar la configuración de la consola remota para que vRealize Automation facilite la solución de problemas y las prácticas recomendadas organizativas.

Al instalar, configurar o mantener vRealize Automation, puede cambiar algunas opciones para habilitar la solución de problemas y la depuración de la instalación. Catalogue y audite cada uno de los cambios que realice para asegurarse de que los componentes aplicables estén protegidos correctamente según su uso requerido. No pase a la etapa de producción si no está seguro de que los cambios de configuración están protegidos correctamente.

Personalizar la caducidad de ticket de VMware Remote Console

Puede personalizar el período de validez de los tickets de consola remota que se utilizan para establecer conexiones de VMware Remote Console.

Cuando un usuario establece conexiones de VMware Remote Console, el sistema crea y devuelve una credencial única que establece una conexión específica con una máquina virtual. Puede establecer la caducidad de ticket para un período de tiempo especificado en minutos.

Procedimiento

- 1 Abra el archivo `/etc/vcac/security.properties` en un editor de texto.
- 2 Agregue una línea al archivo con el formato `consoleproxy.ticket.validitySec=30`.
En esta línea, el valor numérico especifica la cantidad de minutos que debe transcurrir antes de que caduque el ticket.
- 3 Guarde el archivo y ciérrelo.
- 4 Reinicie el servidor vCAC mediante el comando `/etc/init.d/vcac-server restart`.

El valor de caducidad de ticket se restablece en el período de tiempo especificado en minutos.

Personalizar el puerto del servidor proxy de la consola

Puede personalizar el puerto en el que el proxy de la consola VMware Remote Console escucha los mensajes.

Procedimiento

- 1 Abra el archivo `/etc/vcac/security.properties` en un editor de texto.
- 2 Agregue una línea al archivo con el formato `consoleproxy.service.port=8445`.
El valor numérico especifica el número de puerto del servicio de proxy de la consola (en este caso, 8445).
- 3 Guarde el archivo y ciérrelo.
- 4 Reinicie el servidor vCAC mediante el comando `/etc/init.d/vcac-server restart`.

El puerto del servicio de proxy cambia al número de puerto especificado.

Configurar encabezado de respuesta X-XSS-Protection

Agregue el encabezado de respuesta X-XSS-Protection al archivo de configuración de HAProxy.

Procedimiento

- 1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para editarlo.
- 2 Añada las siguientes líneas en una sección de front-end:

```
rspdel X-XSS-Protection:\ 1;\ mode=block
      rspadd X-XSS-Protection:\ 1;\ mode=block
```

- 3 Vuelva a cargar la configuración de HAProxy mediante el siguiente comando.
`/etc/init.d/haproxy reload`

Configurar encabezado de respuesta de seguridad de transporte estricto de HTTP

Agregue el encabezado de respuesta de transporte estricto de HTTP (HSTS) a la configuración de HAProxy.

Procedimiento

- 1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para editarlo.
- 2 Añada las siguientes líneas en una sección de front-end:

```
rspdel Strict-Transport-Security:\ max-age=31536000
      rspadd Strict-Transport-Security:\ max-age=31536000
```

- 3 Vuelva a cargar la configuración de HAProxy mediante el siguiente comando.
`/etc/init.d/haproxy reload`

Configurar encabezado de respuesta X-Frame-Options

El encabezado de respuesta X-Frame-Options puede aparecer dos veces en algunos casos.

El encabezado de respuesta X-Frame-Options puede aparecer dos veces debido a que el servicio de vIDM agrega este encabezado tanto al back-end como a HAProxy. Puede evitar que aparezca dos veces si se configura de forma adecuada.

Procedimiento

- 1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para editarlo.
- 2 En la sección de front-end, busque la siguiente línea:
`rspadd X-Frame-Options:\ SAMEORIGIN`
- 3 Agregue las siguientes líneas antes de la línea que ha encontrado en el paso anterior:
`rspdel X-Frame-Options:\ SAMEORIGIN`
- 4 Vuelva a cargar la configuración de HAProxy mediante el siguiente comando.
`/etc/init.d/haproxy reload`

Configurar encabezados de respuesta de servidor

Como procedimiento de seguridad recomendado, configure el sistema de vRealize Automation para limitar la información que está disponible para los posibles atacantes.

En la medida que sea posible, reduzca la cantidad de información que el sistema comparte sobre su identidad y su versión. Los piratas informáticos y los agentes malintencionados pueden utilizar esta información para realizar ataques contra su versión o su servidor web específicos.

Configurar encabezado de respuesta del servidor Lighttpd

Se recomienda crear un encabezado de servidor en blanco para el servidor Lighttpd del dispositivo de vRealize Automation.

Procedimiento

- 1 Abra el archivo `/opt/vmware/etc/lighttpd/lighttpd.conf` en un editor de texto.
- 2 Añada `server.tag = " "` al archivo.
- 3 Guarde los cambios y cierre el archivo.
- 4 Reinicie el servidor Lighttpd ejecutando el comando `# /opt/vmware/etc/init.d/vami-lighttpd restart`.

Configurar el encabezado de respuesta de TCServer para el dispositivo de vRealize Automation

Se recomienda crear un encabezado de servidor en blanco personalizado para el encabezado de respuesta de TCServer que se utiliza con el dispositivo de vRealize Automation con el fin de limitar la posibilidad de que un atacante malintencionado obtenga información valiosa.

Procedimiento

- 1 Abra el archivo `/etc/vco/app-server/server.xml` con un editor de texto.
- 2 En cada elemento `<Connector>`, agregue `server=" "`.
Por ejemplo, `<Connector protocol="HTTP/1.1" server="" />`.
- 3 Guarde los cambios y cierre el archivo.
- 4 Reinicie el servidor mediante el siguiente comando.
`service vco-server restart`

Configurar el encabezado de respuesta del servidor de Internet Information Services

Se recomienda crear un encabezado de servidor en blanco personalizado para el servidor de Internet Information Services (IIS) que se utiliza con Identity Appliance para limitar la posibilidad de que atacantes malintencionados obtengan información valiosa.

Procedimiento

- 1 Abra el archivo `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` en un editor de texto.
- 2 Busque `RemoveServerHeader=0` y cámbielo por `RemoveServerHeader=1..`

- 3 Guarde los cambios y cierre el archivo.
- 4 Reinicie el servidor ejecutando el comando `iisreset`.

Pasos siguientes

Deshabilite el encabezado "IIS X-Powered by" mediante la eliminación de los encabezados de respuesta HTTP de la lista en la consola de Administrador de IIS.

- 1 Abra la consola de Administrador de IIS.
- 2 Abra el encabezado de respuesta HTTP y quítelo de la lista.
- 3 Reinicie el servidor ejecutando el comando `iisreset`.

Establecer el tiempo de espera de sesión de Dispositivo de vRealize Automation

Configure el tiempo de espera de sesión en Dispositivo de vRealize Automation de acuerdo con la política de seguridad de la empresa.

El tiempo de espera de sesión predeterminado de Dispositivo de vRealize Automation para la inactividad del usuario es de 30 minutos. Para ajustar este valor de tiempo de espera de modo que cumpla con la política de seguridad de la organización, edite el archivo `web.xml` en la máquina host de Dispositivo de vRealize Automation.

Procedimiento

- 1 Abra el archivo `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` en un editor de texto.
- 2 Busque `session-config` y establezca el valor de tiempo de espera de sesión. Consulte el siguiente código de ejemplo.

```
<!-- 30 minutes session expiration time -->
<session-config>
  <session-timeout>30</session-timeout>
  <tracking-mode>COOKIE</tracking-mode>
  <cookie-config>
    <path>/</path>
  </cookie-config>
</session-config>
```

- 3 Reinicie el servidor ejecutando el siguiente comando.

```
service vcac-server restart
```

Administrar software no esencial

Para minimizar los riesgos de seguridad, quite o configure el software no esencial de las máquinas host de vRealize Automation.

Configure todo el software que no haya quitado en función de las recomendaciones del fabricante y los procedimientos recomendados de seguridad para minimizar las posibilidades de que genere infracciones de seguridad.

Proteger el controlador de almacenamiento USB

Proteja el controlador de almacenamiento USB para evitar que se utilice como controlador de dispositivo USB con las máquinas host del dispositivo virtual de VMware. Los posibles atacantes pueden aprovechar este controlador para poner en peligro el sistema.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea `install usb-storage /bin/true` aparezca en el archivo.
- 3 Guarde el archivo y ciérrelo.

Proteger el controlador del protocolo Bluetooth

Proteja el controlador del protocolo Bluetooth en las máquinas host del dispositivo virtual para evitar que los posibles atacantes lo aprovechen.

La vinculación del protocolo Bluetooth con la pila de red es innecesaria y puede incrementar la superficie del host expuesta a ataques.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea siguiente aparezca en el archivo.

```
install bluetooth /bin/true
```
- 3 Guarde el archivo y ciérrelo.

Proteger el protocolo Stream Control Transmission Protocol

Evite que el protocolo Stream Control Transmission Protocol (SCTP) se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovechar este protocolo para poner en peligro el sistema.

Configure el sistema para evitar que se cargue el módulo de Stream Control Transmission Protocol (SCTP), a menos que sea absolutamente necesario. SCTP es un protocolo de capa de transporte estandarizado por IETF que no se utiliza. Al vincular este protocolo con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios podrían causar que el kernel cargue un controlador de protocolo de manera dinámica abriendo un socket mediante el protocolo.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea siguiente aparezca en el archivo.

```
install sctp /bin/true
```
- 3 Guarde el archivo y ciérrelo.

Proteger protocolo de congestión de datagramas

Como parte de las actividades de protección del sistema, evite que el protocolo de congestión de datagramas (Datagram Congestion Protocol, DCCP) se cargue en las máquinas host del dispositivo virtual de forma predeterminada. Los posibles atacantes pueden aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el protocolo de control de congestión de datagramas (Datagram Congestion Control Protocol, DCCP), a menos que sea absolutamente necesario. DCCP es un protocolo de capa de transporte propuesto que no se utiliza. Al vincular este protocolo con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios pueden causar que el kernel cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que las líneas de DCCP aparezcan en el archivo.

```
install dccp/bin/true
install dccp_ipv4/bin/true
install dccp_ipv6/bin/true
```

- 3 Guarde el archivo y ciérrelo.

Proteger el puente de red

Evite que el módulo de puente de red se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovecharlo para poner en peligro el sistema.

Configure el sistema para evitar que se cargue la red, a menos que sea absolutamente necesario. Los posibles atacantes podrían aprovecharla para sortear la seguridad y las particiones de red.

Procedimiento

- 1 Ejecute el siguiente comando en todas las máquinas host del dispositivo virtual de VMware.

```
# rmmod bridge
```

- 2 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 3 Asegúrese de que la línea siguiente aparezca en el archivo.

```
install bridge /bin/false
```

- 4 Guarde el archivo y ciérrelo.

Proteger el protocolo Reliable Datagram Sockets

Como parte de las actividades de protección del sistema, evite que el protocolo Reliable Datagram Sockets (RDS) se cargue en las máquinas host del dispositivo virtual de forma predeterminada. Los posibles atacantes pueden aprovechar este protocolo para poner en peligro el sistema.

Al vincular el protocolo Reliable Datagram Sockets (RDS) con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios pueden causar que el sistema cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea `install rds /bin/true` aparezca en el archivo.
- 3 Guarde el archivo y ciérrelo.

Proteger el protocolo de comunicación transparente entre procesos

Como parte de las actividades de protección del sistema, evite que el Protocolo de comunicación transparente entre procesos (Transparent Inter-Process Communication Protocol, TIPC) se cargue en las máquinas host de dispositivo virtual de forma predeterminada. Los posibles atacantes pueden aprovechar este protocolo para poner en peligro el sistema.

Vincular el TIPC a la pila de red aumenta la superficie del host expuesta a ataques. Los procesos locales sin privilegios pueden causar que el kernel cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea `install tipc /bin/true` aparezca en el archivo.
- 3 Guarde el archivo y ciérrelo.

Proteger el protocolo Internetwork Packet Exchange

Evite que el protocolo Internetwork Packet Exchange (IPX) se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el módulo del protocolo Internetwork Packet Exchange (IPX), a menos que sea absolutamente necesario. El protocolo IPX es un protocolo de nivel de red obsoleto. Al vincular este protocolo con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios podrían causar que el sistema cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea siguiente aparezca en el archivo.

```
install ipx /bin/true
```
- 3 Guarde el archivo y ciérrelo.

Proteger el protocolo Appletalk

Evite que el protocolo Appletalk se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el módulo del protocolo Appletalk, a menos que sea absolutamente necesario. Al vincular este protocolo con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios podrían causar que el sistema cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea siguiente aparezca en el archivo.

```
install appletalk /bin/true
```
- 3 Guarde el archivo y ciérrelo.

Proteger el protocolo DECnet

Evite que el protocolo DECnet se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el módulo del protocolo DECnet, a menos que sea absolutamente necesario. Al vincular este protocolo con la pila de red, se incrementa la superficie del host expuesta a ataques. Los procesos locales sin privilegios podrían causar que el sistema cargue un controlador de protocolo de manera dinámica mediante el protocolo para abrir un socket.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` del protocolo DECnet en un editor de texto.
- 2 Asegúrese de que la línea siguiente aparezca en el archivo.

```
install decnet /bin/true
```
- 3 Guarde el archivo y ciérrelo.

Asegurar el módulo Firewire

Evite que el módulo Firewire se cargue en el sistema de forma predeterminada. Los posibles atacantes podrían aprovechar este protocolo para poner en peligro el sistema.

Evite cargar el módulo Firewire, a menos que sea absolutamente necesario.

Procedimiento

- 1 Abra el archivo `/etc/modprobe.conf.local` en un editor de texto.
- 2 Asegúrese de que la línea siguiente aparezca en el archivo.

```
install ieee1394 /bin/true
```
- 3 Guarde el archivo y ciérrelo.

Proteger el componente de infraestructura como servicio

Al proteger el sistema, ofrezca seguridad al componente de infraestructura como servicio (Infrastructure as a Service, IaaS) de vRealize Automation y su máquina host para evitar que posibles atacantes aprovechen esa vulnerabilidad.

Debe configurar la seguridad del componente de IaaS de vRealize Automation y el host en el que reside. Debe establecer o comprobar la configuración de los demás componentes y aplicaciones relacionados. En algunos casos, puede comprobar la configuración existente; en otros casos, debe cambiar o añadir ajustes para que la configuración sea adecuada.

Deshabilitar el servicio Hora de Windows

Como procedimiento de seguridad recomendado, use servidores horarios autorizados en lugar de la sincronización de hora del host en un entorno de producción de vRealize Automation.

En un entorno de producción, deshabilite la sincronización de hora del host y utilice los servidores horarios autorizados para permitir el seguimiento preciso de las acciones de usuario y la identificación de posibles intrusiones y ataques malintencionados a través de auditoría y registro.

Configurar TLS para datos en tránsito de infraestructura como servicio

Asegúrese de que la implementación de vRealize Automation use protocolos de TLS seguros para proteger los canales de transmisión de los componentes de infraestructura como servicio.

El protocolo Capa de sockets seguros (Secure Sockets Layer, SSL) y el protocolo Seguridad de la capa de transporte (Transport Layer Security, TLS) más reciente son protocolos criptográficos que permiten garantizar la seguridad del sistema durante las comunicaciones de red entre los diferentes componentes del sistema. Como SSL es un estándar más antiguo, muchos de sus implementos ya no ofrecen un nivel de protección adecuado contra posibles ataques. Se han identificado vulnerabilidades importantes en los protocolos SSL anteriores, incluidos SSLv2 y SSLv3. Estos protocolos ya no se consideran seguros.

Según las políticas de seguridad de la organización, puede que también sea recomendable deshabilitar TLS 1.0.

Nota Al finalizar TLS en el equilibrador de carga, deshabilite también los protocolos poco seguros, como SSLv2, SSLv3, así como TLS 1.0 si es necesario.

Deshabilitar SSLv3 en Internet Information Services

Como procedimiento de seguridad recomendado, deshabilite SSLv3 en Internet Information Services (IIS) en la máquina del servidor host de infraestructura como servicio (Infrastructure as a Service, IaaS).

Procedimiento

- 1 Ejecute el editor del Registro de Windows como administrador.
- 2 Desplácese hasta `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\` en la ventana del Registro.

- 3 Haga clic con el botón derecho en **Protocolos** y seleccione **Nuevo > Clave**.
- 4 Introduzca **SSL 3.0**.
- 5 En el árbol de navegación, haga clic con el botón derecho en la clave de **SSL 3.0** recientemente creada y, en el menú emergente, seleccione **Nuevo > Clave** e introduzca **Cliente**.
- 6 En el árbol de navegación, haga clic con el botón derecho en la clave de **SSL 3.0** recientemente creada y, en el menú emergente, seleccione **Nuevo > Clave** e introduzca **Servidor**.
- 7 En el árbol de navegación, en SSL 3.0, haga clic con el botón derecho en **Cliente**, seleccione **Nuevo > Valor DWORD (32 bits)** e introduzca **DisabledByDefault**.
- 8 En el árbol de navegación, en SSL 3.0, seleccione **Cliente** y, en el panel derecho, haga doble clic en **DisabledByDefault** e introduzca **1**.
- 9 En el árbol de navegación, en SSL 3.0, haga clic con el botón derecho en **Servidor**, seleccione **Nuevo > Valor DWORD (32 bits)** e introduzca **Habilitado**.
- 10 En el árbol de navegación, en SSL 3.0, seleccione **Servidor** y, en el panel derecho, haga doble clic en la instancia habilitada de **DWORD** e introduzca **0**.
- 11 Reinicie Windows Server.

Deshabilitar TLS 1.0 para IaaS

Para proporcionar máxima seguridad, configure IaaS para que utilice la limitación de peticiones y deshabilite TLS 1.0.

Para obtener más información, consulte el artículo de Microsoft Knowledge Base <https://support.microsoft.com/en-us/kb/245030>.

Procedimiento

- 1 Configure IaaS para utilizar la limitación de peticiones en lugar de sockets web.
 - a Actualice el archivo de configuración de Manager Service C:\Archivos de programa (x86)\VMware\VCAC\Server\ManagerService.exe.config agregando los siguientes valores en la sección <appSettings>.

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```
 - b Reinicie Manager Service (VMware vCloud Automation Center Service).
- 2 Compruebe que TLS 1.0 esté deshabilitado en el servidor de IaaS.
 - a Ejecute el editor del Registro como administrador.
 - b En la ventana del Registro, desplácese hasta HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\.

- c Haga clic con el botón derecho en Protocolos y seleccione **Nuevo > Clave** y, a continuación, introduzca **TLS 1.0**.
- d En el árbol de navegación, haga clic con el botón derecho en la clave de TLS 1.0 que acaba de crear y, en el menú emergente, seleccione **Nuevo > Clave** e introduzca **Cliente**.
- e En el árbol de navegación, haga clic derecho en la clave de TLS 1.0 que acaba de crear y, en el menú emergente, seleccione **Nuevo > Clave** e introduzca **Servidor**.
- f En el árbol de navegación, en TLS 1.0, haga clic con el botón derecho en **Cliente** y, a continuación, haga clic en **Nuevo > Valor DWORD (32 bits)** e introduzca **DisabledByDefault**.
- g En el árbol de navegación, en TLS 1.0, seleccione **Cliente** y en el panel derecho, haga doble clic en el DWORD **DisabledByDefault** e introduzca **1**.
- h En el árbol de navegación, TLS 1.0, haga clic con el botón derecho en **Servidor** y seleccione **Nuevo > Valor DWORD (32 bits)** e introduzca **Habilitado**.
- i En el árbol de navegación, en TLS 1.0, seleccione **Servidor** y en el panel derecho, haga doble clic en el DWORD **Habilitado** e introduzca **0**.
- j Reinicie Windows Server.

Configurar conjuntos de cifrados TLS

Para lograr la máxima seguridad, debe configurar los componentes de vRealize Automation para que utilicen cifrados seguros. Los cifrados que se negocian entre el servidor y el navegador determinan el nivel de cifrado que se utiliza durante una sesión de TLS. Para asegurarse de que se seleccionen solo cifrados seguros, deshabilite los cifrados no seguros en los componentes de vRealize Automation. Configure el servidor para que admita solo cifrados seguros y para que utilice tamaños de clave lo suficientemente grandes. Además, configure todos los cifrados en un orden adecuado.

Conjuntos de cifrados que no son aceptables

Deshabilite los conjuntos de cifrados que no ofrezcan autenticación, como los conjuntos de cifrados NULL, aNULL o eNULL. Deshabilite también el intercambio de claves Diffie-Hellman anónimo (ADH), los cifrados de nivel de exportación (EXP, cifrados que contienen DES), los tamaños de clave inferiores a 128 bits para el cifrado del tráfico de carga, el uso de MD5 como un mecanismo de hash del tráfico de carga, los conjuntos de cifrados IDEA y los conjuntos de cifrados RC4. Asegúrese también de que estén deshabilitados los conjuntos de cifrados que usen el intercambio de claves Diffie-Hellman (DHE).

Comprobar seguridad del servidor host

Como procedimiento recomendado de seguridad, compruebe la configuración de seguridad de las máquinas de servidor host de infraestructura como servicio (Infrastructure as a Service, IaaS).

Microsoft proporciona varias herramientas para ayudarle a comprobar la seguridad en las máquinas de servidor host. Para obtener instrucciones acerca del uso más adecuado de estas herramientas, póngase en contacto con su proveedor de Microsoft.

Comprobar la línea base segura del servidor host

Ejecute Microsoft Baseline Security Analyzer (MBSA) para confirmar rápidamente que el servidor tiene las actualizaciones o las correcciones más recientes. Puede usar MBSA para instalar las revisiones de seguridad de Microsoft que faltan y mantener el servidor actualizado con las recomendaciones de seguridad de Microsoft.

Descargue la versión más reciente de la herramienta MBSA del sitio web de Microsoft.

Comprobar la configuración de seguridad del servidor host

Utilice el Asistente para configuración de seguridad (Security Configuration Wizard, SCW) de Windows y el kit de herramientas de Microsoft Security Compliance Manager (SCM) para comprobar que el servidor host está configurado de forma segura.

Ejecute el SCW desde las herramientas administrativas del servidor de Windows. Esta herramienta puede identificar las funciones del servidor y las características instaladas, incluidas las redes, los firewalls de Windows y la configuración del registro. Compare el informe con las directrices de protección más recientes del SCM relevante para el servidor de Windows. En función de los resultados, puede ajustar la configuración de seguridad de cada característica (como los servicios de red, la configuración de cuenta y los firewalls de Windows) y aplicar la configuración a su servidor.

Puede encontrar más información acerca de la herramienta SCW en el sitio web de Microsoft Technet.

Proteger recursos de aplicación

Como procedimiento de seguridad recomendado, asegúrese de que todos los archivos pertinentes de infraestructura como servicio tengan los permisos correspondientes.

Revise los archivos de infraestructura como servicio en la instalación de infraestructura como servicio. En la mayoría de los casos, las subcarpetas y los archivos de cada carpeta deben tener la misma configuración que la carpeta.

| Directorio o archivo | Grupo o usuarios | Control total | Modificación | Lectura y ejecución | Lectura | Escritura |
|--|------------------|---------------|--------------|---------------------|---------|-----------|
| VMware\vCAC\Agents \<agent_name> \logs | SISTEMA | X | X | X | X | X |
| | Administrador | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| VMware\vCAC\Agents\<agent_name> \temp | SISTEMA | X | X | X | X | X |
| | Administrador | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| VMware\vCAC\Agents\ | SISTEMA | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| | Usuarios | | | X | X | |
| VMware\vCAC\Distributed Execution Manager\ | SISTEMA | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| | Usuarios | | | X | X | |

| Directorio o archivo | Grupo o usuarios | Control total | Modificación | Lectura y ejecución | Lectura | Escritura |
|---|------------------|---------------|--------------|---------------------|---------|-----------|
| VMware\vmcac\Distributed Execution Manager\DEM\Logs | SISTEMA | X | X | X | X | X |
| | Administrador | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| VMware\vmcac\Distributed Execution Manager\DEO\Logs | SISTEMA | X | X | X | X | X |
| | Administrador | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| VMware\vmcac\Management Agent\ | SISTEMA | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| | Usuarios | | | X | X | |
| VMware\vmcac\Server\ | SISTEMA | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| | Usuarios | | | X | X | |
| VMware\vmcac\Web API | SISTEMA | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| | Usuarios | | | X | X | |

Proteger la máquina host de infraestructura como servicio

Como procedimiento de seguridad recomendado, revise la configuración básica en su máquina host de infraestructura como servicio (Infrastructure as a Service, IaaS) para asegurarse de que cumpla con las directrices de seguridad.

Proteja cuentas, aplicaciones, puertos y servicios varios en la máquina host de IaaS.

Comprobar la configuración de la cuenta de usuario de servidor

Compruebe que no existan cuentas de usuario locales y de dominio, ni parámetros de configuración que no sean necesarios. Restrinja las cuentas de usuario que no estén relacionadas con las funciones de aplicación a aquellas que sean necesarias para la administración, el mantenimiento y la solución de problemas. Además, restrinja el acceso remoto de cuentas de usuario de dominio al mínimo necesario para mantener el servidor, y controle y audite estas cuentas de manera estricta.

Eliminar aplicaciones innecesarias

Elimine todas las aplicaciones innecesarias de los servidores host. Las aplicaciones innecesarias aumentan el riesgo de exposición debido a vulnerabilidades desconocidas o no revisadas.

Deshabilitar servicios y puertos innecesarios

Revise el firewall del servidor host para obtener la lista de puertos abiertos. Bloquee todos los puertos que no sean necesarios para el funcionamiento crítico del sistema o el componente de IaaS. Consulte [Configurar puertos y protocolos](#). Audite los servicios que se ejecutan en el servidor host y desactive aquellos que no sean necesarios.

Configurar la seguridad de la red del host

Para proporcionar la máxima protección frente a amenazas de seguridad conocidas, configure los ajustes de comunicación e interfaz de red en todas las máquinas host de VMware.

Como parte de un plan de seguridad integral, configure los ajustes de seguridad de la interfaz de red de los componentes de infraestructura como servicio y los dispositivos virtuales de VMware de acuerdo con las directrices de seguridad establecidas.

Configurar ajustes de red para dispositivos de VMware

Para garantizar que las máquinas host del dispositivo virtual de VMware admitan únicamente comunicaciones esenciales y seguras, revise y edite su configuración de comunicación de red.

Examine la configuración del protocolo IP de red de las máquinas host de VMware y configure los ajustes de red en función de las directrices de seguridad. Deshabilite todos los protocolos de comunicación que no sean esenciales.

Evitar el control de usuario de las interfaces de red

Como procedimiento de seguridad recomendado, conceda a los usuarios solo los privilegios de sistema que necesitan para realizar su trabajo en las máquinas host del dispositivo de VMware.

Si se permite que las cuentas de usuario con privilegios manipulen interfaces de red, es posible que se sorteen los mecanismos de seguridad de red o se deniegue el servicio. Restrinja la capacidad de los usuarios con privilegios para cambiar la configuración de interfaces de red.

Procedimiento

- 1 Ejecute el siguiente comando en cada máquina host del dispositivo de VMware.

```
# grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

- 2 Asegúrese de que cada interfaz esté establecida en NO.

Establecer el tamaño de cola de trabajo pendiente de TCP

Para proporcionar un cierto nivel de defensa contra ataques malintencionados, configure un tamaño de cola de trabajo pendiente de TCP en las máquinas host de dispositivo VMware.

Defina los tamaños de cola de trabajo pendiente de TCP en un tamaño predeterminado adecuado para mitigar los ataques de denegación de servicio de TCP. La configuración predeterminada recomendada es 1280.

Procedimiento

- 1 Ejecute el siguiente comando en cada máquina del host de dispositivo de VMware.

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```

- 2 Abra el archivo `/etc/sysctl.conf` en un editor de texto.

- 3 Establezca el tamaño predeterminado de cola de trabajo pendiente de TCP añadiendo la siguiente entrada al archivo.

```
net.ipv4.tcp_max_syn_backlog=1280
```

- 4 Guarde los cambios y cierre el archivo.

Denegar ecos de ICMPv4 a direcciones de difusión

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo de VMware omitan las solicitudes de eco de direcciones de difusión de ICMP.

Las respuestas a ecos del Protocolo de mensajes de control de Internet (Internet Control Message Protocol, ICMP) de difusión proporcionan un vector de ataque para ataques de amplificación y pueden facilitar la asignación de redes por parte de agentes malintencionados. La configuración de las máquinas host del dispositivo para que omitan los ecos de ICMPv4 protege contra este tipo de ataques.

Procedimiento

- 1 Ejecute el comando `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` en las máquinas host del dispositivo virtual de VMware para confirmar que deniegan las solicitudes de ecos de direcciones de difusión de IPv4.

Si se configuran las máquinas host para que denieguen las redirecciones de IPv4, este comando devolverá 0 para `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`.

- 2 Si desea configurar una máquina host del dispositivo virtual para que deniegue solicitudes de ecos de direcciones de difusión de ICMPv4, abra el archivo de `/etc/sysctl.conf` de las máquinas host de Windows en un editor de texto.
- 3 Busque la entrada que rece `net.ipv4.icmp_echo_ignore_broadcasts=0` . Si el valor para esta entrada no es 0 o si no existe la entrada, agréguela o actualice la entrada existente según corresponda.
- 4 Guarde los cambios y cierre el archivo.

Deshabilitar ARP de proxy de IPv4

Compruebe que el ARP de proxy de IPv4 está deshabilitado si no es necesario en las máquinas host del dispositivo de VMware para evitar el uso compartido de información sin autorización.

El ARP de proxy de IPv4 permite a un sistema enviar respuestas a solicitudes de ARP en una interfaz en nombre de los hosts conectados a otra interfaz. Deshabilite esta opción si no es necesaria para evitar que se filtre información de direccionamiento entre los segmentos de red asociados.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all"` en las máquinas host del dispositivo virtual de VMware para comprobar que el ARP de proxy de IPv4 está deshabilitado.

Si el ARP de proxy de IPv6 está deshabilitado en las máquinas host, este comando devolverá 0.

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar el ARP de proxy de IPv6 en las máquinas host, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv4.conf.default.proxy_arp=0
net.ipv4.conf.all.proxy_arp=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

Denegar mensajes de redirección de ICMP IPv4

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo virtual de VMware deniegan los mensajes de redirección de ICMP IPv4.

Los enrutadores utilizan mensajes de redirección de ICMP para indicar a los hosts que existe una ruta más directa a un destino. Un mensaje de redirección de ICMP malintencionado puede facilitar un ataque de tipo "Man in the middle". Estos mensajes modifican la tabla de rutas del host y no están autenticados. Asegúrese de que su sistema está configurado para omitirlos si no se necesitan por algún otro motivo.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all"` en las máquinas host del dispositivo de VMware para confirmar que deniegan los mensajes de redirección de IPv4.

Si las máquinas host están configuradas para denegar las redirecciones de IPv4, este comando devuelve lo siguiente:

```
/proc/sys/net/ipv4/conf/all/accept_reidrects:0
/proc/sys/net/ipv4/conf/default/accept_redirects:0
```

- 2 Si necesita configurar una máquina host del dispositivo virtual para denegar los mensajes de redirección de IPv4, abra el archivo `/etc/sysctl.conf` en un editor de texto.

- 3 Compruebe los valores de las líneas que comiencen con `net.ipv4.conf`.

Si los valores de las siguientes entradas no son 0 o si las entradas no existen, agréguelas al archivo o actualice las entradas existentes según corresponda.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

- 4 Guarde los cambios realizados y cierre el archivo.

Denegar mensajes de redirección de ICMP IPv6

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo virtual de VMware denieguen los mensajes de redirección de ICMP IPv6.

Los enrutadores utilizan mensajes de redirección de ICMP para indicar a los hosts que existe una ruta más directa a un destino. Un mensaje de redirección de ICMP malintencionado puede facilitar un ataque de tipo "Man in the middle". Estos mensajes modifican la tabla de rutas del host y no están autenticados. Asegúrese de que el sistema esté configurado para omitirlos si no se necesitan por algún otro motivo.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` en las máquinas host del dispositivo virtual de VMware para confirmar que denieguen los mensajes de redirección de IPv6.

Si las máquinas host están configuradas para denegar las redirecciones de IPv6, este comando devuelve lo siguiente:

```
/proc/sys/net/ipv6/conf/all/accept_redirects:0
/proc/sys/net/ipv6/conf/default/accept_redirects:0
```

- 2 Para configurar una máquina host del dispositivo virtual para que se denieguen mensajes de redirección de IPv4, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe los valores de las líneas que comiencen con `net.ipv6.conf`.

Si los valores de las siguientes entradas no son 0 o si las entradas no existen, agréguelas al archivo o actualice las entradas existentes según corresponda.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Guarde los cambios y cierre el archivo.

Registrar paquetes de datos con marcadores sospechosos IPv4

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo virtual de VMware registren paquetes de datos con marcadores sospechosos IPv4.

Los paquetes de datos con marcadores sospechosos contienen direcciones que el sistema sabe que no son válidas. Configure las máquinas host para registrar estos mensajes, de modo que pueda identificar configuraciones incorrectas o ataques en curso.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que registran paquetes de datos con marcadores sospechosos IPv4.

Si las máquinas virtuales están configuradas para registrar paquetes de datos con marcadores sospechosos, devuelven lo siguiente:

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/conf/default/log_martians:1
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar máquinas virtuales para que registren paquetes de datos con marcadores sospechosos IPv4, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe los valores de las líneas que comienzan con `net.ipv4.conf`.

Si el valor de las siguientes entradas no es igual a 1 o si las entradas no existen, agréguelas al archivo o actualice las entradas existentes según corresponda.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

- 4 Guarde los cambios y cierre el archivo.

Utilizar el filtrado de rutas inversas IPv4

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo virtual de VMware utilicen el filtrado de rutas inversas IPv4.

El filtrado de rutas inversas protege contra las direcciones de origen suplantado haciendo que el sistema descarte los paquetes con direcciones de origen que no tengan una ruta o que tengan una que no apunte a la interfaz de origen. Configure las máquinas host de manera que utilicen el filtrado de rutas inversas siempre que sea posible. En algunos casos, según la función del sistema, el filtrado de rutas inversas puede hacer que el sistema descarte tráfico legítimo. Si encuentra problemas como este, es posible que deba utilizar un modo más permisivo o deshabilitar por completo el filtrado de rutas inversas.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter | egrep "default|all"` en las máquinas host del dispositivo virtual de VMware para asegurarse de que utilicen el filtrado de rutas inversas IPv4.

Si las máquinas virtuales utilizan el filtrado de rutas inversas IPv4, el comando devuelve lo siguiente:

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/re_filter:1
```

Si las máquinas virtuales se configuran correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar el filtrado de rutas inversas IPv4 en las máquinas host, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe los valores de las líneas que comiencen con `net.ipv4.conf`.

Si los valores de las siguientes entradas no se establecen como 1 o si no existen, agréguelas al archivo o actualice las entradas existentes según corresponda.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

- 4 Guarde los cambios y cierre el archivo.

Denegar reenvío de IPv4

Compruebe que las máquinas host del dispositivo de VMware deniegan el reenvío de IPv4.

Si el sistema está configurado para el reenvío de IP y no es un enrutador designado, los atacantes podrían utilizarlo para sortear la seguridad de red proporcionando una ruta de acceso para comunicación no filtrada por dispositivos de red. Para evitar el riesgo, configure las máquinas host del dispositivo virtual para que denieguen el reenvío de IPv4.

Procedimiento

- 1 Ejecute el comando `# cat /proc/sys/net/ipv4/ip_forward` en las máquinas host del dispositivo de VMware para confirmar que deniegan el reenvío de IPv4.

Si las máquinas host están configuradas para denegar el reenvío de IPv4, este comando devolverá 0 para `/proc/sys/net/ipv4/ip_forward`. Si las máquinas virtuales están configuradas correctamente, no se necesita ninguna otra acción.
- 2 Si desea configurar una máquina host del dispositivo virtual para que deniegue el reenvío de IPv4, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Busque la entrada que rece `net.ipv4.ip_forward=0`. Si el valor para esta entrada no es 0 actualmente o si la entrada no existe, agréguela o actualice la entrada existente según corresponda.
- 4 Guarde todos los cambios y cierre el archivo.

Denegar el reenvío de IPv6

Como procedimiento de seguridad recomendado, compruebe que los sistemas host del dispositivo de VMware denieguen el reenvío de IPv6.

Si el sistema está configurado para el reenvío de IP y no es un enrutador designado, los atacantes podrían utilizarlo para sortear la seguridad de red proporcionando una ruta de acceso para comunicación no filtrada por dispositivos de red. Configure las máquinas host del dispositivo virtual para que denieguen el reenvío de IPv6 para no correr este riesgo.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan el reenvío de IPv6.

Si las máquinas host están configuradas para denegar el reenvío de IPv6, este comando devolverá lo siguiente:

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar una máquina host para que deniegue el reenvío de IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe los valores de las líneas que comiencen con `net.ipv6.conf`.

Si los valores de las siguientes entradas no son 0 o si las entradas no existen, agréguelas o actualice las entradas existentes según corresponda.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

Usar cookies SYN de TCP IPv4

Compruebe que las máquinas host del dispositivo VMware utilizan cookies SYN de TCP IPv4.

Un ataque "flood" SYN de TCP podría provocar una denegación de servicio al rellenar la tabla de conexiones TCP de un sistema con conexiones con el estado SYN_RCVD. Las cookies SYN impiden que se realice el seguimiento de una conexión hasta que se reciba un ACK posterior que comprueba que el iniciador está intentando una conexión válida y no es un origen "flood". Esta técnica no funciona de una manera totalmente conforme con los estándares, pero solo se activa durante una condición "flood" y permite defender el sistema mientras continúa dando servicio a las solicitudes de servicio válidas.

Procedimiento

- 1 Ejecute el comando `# cat /proc/sys/net/ipv4/tcp_syncookies` en las máquinas host del dispositivo de VMware para comprobar que utilizan cookies SYN de TCP IPv4.

Si las máquinas host se configuran para denegar el reenvío de IPv4, este comando devolverá 1 para `/proc/sys/net/ipv4/tcp_syncookies`. Si las máquinas virtuales están configuradas correctamente, no se necesita ninguna otra acción.

- 2 Si necesita configurar un dispositivo virtual para utilizar cookies SYN de TCP IPv4, abra el archivo `/etc/sysctl.conf` en un editor de texto.

- 3 Busque la entrada que rece `net.ipv4.tcp_syncookies=1`.

Si el valor para esta entrada no está establecido actualmente en 1, o bien si no existe, agregue la entrada o actualice la entrada existente según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

Denegar anuncios de enrutador IPv6

Compruebe que las máquinas host de VMware denieguen la aceptación de anuncios de enrutador y redirecciones de ICMP, a menos que sean necesarios para el funcionamiento del sistema.

IPv6 permite a los sistemas configurar sus dispositivos de red mediante el uso automático de información de la red. Desde una perspectiva de seguridad, es preferible definir manualmente la información de configuración importante a aceptarla desde la red de una forma no autenticada.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan los anuncios de enrutador.

Si las máquinas host están configuradas para denegar anuncios de enrutador IPv6, este comando devolverá 0:

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar una máquina host para que deniegue anuncios de enrutador IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

Si no existen estas entradas o sus valores no son 0, agregue las entradas o actualice las existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

Denegar solicitudes de enrutador IPv6

Como procedimiento de seguridad recomendado, compruebe que las máquinas host del dispositivo de VMware denieguen solicitudes de enrutador IPv6, a menos se requieran para el funcionamiento del sistema.

La configuración de solicitudes de enrutador determina cuántas solicitudes de enrutador se envían al acceder a la interfaz. Si las direcciones se asignan de forma estática, no es necesario enviar ninguna solicitud.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan las solicitudes de enrutador IPv6.

Si las máquinas host están configuradas para denegar anuncios de enrutador IPv6, este comando devolverá lo siguiente:

```
/proc/sys/net/ipv6/conf/all/router_solicitations:0
/proc/sys/net/ipv6/conf/default/router_solicitations:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar máquinas host para denegar solicitudes de enrutador IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde todos los cambios y cierre el archivo.

Denegar la preferencia de enrutador IPv6 en solicitudes de enrutador

Compruebe que las máquinas host del dispositivo de VMware denieguen las solicitudes de enrutador IPv6, a menos que sean necesarias para el funcionamiento del sistema.

La opción de preferencia de enrutador en las solicitudes determina las preferencias de enrutador. Si las direcciones se asignan de forma estática, no es necesario recibir ninguna preferencia de enrutador para las solicitudes.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan las solicitudes de enrutador IPv6.

Si las máquinas host están configuradas para denegar anuncios de enrutador IPv6, este comando devolverá lo siguiente:

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar las máquinas host para que denieguen solicitudes de enrutamiento de IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.

3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

4 Guarde cualquier cambio que haya realizado y cierre el archivo.

Denegar prefijos de enrutador IPv6

Compruebe que las máquinas host del dispositivo de VMware denieguen la información de prefijos de enrutador IPv6, a menos que sea necesaria para el funcionamiento del sistema.

La opción `accept_ra_pinfo` determina si el sistema acepta información de prefijos procedente del enrutador. Si las direcciones se asignan de forma estática, no es necesario recibir ninguna información de prefijos de enrutador.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan la información de prefijos de enrutador IPv6.

Si las máquinas host están configuradas para denegar anuncios de enrutador IPv6, este comando devolverá lo siguiente.

```
/proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar las máquinas host para que denieguen la información de prefijos de enrutador IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde todos los cambios y cierre el archivo.

Denegar opciones de límite de saltos de anuncio de enrutador IPv6

Compruebe que las máquinas host del dispositivo de VMware denieguen las opciones de límite de saltos de enrutador IPv6, a menos que sean necesarias.

La opción `accept_ra_defrtr` determina si el sistema aceptará las opciones de límite de saltos de un anuncio de enrutador. Si se establece como 0, evita que un enrutador cambie el límite de saltos de IPv6 predeterminado para los paquetes salientes.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan las opciones de límite de saltos de enrutador IPv6.

Si las máquinas host están configuradas para denegar las opciones de límite de saltos de enrutador IPv6, este comando devolverá 0.

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar una máquina host para que deniegue las opciones de límite de saltos de enrutador IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

Denegar opciones de configuración automática de anuncios de enrutador IPv6

Compruebe que las máquinas host del dispositivo de VMware denieguen las opciones de configuración automática de enrutador IPv6, a menos que sean necesarias.

La opción `autoconf` determina si los anuncios de enrutador pueden hacer que el sistema asigne una dirección de unidifusión global a una interfaz.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que deniegan las opciones de configuración automática de enrutador IPv6.

Si las máquinas host están configuradas para denegar las opciones de configuración automática de enrutador IPv6, este comando devolverá 0.

```
/proc/sys/net/ipv6/conf/all/autoconf:0
/proc/sys/net/ipv6/conf/default/autoconf:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar una máquina host para que deniegue las opciones de configuración automática de enrutador IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

Denegar solicitudes de vecino de IPv6

Compruebe que las máquinas host del dispositivo de VMware estén configuradas para denegar solicitudes de vecino de IPv6, a menos que sean necesarias.

La configuración de `dad_transmits` determina cuántas solicitudes de vecino se deben enviar por dirección (globales y locales de vínculo) al acceder a una interfaz para garantizar que la dirección deseada sea única en la red.

Procedimiento

- 1 Ejecute el comando `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | egrep "default|all"` en las máquinas host del dispositivo de VMware para confirmar que denieguen las solicitudes de vecino de IPv6.

Si las máquinas host están configuradas para denegar solicitudes de vecino de IPv6, este comando devolverá 0.

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar una máquina host para que deniegue solicitudes de vecino de IPv6, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

Si las entradas no existen o si sus valores no son 0, agréguelas o actualice las entradas existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

Restringir la cantidad máxima de direcciones IPv6

Compruebe las máquinas host del dispositivo de VMware para restringir la configuración de la cantidad máxima de direcciones IPv6 al valor mínimo necesario para el funcionamiento del sistema.

La configuración de la cantidad máxima de direcciones determina cuántas direcciones IPv6 de unidifusión globales están disponibles para cada interfaz. El valor predeterminado es 16, pero debe establecerlo como la cantidad exacta de direcciones globales configuradas de manera estática que sean necesarias para el sistema.

Procedimiento

- 1 Ejecute el comando `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"` en las máquinas host del dispositivo de VMware para comprobar que la cantidad máxima de direcciones IPv6 se restrinja correctamente.

Si se configuran las máquinas host para restringir la cantidad máxima de direcciones IPv6, este comando devolverá valores iguales a 1.

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

Si las máquinas host están configuradas correctamente, no se necesita ninguna acción adicional.

- 2 Si necesita configurar la cantidad máxima de direcciones IPv6 en máquinas host, abra el archivo `/etc/sysctl.conf` en un editor de texto.
- 3 Compruebe si existen las siguientes entradas.

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

Si las entradas no existen o si sus valores no se establecen como 1, añada entradas o actualice las entradas existentes según corresponda.

- 4 Guarde cualquier cambio que haya realizado y cierre el archivo.

Configurar ajustes de red para el host de infraestructura como servicio

Como procedimiento de seguridad recomendado, configure los ajustes de comunicación de red en la máquina host del componente de infraestructura como servicio (IaaS) de VMware según los requisitos y las directrices de VMware.

Configure la red de la máquina host de infraestructura como servicio (IaaS) para admitir todas las funciones de vRealize Automation con la seguridad apropiada.

Consulte [Proteger el componente de infraestructura como servicio](#).

Configurar puertos y protocolos

Como procedimiento de seguridad recomendado, configure los puertos y los protocolos de todos los dispositivos y componentes de vRealize Automation siguiendo las directrices de VMware.

Configure los puertos entrantes y salientes de los componentes de vRealize Automation según lo que se requiere para que los componentes críticos del sistema funcionen en producción. Deshabilite todos los protocolos y los puertos innecesarios. Consulte [Arquitectura de referencia de vRealize Automation](#).

Puertos de usuario necesarios

Como procedimiento de seguridad recomendado, configure los puertos de usuario de vRealize Automation según las directrices de VMware.

Exponga los puertos necesarios solo en una red segura.

| SERVIDOR | PUERTOS |
|------------------------------------|-----------|
| Dispositivo de vRealize Automation | 443, 8443 |

Puertos de administrador necesarios

Como procedimiento de seguridad recomendado, configure los puertos de administrador de vRealize Automation según las directrices de VMware.

Exponga los puertos necesarios solo en una red segura.

| SERVIDOR | PUERTOS |
|---|---------|
| Servidor de vRealize Application Services | 5480 |

Puertos de dispositivo de vRealize Automation

Como procedimiento recomendado de seguridad, configure los puertos entrantes y salientes de Dispositivo de vRealize Automation según las recomendaciones de VMware.

Puertos entrantes

Configure el número mínimo de puertos entrantes necesarios para Dispositivo de vRealize Automation. Configure puertos opcionales si son necesarios para la configuración de su sistema.

Tabla 1-4. Cantidad mínima de puertos entrantes necesaria

| PUERTO | PROTOCOLO | COMENTARIOS |
|------------|-----------|--|
| 443 | TCP | Acceso a la consola de vRealize Automation y a las llamadas de API. |
| 8443 | TCP | Proxy de la consola (VMRC). |
| 5480 | TCP | Acceso a la consola de administración web del dispositivo virtual. |
| 5488, 5489 | TCP | Interno. Utilizado por Dispositivo de vRealize Automation para las actualizaciones. |
| 5672 | TCP | Mensajes de RabbitMQ. Nota Cuando agrupa instancias de Dispositivo de vRealize Automation en clústeres, es posible que deba configurar los puertos abiertos 4369 y 25672. |
| 40002 | TCP | Necesario para el servicio de vIDM. Protegido por un firewall contra todo el tráfico externo a excepción del tráfico procedente de otros nodos de Dispositivo de vRealize Automation cuando se agrega en la configuración de HA. |

Si es necesario, configure puertos entrantes opcionales.

Tabla 1-5. Puertos entrantes opcionales

| PUERTO | PROTOCOLO | COMENTARIOS |
|--------|-----------|---|
| 22 | TCP | (Opcional) SSH. En un entorno de producción, deshabilite el servicio SSH que escucha en el puerto 22 y cierre el puerto 22. |
| 80 | TCP | (Opcional) Redirige a 443. |

Puertos salientes

Configure los puertos salientes necesarios.

Tabla 1-6. Cantidad mínima de puertos salientes

| PUERTO | PROTOCOLO | COMENTARIOS |
|------------------|-----------|---|
| 25, 587 | TCP, UDP | SMTP para enviar correos electrónicos de notificación salientes. |
| 53 | TCP, UDP | DNS. |
| 67, 68, 546, 547 | TCP, UDP | DHCP. |
| 110, 995 | TCP, UDP | POP para recibir correos electrónicos de notificación entrantes. |
| 143, 993 | TCP, UDP | IMAP para recibir correos electrónicos de notificación entrantes. |
| 443 | TCP | Manager Service de infraestructura como servicio en HTTPS. |

Si es necesario, configure puertos salientes opcionales.

Tabla 1-7. Puertos salientes opcionales

| PUERTO | PROTOCOLO | COMENTARIOS |
|--------|-----------|--|
| 80 | TCP | (Opcional) Para obtener actualizaciones de software. Puede descargar y aplicar las actualizaciones por separado. |
| 123 | TCP, UDP | (Opcional) Para conectarse directamente a NTP en lugar de usar la hora del host. |

Puertos de infraestructura como servicio

Como procedimiento de seguridad recomendado, configure los puertos entrantes y salientes de los componentes de infraestructura como servicio (Infrastructure as a Service, IaaS) según las directrices de VMware.

Puertos entrantes

Configure la cantidad mínima de puertos entrantes necesaria para los componentes de IaaS.

Tabla 1-8. Cantidad mínima de puertos entrantes necesaria

| COMPONENTE | PUERTO | PROTOCOLO | COMENTARIOS |
|-----------------|--------|-----------|---|
| Manager Service | 443 | TCP | Comunicación con los componentes de IaaS y el dispositivo de vRealize Automation en HTTPS. Todos los hosts de virtualización que administren agentes de proxy también deben tener el puerto TCP 443 abierto para el tráfico entrante. |

Puertos salientes

Configure la cantidad mínima de puertos salientes necesaria para los componentes de IaaS.

Tabla 1-9. Cantidad mínima de puertos salientes

| COMPONENTE | PUERTO | PROTOCOL O | COMENTARIOS |
|--------------------------------|--------|------------|---|
| Todo | 53 | TCP, UDP | DNS. |
| Todo | | TCP, UDP | DHCP. |
| Manager Service | 443 | TCP | Comunicación con el dispositivo de vRealize Automation en HTTPS. |
| Sitio web | 443 | TCP | Comunicación con Manager Service sobre HTTPS. |
| Distributed Execution Managers | 443 | TCP | Comunicación con Manager Service sobre HTTPS. |
| Agentes de proxy | 443 | TCP | Comunicación con Manager Service y con los hosts de virtualización sobre HTTPS. |
| Agente invitado | 443 | TCP | Comunicación con Manager Service sobre HTTPS. |
| Manager Service, sitio web | 1433 | TCP | MSSQL. |

Si es necesario, configure puertos salientes opcionales.

Tabla 1-10. Puertos salientes opcionales

| COMPONENTE | PUERTO | PROTOCOLO | COMENTARIOS |
|------------|--------|-----------|------------------|
| Todo | 123 | TCP, UDP | NTP es opcional. |

Auditoría y registro

Como procedimiento de seguridad recomendado, configure la auditoría y el registro en el sistema de vRealize Automation de acuerdo con las recomendaciones de VMware.

El registro remoto en un host de log central proporciona un almacén seguro para los archivos de log. Mediante la recopilación de archivos de log en un host central, puede supervisar el entorno con una sola herramienta. Además, puede realizar análisis agregados y buscar evidencias de amenazas, como ataques coordinados a varias entidades en la infraestructura. El inicio de sesión en un servidor de log centralizado y seguro puede ayudar a prevenir la adulteración de logs, además de proporcionar un registro de auditoría a largo plazo.

Garantizar la seguridad del servidor de registro remoto

A menudo, después de que los atacantes vulneran la seguridad de la máquina host, intentan buscar y manipular los archivos de log para borrar su rastro y mantener el control sin ser descubiertos. La protección correcta del servidor de registro remoto permite impedir que se adulteren los logs.

Utilizar un servidor NTP autorizado

Asegúrese de que todas las máquinas host usen el mismo origen de hora relativo, incluido el desfase de localización correspondiente, y que puedan relacionar el origen de hora relativo con un tiempo acordado estándar, como la hora universal coordinada (UTC). Un enfoque disciplinado en los orígenes de hora le permite realizar un seguimiento de las acciones de un intruso y relacionarlas de forma rápida al revisar los archivos de log pertinentes. Una configuración incorrecta de la hora puede dificultar la inspección y la correlación de los archivos de log a fin de detectar ataques; también puede hacer imprecisas las auditorías.

Utilice al menos tres servidores NTP de orígenes de hora externos, o bien configure algunos servidores NTP locales en una red de confianza que, a su vez, obtenga la hora de al menos tres orígenes de hora externos.

Instalar vRealize Automation

Siga las instrucciones proporcionadas para instalar una nueva instancia de vRealize Automation.

Descripción general de la instalación de vRealize Automation

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.

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 vRealize Suite Lifecycle Manager. Consulte la [documentación de vRealize Suite](#).

Novedad en esta instalación de vRealize Automation

Si instaló versiones anteriores de vRealize Automation, familiarícese con los cambios en la instalación de esta versión antes de comenzar.

- Esta versión simplifica el proceso de cambio de nombre del dispositivo de vRealize Automation. Consulte [Cambiar el nombre de host del dispositivo de vRealize Automation](#).
- En esta versión, el dispositivo de vRealize Automation utiliza TLS 1.2 de forma predeterminada. La interfaz de administración incluye una opción para habilitar temporalmente TLS 1.0 y 1.1, acción que es necesaria para actualizar los agentes existentes a esta versión.
- La interfaz de administración de dispositivos de vRealize Automation ahora incluye una página para la instalación y administración de revisiones. Consulte [Acceder a la administración de revisiones](#).
- Esta versión describe cómo cambiar el puerto de proxy predeterminado de VMware Remote Console. Consulte [Cambiar el puerto de proxy de VMware Remote Console](#).
- Esta versión repara algunos vínculos rotos de la Ayuda del Asistente de instalación.

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 Automation IaaS 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.

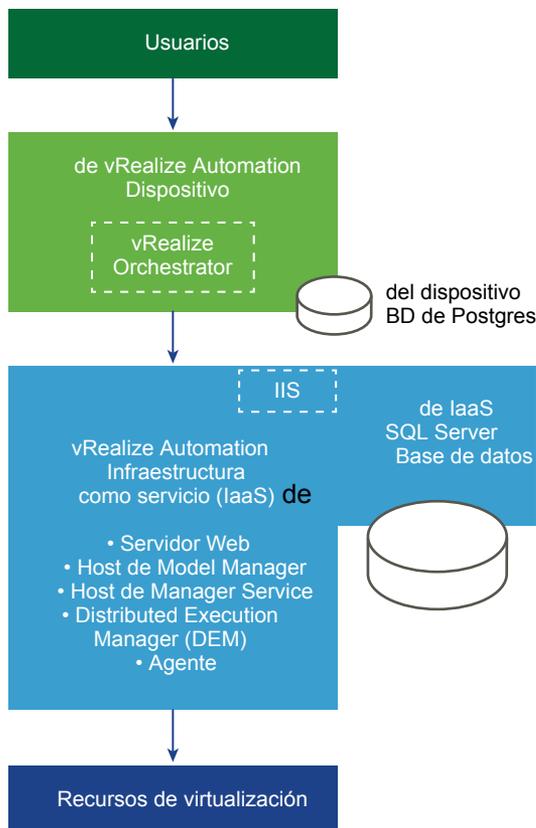
Tipo de implementación

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 1-10. Implementación mínima de vRealize Automation



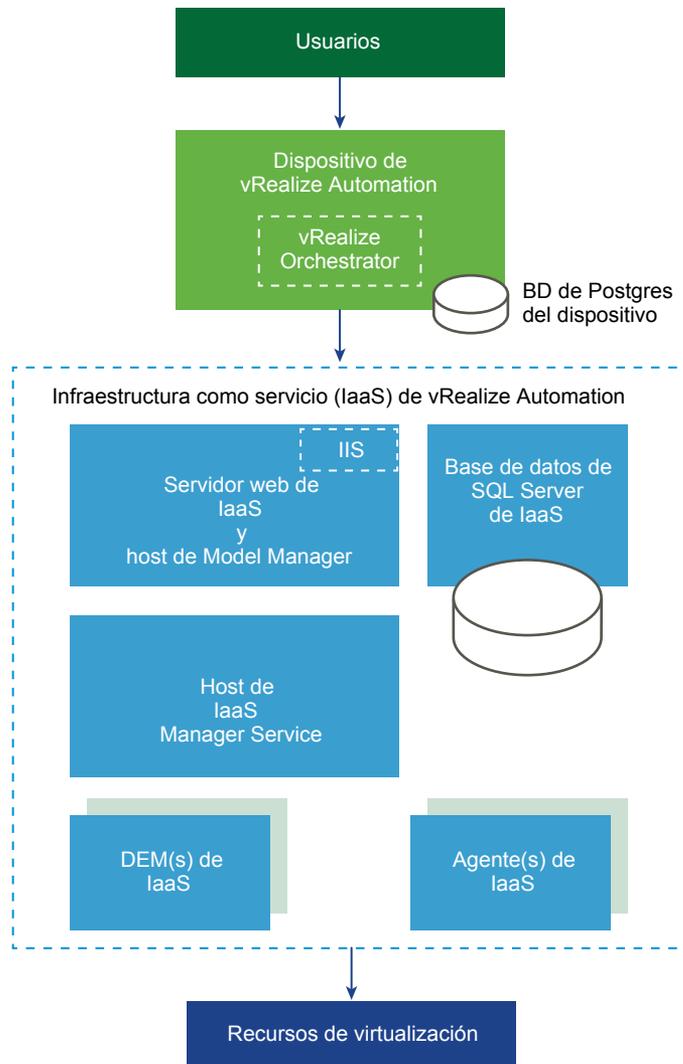
No se puede convertir una implementación mínima en una implementación empresarial. Para ampliar una implementación, comience con una implementación empresarial pequeña y añada componentes. No es posible comenzar a partir de una implementación mínima.

Nota En la documentación de vRealize Automation se incluye un completo escenario de implementación mínima de muestra que le asiste durante la instalación y le indica cómo empezar a utilizar el producto para una prueba de concepto. Consulte *Instalar y configurar vRealize Automation para el escenario de Rainpole*.

Implementaciones distribuidas de vRealize Automation

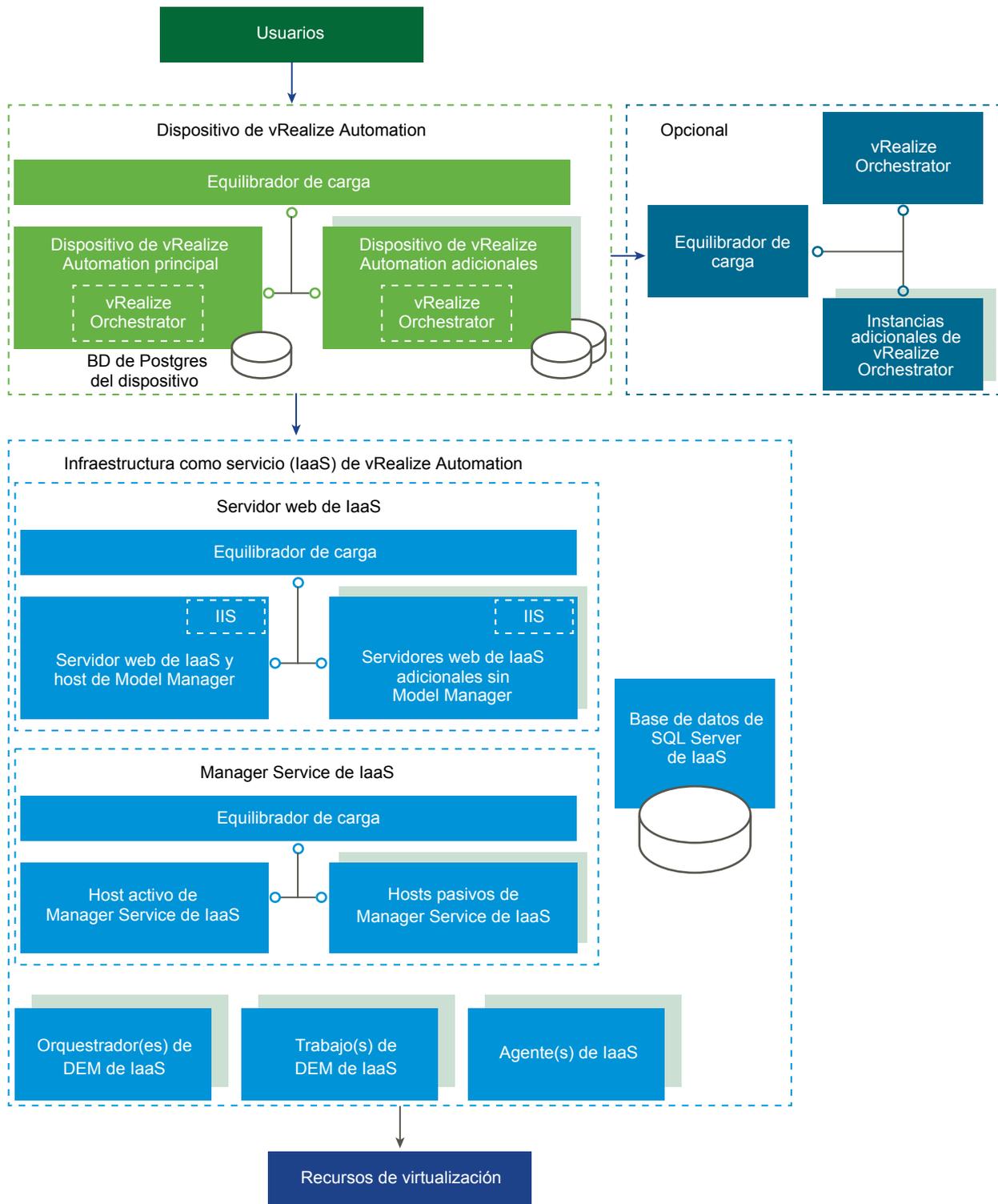
Las implementaciones empresariales distribuidas pueden tener distintos tamaños. Una implementación distribuida básica podría mejorar vRealize Automation con solo alojar los componentes de IaaS en servidores Windows independientes, como se muestra en la siguiente figura.

Figura 1-11. 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 1-12. 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

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.

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.

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.

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 1-11. 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 ■ 60 GB de almacenamiento en disco | <ul style="list-style-type: none"> ■ 4 CPU ■ 22 GB de memoria ■ 60 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 1-12. 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. 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. |
| 9300-9400 | TCP | Acceso para las auditorías de Identity Manager. |
| 54328 | UDP | |

Tabla 1-13. 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. |

Tabla 1-13. Puertos salientes (Continuación)

| Puerto | Protocolo | Comentarios |
|-----------|-----------|---|
| 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. |
| | | 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. |
| 9300-9400 | TCP | Acceso para las auditorías de Identity Manager. |
| 54328 | UDP | |

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. Ocupese de los requisitos antes de ejecutar el Asistente de instalación de vRealize Automation o el instalador estándar basado en Windows.

- 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.

- 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 2.0, 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.

- 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 lo permite la política del sitio, deshabilite los firewalls entre los servidores de Windows de IaaS y SQL Server.

Tabla 1-14. 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 |

Tabla 1-14. Puertos entrantes (Continuación)

| Puerto | Protocolo | Componente | Comentarios |
|--------|-----------|--|--|
| 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 1-15. 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. |
| 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 161 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 1-16. Internet Information Services para el host de IaaS

| 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.

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

- 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](#).
- El host de Manager Service debe poder resolver el nombre de NETBIOS del host de base de datos de SQL Server. Si no se puede resolver el nombre de NETBIOS, agregue el nombre de NETBIOS de SQL Server al archivo `/etc/hosts` de la máquina de Manager Service.

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 grupo de disponibilidad AlwaysOn (AlwaysOn Availability Group, AAG) solo es compatible con SQL Server 2016 Enterprise. Cuando se utilice AAG, especifique el FQDN del agente de escucha de AAG como el host de SQL Server.
- Si se aloja junto con los componentes de IaaS, debe configurar Java.
 - Instale la actualización 161 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 del hardware y valores máximos de capacidad de vRealize Automation](#).

- 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 1-17. 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 [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 [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 información adicional sobre la preparación de aprovisionamiento de máquinas, consulte [Preparación del entorno de SCVMM](#).

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 1-18. 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 |
| Compatible 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 |
| Compatible 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 que se usan con los dispositivos virtuales deben tener el formato de archivo PEM.

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

Tabla 1-19. Comandos y valores de certificados de ejemplo (openssl)

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

Implementar el dispositivo de vRealize Automation

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

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 1-13. 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 the status of the SSH service in 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 DHCP. 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 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-address netmask gateway-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

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 [Las interfaces estándar de instalación de vRealize Automation](#).

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 [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.

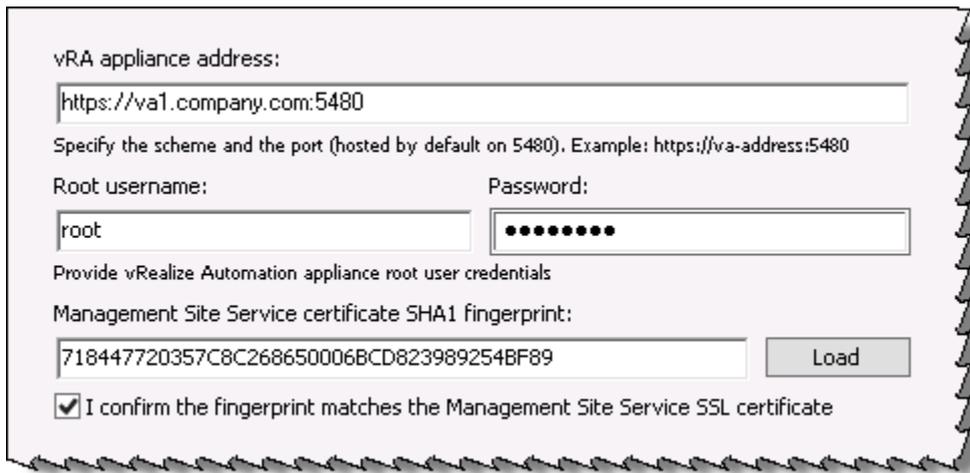
```
Archivos de programa (x86)\VMware\vCAC\Management Agent
```

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 1-14. 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.

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 [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 ver un ejemplo de cómo solicitar el elemento y completar la acción de usuario manual, consulte [Escenario: Solicitar el contenido inicial para una implementación de prueba de concepto de Rainpole](#).
- 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 [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 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 empresarial](#).

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 1-15. Agente de administración: detalles del dispositivo de vRealize Automation

vRA appliance address:
https://va1.company.com:5480
Specify the scheme and the port (hosted by default on 5480). Example: https://va-address:5480
Root username: root Password: [masked]
Provide vRealize Automation appliance root user credentials
Management Site Service certificate SHA1 fingerprint:
718447720357C8C268650006BCD823989254BF89 [Load]
 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.

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 [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 ver un ejemplo de cómo solicitar el elemento y completar la acción de usuario manual, consulte [Escenario: Solicitar el contenido inicial para una implementación de prueba de concepto de Rainpole](#).
- Para configurar el acceso al tenant predeterminado para otros usuarios, consulte [Configurar el acceso al tenant predeterminado](#).

Descripción de los pasos del asistente de instalación de vRealize Automation

El asistente de instalación de vRealize Automation le presenta unas páginas fáciles de usar en las que puede consultar los requisitos previos, especificar su configuración y validarla, así como instalar componentes de vRealize Automation.

Nota El asistente incluye pasos en los que se requiere pausar para iniciar sesión en otros sistemas, como en equilibradores de carga y servidores Windows de IaaS.

Requisitos previos

- Cree uno o más dispositivos sin configurar. Consulte [Implementar el dispositivo de vRealize Automation](#).

Las implementaciones mínimas usan un dispositivo de vRealize Automation. mientras que las implementaciones empresariales pueden tener varios dispositivos detrás del equilibrio de carga.

- Tenga uno o más sistemas de Windows disponibles en los que alojar componentes de IaaS.
- Inicie al asistente. Para ello, inicie sesión como raíz en la interfaz de administración de dispositivos de vRealize Automation.

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

Procedimiento

1 Tipo de implementación

En la página Tipo de implementación, decida qué componentes de vRealize Automation, y cuántos de cada uno, desea instalar.

2 Requisitos previos de instalación

En la página Requisitos previos de instalación, debe hacer una pausa para establecer una conexión con las máquinas Windows que alojarán a vRealize Automation IaaS. Además, debe seleccionar un origen de sincronización de hora.

3 Dispositivos de vRealize Appliance

(Solo implementaciones empresariales) En la página Dispositivos de vRealize Appliance, se ofrece la opción de crear una implementación de alta disponibilidad con varios dispositivos de vRealize Automation.

4 Funciones de servidor

(Solo implementaciones empresariales) En la página Funciones de servidor, debe asignar las funciones de los componentes IaaS de vRealize Automation a las máquinas Windows en las que haya instalado antes el agente de administración.

5 Comprobador de requisitos previos

En la página Comprobador de requisitos previos, compruebe y repare los servidores Windows de vRealize Automation para poder realizar la instalación de IaaS .

6 Host de vRealize Automation

En la página Host de vRealize Automation, debe establecer la dirección URL base para vRealize Automation. Por lo general, la dirección es el dispositivo de vRealize Automation o, en las implementaciones de alta disponibilidad, un equilibrador de carga.

7 Single Sign-On

En la página Single Sign-On, se determinan las credenciales de inicio de sesión para el administrador del sistema de tenants predeterminado de vRealize Automation.

8 Host de IaaS

En la página Host de IaaS, se establecen las direcciones URL de base para determinados componentes de IaaS. Además, se crea una frase de contraseña de seguridad para la base de datos SQL de IaaS de vRealize Automation.

9 Microsoft SQL Server

En la página Microsoft SQL Server, debe configurar la base de datos SQL de vRealize Automation IaaS. La base de datos de IaaS registra las máquinas aprovisionadas, los elementos asociados y las políticas.

10 Función web

(Solo implementaciones empresariales) En la página Función web, debe configurar por separado el sitio web de IaaS vRealize Automation en IIS.

11 Función de Manager Service

(Solo implementaciones empresariales) En la página Función de Manager Service, debe configurar la máquina Windows de vRealize Automation independiente que aloja la instancia de Función de Manager Service de IaaS.

12 [Distributed Execution Managers](#)

En la página Distributed Execution Managers, debe configurar las máquinas Windows de vRealize Automation que alojan DEM de IaaS. Se admiten varios hosts DEM.

13 [Agentes](#)

En la página Agentes, se crea la vinculación entre vRealize Automation IaaS y los recursos de virtualización en los que se implementa la infraestructura. Seleccione un tipo de agente y complete los detalles para el endpoint correspondiente.

14 [Certificado de vRealize Appliance](#)

En la página Certificado de vRealize Appliance, puede crear o seleccionar el certificado de autenticación que utiliza el dispositivo de vRealize Automation. Cuando el certificado es autofirmado, los usuarios finales pueden verlo y confirmarlo cuando inician sesión en vRealize Automation desde un navegador.

15 [Certificado web](#)

En la página Certificado web, puede crear o seleccionar el certificado de autenticación que utiliza el servidor web de IaaS. El dispositivo de vRealize Automation se conecta al servidor web, por lo que debe autenticarlo y considerarlo de confianza.

16 [Certificado de Manager Service](#)

(Solo implementaciones empresariales) En la página Certificado de Manager Service, puede crear o seleccionar el certificado de autenticación que usa el host de Manager Service de vRealize Automation IaaS. Los otros servidores Windows de IaaS se conectan al host de Manager Service, por lo que debe autenticarlo y considerarlo de confianza.

17 [Equilibradores de carga](#)

(Solo implementaciones empresariales) En la página Equilibradores de carga, tiene que hacer una pausa para configurar los equilibradores de carga del grupo correcto de los sistemas de miembros de vRealize Automation .

18 [Validación](#)

En la página Validación, compruebe que puede proceder con la instalación de vRealize Automation.

19 [Crear snapshots](#)

En la página Crear Snapshots, puede realizar una pausa para tomar snapshots de máquina virtual de todos los componentes de vRealize Automation antes de continuar con la instalación.

20 [Detalles de la instalación](#)

En la página Detalles de la instalación, inicie la instalación de vRealize Automation o vuelva a intentarlo si se produjeron problemas.

21 [Licencias](#)

En la página Licencias, introduzca una clave para activar el producto vRealize Automation instalado.

22 [Telemetría](#)

En la página Telemetría, decide si vRealize Automation debe enviar o no estadísticas de uso a VMware como parte del programa de mejora de la experiencia de cliente.

23 Opciones posteriores a la instalación

En la página Opciones posteriores a la instalación, tiene opciones para crear nuevos datos de vRealize Automation o migrar datos de implementación antiguos a la nueva instalación.

24 Configuración de contenido inicial

En la página Configuración de contenido inicial, debe crear un nuevo usuario tenant predeterminado de vRealize Automation local que puede iniciar un flujo de trabajo de contenido para un endpoint de vSphere.

25 Configuración de migración

En la página Configuración de migración, puede iniciar la transferencia de una implementación de vRealize Automation anterior a su implementación recién instalada.

Tipo de implementación

En la página Tipo de implementación, decida qué componentes de vRealize Automation, y cuántos de cada uno, desea instalar.

Mínima

En las implementaciones mínimas, se usa un solo dispositivo de vRealize Automation y un servidor de Windows para alojar a los componentes de IaaS. En las implementaciones mínimas, se puede alojar la base de datos de IaaS en un sistema SQL Server independiente o instalar SQL en la instancia de Windows Server de IaaS.

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.

Empresarial

Las implementaciones empresariales abarcan varios dispositivos independientes y hosts de Windows, por lo general, con equilibrio de carga. En las implementaciones empresariales, también se permite alojar la base de datos de IaaS en un sistema SQL Server independiente o en uno de los servidores Windows de IaaS.

Cuando se selecciona una implementación empresarial, se presentan páginas adicionales del asistente de instalación en la lista de resumen a la izquierda del asistente.

Infraestructura como servicio

La opción Infraestructura como servicio (IaaS) permite seleccionar si se deben configurar o no las máquinas Windows existentes con capacidades de modelado y aprovisionamiento de vRealize Automation.

Cuando se selecciona IaaS, se presentan páginas adicionales del asistente de instalación en la lista de resumen a la izquierda del asistente.

Requisitos previos de instalación

En la página Requisitos previos de instalación, debe hacer una pausa para establecer una conexión con las máquinas Windows que alojarán a vRealize Automation IaaS. Además, debe seleccionar un origen de sincronización de hora.

Servidores de Windows de IaaS

Para que una máquina Windows funcione como host de un componente IaaS, debe descargar e instalar `vCAC-IaaSManagementAgent-Setup.msi` en la máquina Windows.

La instalación del agente de administración requiere tener comunicación con un dispositivo de vRealize Automation en ejecución. Cada vez que se instala el agente de administración en Windows, ese sistema se vincula de forma exclusiva con el dispositivo específico y la implementación.

Los servidores Windows de IaaS potenciales que tienen instalado el agente de administración correcto se muestran en **Hosts detectados**.

Para que el asistente de instalación ignore un host detectado, haga clic en **Eliminar**. La eliminación de un host de Windows no elimina su agente de administración. Para desinstalar el agente, use la función Agregar o quitar programas directamente en Windows.

Origen de hora

Debe sincronizar cada dispositivo de vRealize Automation y cada instancia de Windows Server de IaaS con el mismo origen de hora. Se permiten los siguientes orígenes:

- Usar hora del host: se sincroniza con el host ESXi del dispositivo de vRealize Automation.
- Usar servidor horario: se sincroniza con un servidor de protocolo de tiempo de redes (Network Time Protocol, NTP) externo. Escriba el FQDN o la dirección IP del servidor NTP.

No combine orígenes de hora dentro de una implementación de vRealize Automation.

Dispositivos de vRealize Appliance

(Solo implementaciones empresariales) En la página Dispositivos de vRealize Appliance, se ofrece la opción de crear una implementación de alta disponibilidad con varios dispositivos de vRealize Automation.

Varios dispositivos deben estar alojados detrás de un equilibrador de carga que haya instalado por separado. En una página posterior del asistente, compruebe y complete la configuración de los dispositivos y el equilibrador de carga. Para cada dispositivo de vRealize Automation que añada, introduzca su FQDN y sus credenciales raíz.

Funciones de servidor

(Solo implementaciones empresariales) En la página Funciones de servidor, debe asignar las funciones de los componentes IaaS de vRealize Automation a las máquinas Windows en las que haya instalado antes el agente de administración.

Las máquinas Windows de IaaS pueden servir como servidores web principales y adicionales, hosts de Manager Service, hosts de DEM y hosts del agente. Para obtener más información sobre las funciones de los componentes de IaaS, consulte [infraestructura como servicio](#).

La separación de las funciones de servidor de IaaS solo es posible en las implementaciones empresariales. En las implementaciones mínimas, una máquina Windows realiza todas las funciones.

Comprobador de requisitos previos

En la página Comprobador de requisitos previos, compruebe y repare los servidores Windows de vRealize Automation para poder realizar la instalación de IaaS .

El Comprobador de requisitos previos inspecciona las máquinas de Windows donde ha instalado el agente de administración y alojará componentes de IaaS. Entre los requisitos previos se incluyen Java, la configuración de Internet Information Services (IIS), el servicio de Coordinador de transacciones distribuidas (DTC) de Microsoft, etc. Para obtener una lista detallada de los requisitos previos, haga clic en **Mostrar detalles**.

Con el asistente de instalación podrá continuar sin comprobar los requisitos previos, pero debe tener en cuenta que se podrían generar errores en la instalación.

- Para comprobar los requisitos previos, haga clic en **Ejecutar**.
- Si los requisitos previos no se cumplen, haga clic en **Mostrar detalles** para obtener más información; después, haga clic en **Reparar**.

El asistente de instalación puede solucionar la mayoría de requisitos previos de software o los que están basados en la configuración. Tras realizar los cambios, el asistente de instalación reinicia los hosts de IaaS.

El asistente no puede reparar problemas de recursos de CPU o de memoria insuficiente. Si se produjeran, deberá resolver esos problemas en vSphere o en su hardware.

Host de vRealize Automation

En la página Host de vRealize Automation, debe establecer la dirección URL base para vRealize Automation. Por lo general, la dirección es el dispositivo de vRealize Automation o, en las implementaciones de alta disponibilidad, un equilibrador de carga.

- Al implementar un solo dispositivo de vRealize Automation sin equilibrador de carga, introduzca el FQDN del dispositivo de vRealize Automation. Puede hacer clic para que el asistente de instalación rellene el FQDN por usted.
- Al implementar una configuración empresarial con uno o más dispositivos de vRealize Automation detrás de equilibrio de carga, introduzca el FQDN del equilibrador de carga.

Todavía es posible implementar un solo dispositivo de vRealize Automation detrás de un equilibrador de carga. Ese enfoque permite añadir dispositivos posteriores más fácilmente para expandir la implementación.

Single Sign-On

En la página Single Sign-On, se determinan las credenciales de inicio de sesión para el administrador del sistema de tenants predeterminado de vRealize Automation.

El administrador del sistema de tenants predeterminado tiene más permisos que cualquier otro usuario, incluso el permiso para crear tenants adicionales. Las credenciales para el administrador del sistema de tenants predeterminado son independientes de las credenciales raíz para el dispositivo de vRealize Automation.

Host de IaaS

En la página Host de IaaS, se establecen las direcciones URL de base para determinados componentes de IaaS. Además, se crea una frase de contraseña de seguridad para la base de datos SQL de IaaS de vRealize Automation.

Implementaciones mínimas

| Configuración | Descripción |
|---|--|
| Dirección web de IaaS | Introduzca el nombre de dominio completo del servidor Windows de IaaS. |
| Instalación de componentes de IaaS activada | Seleccione o escriba el nombre de dominio completo del servidor Windows de IaaS. |
| Username | En el formato DOMINIO\nombre de usuario, especifique la cuenta de servicio. La cuenta debe ser una cuenta de dominio con privilegios de administrador local en el servidor Windows de IaaS. |
| Password | Introduzca la contraseña de la cuenta. |
| Frase de contraseña de seguridad | <p>Cree una frase de contraseña para cifrar los datos de la base de datos SQL de IaaS.</p> <ul style="list-style-type: none"> ■ Registre la frase de contraseña, dado que la va a necesitar para restaurar la base de datos en caso de producirse algún error o para agregar componentes tras la instalación inicial. ■ La frase de contraseña no puede contener un carácter de comillas dobles ("). |
| Confirmar la frase de contraseña | Vuelva a escribir la frase de contraseña. |

Implementaciones empresariales

| Configuración | Descripción |
|------------------------------|---|
| Dirección web de IaaS | Introduzca el nombre de dominio completo del servidor web principal de IaaS. Si se dispone a implementar una configuración empresarial que incluya varios servidores web de IaaS con equilibrio de cargas, introduzca en su lugar el nombre de dominio completo del equilibrador de carga. |
| Dirección de Manager Service | Introduzca el nombre de dominio completo del host principal de Manager Service. Si se dispone a implementar una configuración empresarial que incluya varios hosts de Manager Service con equilibrio de cargas, introduzca en su lugar el nombre de dominio completo del equilibrador de carga. |

| Configuración | Descripción |
|----------------------------------|--|
| Frase de contraseña de seguridad | <p>Cree una frase de contraseña para cifrar los datos de la base de datos SQL de IaaS.</p> <ul style="list-style-type: none"> ■ Registre la frase de contraseña, dado que la va a necesitar para restaurar la base de datos en caso de producirse algún error o para agregar componentes tras la instalación inicial. ■ La frase de contraseña no puede contener un carácter de comillas dobles ("). |
| Confirmar la frase de contraseña | Vuelva a escribir la frase de contraseña. |

Microsoft SQL Server

En la página Microsoft SQL Server, debe configurar la base de datos SQL de vRealize Automation IaaS. La base de datos de IaaS registra las máquinas aprovisionadas, los elementos asociados y las políticas.

| Configuración | Descripción |
|--|---|
| Nombre del servidor | <p>Introduzca el FQDN del host de SQL Server, el cual puede ser una instancia de Windows Server de IaaS o un servidor distinto.</p> <p>Si necesita especificar un número de puerto o una instancia con nombre, utilice el formato FQDN, Port\Instance.</p> <p>Cuando utiliza el grupo de disponibilidad AlwaysOn (AlwaysOn Availability Group, AAG) de SQL, se especifica el FQDN del agente de escucha de AAG.</p> |
| Nombre de la base de datos | Acepte el valor predeterminado de vra o introduzca un nombre diferente para la base de datos de IaaS. |
| Crear base de datos nueva | <p>Permita que el asistente de instalación cree la base de datos.</p> <p>Para que esta opción funcione, la cuenta que ejecuta el agente de administración en el servidor web de IaaS principal debe tener el rol de administrador del sistema en SQL.</p> |
| Usar base de datos vacía existente | <p>No permita que el asistente de instalación cree la base de datos.</p> <p>Cuando se crea por separado la base de datos, las credenciales de usuario SQL o usuario de Windows que se proporcionan requieren el permiso dbo en la base de datos.</p> |
| Configuración predeterminada | <p>(Solo base de datos nueva) Desactive esta opción únicamente si desea utilizar una ubicación de almacenamiento alternativa para los datos y los archivos de log de IaaS.</p> <p>Después de desactivar esto, introduzca directorios para los datos (MDF) y los logs. Su cuenta de servicio de SQL Server debe tener permiso de escritura en los directorios.</p> |
| Usar SSL para la conexión con la base de datos | Cifre las conexiones a la base de datos. Para utilizar esta opción, debe configurar el host de SQL Server para SSL por separado. Además, el servidor web de IaaS y el host de Manager Service deben confiar en el certificado SSL del host de SQL Server. |

| Configuración | Descripción |
|--------------------------|---|
| Autenticación de Windows | <p>Desactive esta opción únicamente si desea utilizar la autenticación de SQL en lugar de la de Windows.</p> <p>Después de desactivar esto, introduzca las credenciales de autenticación de SQL.</p> |
| Ruta de instalación | <p>Deje esta opción desactivada para aceptar el valor predeterminado %ProgramFiles(x86)%\VMware o introduzca una ubicación alternativa.</p> <ul style="list-style-type: none"> ■ Los archivos de vRealize Automation no se instalan en el host de SQL Server. Se colocan en el servidor web de IaaS principal. ■ Si instala varios componentes de IaaS en la misma máquina Windows, instálelos todos en la misma ruta de instalación. |

Función web

(Solo implementaciones empresariales) En la página Función web, debe configurar por separado el sitio web de IaaS vRealize Automation en IIS.

En una implementación empresarial, debe especificar por separado la máquina Windows de IaaS que aloja el componente web. Para alta disponibilidad, se admiten varios hosts.

| Configuración | Descripción |
|------------------------|--|
| Nombre del sitio web | <p>Personalice el nombre o déjelo como el sitio web predeterminado de IIS.</p> <p>Evite alojar sitios web adicionales 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.</p> |
| Port | <p>Personalice los puertos o acepte el valor predeterminado de 443.</p> |
| Servidores web de IaaS | <p>Nombre del host de IaaS</p> <p>Escriba el FQDN de cada máquina Windows de IaaS que aloja el componente web de IaaS.</p> |
| | <p>Username</p> <p>En el formato DOMINIO\nombre de usuario, especifique la cuenta de servicio. La cuenta debe ser una cuenta de dominio con privilegios de administrador local en el servidor Windows de IaaS.</p> |
| | <p>Contraseña</p> <p>Introduzca la contraseña de la cuenta.</p> |
| | <p>Ruta de instalación</p> <p>Deje esta opción desactivada para aceptar el valor predeterminado %ProgramFiles(x86)%\VMware o introduzca una ubicación alternativa.</p> <p>Si instala varios componentes de IaaS en la misma máquina Windows, instálelos todos en la misma ruta de instalación.</p> |

Función de Manager Service

(Solo implementaciones empresariales) En la página Función de Manager Service, debe configurar la máquina Windows de vRealize Automation independiente que aloja la instancia de Función de Manager Service de IaaS.

En una implementación empresarial, especifique por separado el host de Manager Service, que es un servicio de Windows. Para alta disponibilidad, se admiten varios hosts.

| Configuración | Descripción |
|-------------------------|--|
| Active | <p>Seleccione el host de Manager Service principal. Todos los hosts adicionales actúan como copias de seguridad del principal.</p> <p>Cuando se realiza la instalación mediante el asistente de instalación, el servicio realiza una conmutación por error de manera transparente a una copia de seguridad si se produce un problema. Consulte Acerca de la conmutación por error automática de Manager Service.</p> |
| Nombre del host de IaaS | <p>Escriba el FQDN de cada máquina Windows de IaaS que aloja a Manager Service.</p> |
| Username | <p>En el formato DOMINIO\nombre de usuario, especifique la cuenta de servicio. La cuenta debe ser una cuenta de dominio con privilegios de administrador local en el servidor Windows de IaaS.</p> |
| Contraseña | <p>Introduzca la contraseña de la cuenta.</p> |
| Ruta de instalación | <p>Deje esta opción desactivada para aceptar el valor predeterminado %ProgramFiles(x86)%\VMware o introduzca una ubicación alternativa.</p> <p>Si instala varios componentes de IaaS en la misma máquina Windows, instálelos todos en la misma ruta de instalación.</p> |

Distributed Execution Managers

En la página Distributed Execution Managers, debe configurar las máquinas Windows de vRealize Automation que alojan DEM de IaaS. Se admiten varios hosts DEM.

| Configuración | Descripción |
|-----------------------------|---|
| Nombre del host de IaaS | <p>Introduzca el FQDN de cada máquina Windows de IaaS que aloja a un DEM.</p> |
| Nombre de instancia | <p>Introduzca un identificador único para cada DEM. Todos los nombres de DEM deben ser exclusivos, ya sea que se encuentren en el mismo host o en hosts diferentes.</p> |
| Username | <p>En el formato DOMINIO\nombre de usuario, especifique la cuenta de servicio. La cuenta debe ser una cuenta de dominio con privilegios de administrador local en el servidor Windows de IaaS.</p> |
| Password | <p>Introduzca la contraseña de la cuenta.</p> |
| Descripción de la instancia | <p>Si es necesario, introduzca una explicación de los flujos de trabajo asociados con cada DEM.</p> |
| Ruta de instalación | <p>Deje esta opción desactivada para aceptar el valor predeterminado %ProgramFiles(x86)%\VMware o introduzca una ubicación alternativa.</p> <p>Si instala varios componentes de IaaS en la misma máquina Windows, instálelos todos en la misma ruta de instalación.</p> |

Agentes

En la página Agentes, se crea la vinculación entre vRealize Automation IaaS y los recursos de virtualización en los que se implementa la infraestructura. Seleccione un tipo de agente y complete los detalles para el endpoint correspondiente.

- Se admiten varios agentes del mismo tipo o de tipos diferentes.

- Puede instalar agentes en el mismo servidor o en servidores distintos.
- Cuando están en el mismo servidor, se admiten hasta 25 agentes de cualquier tipo.
- Cuando varios agentes del mismo tipo se encuentran en el mismo servidor, cada uno debe tener un nombre exclusivo y un endpoint diferente.
- Para alta disponibilidad, puede instalar un agente con el mismo tipo, nombre y endpoint en servidores distintos.
- vSphere es normalmente uno de los tipos de agente.
- Puede añadir agentes después de la instalación.

Tipos de agente

Tabla 1-20. vSphere

| Configuración | Descripción |
|-------------------------|--|
| Tipo de agente | En el menú desplegable, seleccione vSphere. |
| Nombre del host de IaaS | En el menú desplegable, seleccione el FQDN de la máquina Windows de IaaS que aloja al agente. |
| Nombre de agente | Introduzca un identificador único, a menos que planee añadir el mismo nombre de agente y endpoint en servidores independientes para obtener alta disponibilidad. |
| Endpoint | Introduzca un nombre para el endpoint de vSphere. |
| Ruta de instalación | Deje esta opción desactivada para aceptar el valor predeterminado %ProgramFiles(x86)%\VMware o introduzca una ubicación alternativa. Si instala varios componentes de IaaS en la misma máquina Windows, instálelos todos en la misma ruta de instalación. |
| Nombre de usuario | En el formato DOMINIO\nombre de usuario, especifique la cuenta de servicio. La cuenta debe ser una cuenta de dominio con privilegios de administrador local en el servidor Windows de IaaS. |
| Contraseña | Introduzca la contraseña de la cuenta. |

Tabla 1-21. EPI PowerShell

| Configuración | Descripción |
|-------------------------|--|
| Tipo de agente | En el menú desplegable, seleccione EpiPowerShell. |
| Nombre del host de IaaS | En el menú desplegable, seleccione el FQDN de la máquina Windows de IaaS que aloja al agente. |
| Nombre de agente | Introduzca un identificador único, a menos que planee añadir el mismo nombre de agente y endpoint en servidores independientes para obtener alta disponibilidad. |
| Tipo | En el menú desplegable, seleccione la marca de aprovisionamiento que aloja el endpoint de EPI Server. |
| Servidor | Introduzca el FQDN de EPI Server. |

Tabla 1-21. EPI PowerShell (Continuación)

| Configuración | Descripción |
|---------------------|--|
| Ruta de instalación | Deje esta opción desactivada para aceptar el valor predeterminado %ProgramFiles(x86)%\VMware o introduzca una ubicación alternativa. Si instala varios componentes de IaaS en la misma máquina Windows, instálelos todos en la misma ruta de instalación. |
| Nombre de usuario | En el formato DOMINIO\nombre de usuario, especifique la cuenta de servicio. La cuenta debe ser una cuenta de dominio con privilegios de administrador local en el servidor Windows de IaaS. |
| Contraseña | Introduzca la contraseña de la cuenta. |

Tabla 1-22. HyperV

| Configuración | Descripción |
|-------------------------|--|
| Tipo de agente | En el menú desplegable, seleccione HyperV. |
| Nombre del host de IaaS | En el menú desplegable, seleccione el FQDN de la máquina Windows de IaaS que aloja al agente. |
| Nombre de agente | Introduzca un identificador único, a menos que planea añadir el mismo nombre de agente y endpoint en servidores independientes para obtener alta disponibilidad. |
| Nombre de usuario | Introduzca la cuenta de inicio de sesión en la instancia de endpoint de HyperV. |
| Contraseña | Introduzca la contraseña de la cuenta. |
| Ruta de instalación | Deje esta opción desactivada para aceptar el valor predeterminado %ProgramFiles(x86)%\VMware o introduzca una ubicación alternativa. Si instala varios componentes de IaaS en la misma máquina Windows, instálelos todos en la misma ruta de instalación. |
| Nombre de usuario | En el formato DOMINIO\nombre de usuario, especifique la cuenta de servicio. La cuenta debe ser una cuenta de dominio con privilegios de administrador local en el servidor Windows de IaaS. |
| Contraseña | Introduzca la contraseña de la cuenta. |

Tabla 1-23. VDI PowerShell

| Configuración | Descripción |
|-------------------------|--|
| Tipo de agente | En el menú desplegable, seleccione VdiPowerShell. |
| Nombre del host de IaaS | En el menú desplegable, seleccione el FQDN de la máquina Windows de IaaS que aloja al agente. |
| Nombre de agente | Introduzca un identificador único, a menos que planea añadir el mismo nombre de agente y endpoint en servidores independientes para obtener alta disponibilidad. |
| Tipo | El tipo de endpoint predeterminado es XenDesktop y no se puede cambiar. |
| Servidor | Escriba el FQDN del endpoint de XenDesktop. |
| Versión de XenDesktop | En el menú desplegable, seleccione la versión. |

Tabla 1-23. VDI PowerShell (Continuación)

| Configuración | Descripción |
|---------------------|--|
| Ruta de instalación | Deje esta opción desactivada para aceptar el valor predeterminado %ProgramFiles(x86)%\VMware o introduzca una ubicación alternativa. Si instala varios componentes de IaaS en la misma máquina Windows, instálelos todos en la misma ruta de instalación. |
| Nombre de usuario | En el formato DOMINIO\nombre de usuario, especifique la cuenta de servicio. La cuenta debe ser una cuenta de dominio con privilegios de administrador local en el servidor Windows de IaaS. |
| Contraseña | Introduzca la contraseña de la cuenta. |

Tabla 1-24. Xen

| Configuración | Descripción |
|-------------------------|--|
| Tipo de agente | En el menú desplegable, seleccione Xen. |
| Nombre del host de IaaS | En el menú desplegable, seleccione el FQDN de la máquina Windows de IaaS que aloja al agente. |
| Nombre de agente | Introduzca un identificador único, a menos que planea añadir el mismo nombre de agente y endpoint en servidores independientes para obtener alta disponibilidad. |
| Nombre de usuario | Introduzca la cuenta de inicio de sesión en la instancia de endpoint de Xen. |
| Contraseña | Introduzca la contraseña de la cuenta. |
| Ruta de instalación | Deje esta opción desactivada para aceptar el valor predeterminado %ProgramFiles(x86)%\VMware o introduzca una ubicación alternativa. Si instala varios componentes de IaaS en la misma máquina Windows, instálelos todos en la misma ruta de instalación. |
| Nombre de usuario | En el formato DOMINIO\nombre de usuario, especifique la cuenta de servicio. La cuenta debe ser una cuenta de dominio con privilegios de administrador local en el servidor Windows de IaaS. |
| Contraseña | Introduzca la contraseña de la cuenta. |

Tabla 1-25. WMI

| Configuración | Descripción |
|-------------------------|--|
| Tipo de agente | En el menú desplegable, seleccione WMI. |
| Nombre del host de IaaS | En el menú desplegable, seleccione el FQDN de la máquina Windows de IaaS que aloja al agente. |
| Nombre de agente | Introduzca un identificador único, a menos que planea añadir el mismo nombre de agente y endpoint en servidores independientes para obtener alta disponibilidad. |
| Ruta de instalación | Deje esta opción desactivada para aceptar el valor predeterminado %ProgramFiles(x86)%\VMware o introduzca una ubicación alternativa. Si instala varios componentes de IaaS en la misma máquina Windows, instálelos todos en la misma ruta de instalación. |

Tabla 1-25. WMI (Continuación)

| Configuración | Descripción |
|-------------------|---|
| Nombre de usuario | En el formato DOMINIO\nombre de usuario, especifique la cuenta de servicio. La cuenta debe ser una cuenta de dominio con privilegios de administrador local en el servidor Windows de IaaS. |
| Contraseña | Introduzca la contraseña de la cuenta. |

Tabla 1-26. Probar

| Configuración | Descripción |
|-------------------------|--|
| Tipo de agente | En el menú desplegable, seleccione Prueba. |
| Nombre del host de IaaS | En el menú desplegable, seleccione el FQDN de la máquina Windows de IaaS que aloja al agente. |
| Nombre de agente | Introduzca un identificador único, a menos que planee añadir el mismo nombre de agente y endpoint en servidores independientes para obtener alta disponibilidad. |
| Ruta de instalación | Deje esta opción desactivada para aceptar el valor predeterminado %ProgramFiles(x86)%\VMware o introduzca una ubicación alternativa. Si instala varios componentes de IaaS en la misma máquina Windows, instálelos todos en la misma ruta de instalación. |
| Nombre de usuario | En el formato DOMINIO\nombre de usuario, especifique la cuenta de servicio. La cuenta debe ser una cuenta de dominio con privilegios de administrador local en el servidor Windows de IaaS. |
| Contraseña | Introduzca la contraseña de la cuenta. |

Certificado de vRealize Appliance

En la página Certificado de vRealize Appliance, puede crear o seleccionar el certificado de autenticación que utiliza el dispositivo de vRealize Automation. Cuando el certificado es autofirmado, los usuarios finales pueden verlo y confirmarlo cuando inician sesión en vRealize Automation desde un navegador.

| Configuración | Descripción | |
|-----------------------|----------------------------|--|
| Acción de certificado | Mantener existente | Utilice el certificado ya guardado en este dispositivo de vRealize Automation. Compruebe los detalles de las entradas a continuación, como el número de serie y la huella digital. |
| | Generar certificado | Use el asistente para generar un certificado autofirmado de dispositivo de vRealize Automation. |
| | Generar solicitud de firma | Cree un archivo de solicitud de firma del certificado (CSR) para la entidad de certificación (CA). Una CSR ayuda a la entidad de certificación a crear un certificado con los valores correctos para importarlo. <ol style="list-style-type: none"> 1 Introduzca la organización, la unidad organizativa y el código de país (vea abajo). 2 Haga clic en Generar solicitud de firma. 3 Para descargar el archivo CSR para la entidad de certificación, haga clic en el vínculo que se muestra. |

| Configuración | | Descripción |
|---------------------|----------|---|
| | Importar | <p>Identifique un archivo de certificado en formato PEM, haga que el asistente lo añada al almacén correcto y cárguelo para que lo use vRealize Automation.</p> <p>A menos que desee importar un certificado creado a partir de una CSR, esta opción requiere que se especifique la clave privada del certificado, la frase de contraseña de clave privada (si existe una) y la cadena de certificados.</p> <p>Al importar un PEM proporcionado por una entidad de certificación que se creó a partir de una CSR, deje la clave privada y la frase de contraseña en blanco.</p> |
| Nombre común | | <p>El FQDN del dispositivo de vRealize Automation.</p> <p>En las implementaciones empresariales de alta disponibilidad con un equilibrador de carga delante de varios dispositivos, esta entrada es el FQDN del equilibrador de carga.</p> |
| Organización | | Introduzca texto para representar el departamento o la unidad de negocio más grande. |
| Unidad organizativa | | Introduzca texto para representar el departamento o el grupo de trabajo más pequeño. |
| Código de país | | Introduzca una abreviatura para el país de operación. |
| Serie | | Identificador alfanumérico único |
| Huella digital | | Cadena alfanumérica única que se utiliza para identificar un certificado o comparar uno con otro |
| Válido desde | | Marca de hora después de la cual se puede utilizar el certificado |
| Válido hasta | | Marca de hora después de la cual ya no se puede utilizar el certificado |

Certificado web

En la página Certificado web, puede crear o seleccionar el certificado de autenticación que utiliza el servidor web de IaaS. El dispositivo de vRealize Automation se conecta al servidor web, por lo que debe autenticarlo y considerarlo de confianza.

| Configuración | | Descripción |
|-----------------------|---------------------|--|
| Acción de certificado | Mantener existente | Utilice el certificado ya guardado en este servidor web de IaaS. Compruebe los detalles de las entradas a continuación, como el número de serie y la huella digital. |
| | Generar certificado | Use el asistente para generar un certificado autofirmado de servidor web de IaaS. |

| Configuración | Descripción |
|--|---|
| Generar solicitud de firma | <p>Cree un archivo de solicitud de firma del certificado (CSR) para la entidad de certificación (CA). Una CSR ayuda a la entidad de certificación a crear un certificado con los valores correctos para importarlo.</p> <ol style="list-style-type: none"> 1 Introduzca la organización, la unidad organizativa y el código de país (vea abajo). 2 Haga clic en Generar solicitud de firma. 3 Para descargar el archivo CSR para la entidad de certificación, haga clic en el vínculo que se muestra. |
| Importar | <p>Identifique un archivo de certificado en formato PEM, haga que el asistente lo añada al almacén correcto y cárguelo para que lo use vRealize Automation.</p> <p>A menos que desee importar un certificado creado a partir de una CSR, esta opción requiere que se especifique la clave privada del certificado, la frase de contraseña de clave privada (si existe una) y la cadena de certificados.</p> <p>Al importar un PEM proporcionado por una entidad de certificación que se creó a partir de una CSR, deje la clave privada y la frase de contraseña en blanco.</p> |
| Proporcionar huella digital de certificado | Cargue un certificado ya añadido al almacén correcto. |
| Nombre común | <p>El FQDN del servidor web de IaaS.</p> <p>En las implementaciones empresariales de alta disponibilidad con un equilibrador de carga delante de varios servidores web, esta entrada es el FQDN del equilibrador de carga.</p> |
| Organización | Introduzca texto para representar el departamento o la unidad de negocio más grande. |
| Unidad organizativa | Introduzca texto para representar el departamento o el grupo de trabajo más pequeño. |
| Código de país | Introduzca una abreviatura para el país de operación. |
| Serie | Identificador alfanumérico único |
| Huella digital | Cadena alfanumérica única que se utiliza para identificar un certificado o comparar uno con otro |
| Válido desde | Marca de hora después de la cual se puede utilizar el certificado |
| Válido hasta | Marca de hora después de la cual ya no se puede utilizar el certificado |

Certificado de Manager Service

(Solo implementaciones empresariales) En la página Certificado de Manager Service, puede crear o seleccionar el certificado de autenticación que usa el host de Manager Service de vRealize Automation IaaS. Los otros servidores Windows de IaaS se conectan al host de Manager Service, por lo que debe autenticarlo y considerarlo de confianza.

Esta página solo se muestra cuando Manager Service se aloja en una máquina separada del servidor web de IaaS. Cuando se alojan en la misma máquina, el certificado web proporciona autenticación para ambas funciones.

| Configuración | | Descripción |
|-----------------------|---|---|
| Acción de certificado | Mantener existente | Utilice el certificado ya guardado en este host de Manager Service de IaaS. Compruebe los detalles de las entradas a continuación, como el número de serie y la huella digital. |
| | Generar certificado | Use el asistente para generar un certificado autofirmado de host de Manager Service de IaaS. |
| | Generar solicitud de firma | <p>Cree un archivo de solicitud de firma del certificado (CSR) para la entidad de certificación (CA). Una CSR ayuda a la entidad de certificación a crear un certificado con los valores correctos para importarlo.</p> <ol style="list-style-type: none"> 1 Introduzca la organización, la unidad organizativa y el código de país (vea abajo). 2 Haga clic en Generar solicitud de firma. 3 Para descargar el archivo CSR para la entidad de certificación, haga clic en el vínculo que se muestra. |
| | Importar | <p>Identifique un archivo de certificado en formato PEM, haga que el asistente lo añada al almacén correcto y cárguelo para que lo use vRealize Automation.</p> <p>A menos que desee importar un certificado creado a partir de una CSR, esta opción requiere que se especifique la clave privada del certificado, la frase de contraseña de clave privada (si existe una) y la cadena de certificados.</p> <p>Al importar un PEM proporcionado por una entidad de certificación que se creó a partir de una CSR, deje la clave privada y la frase de contraseña en blanco.</p> |
| | Proporcionar huella digital de certificado | Cargue un certificado ya añadido al almacén correcto. |
| Nombre común | <p>El FQDN para el host de Manager Service de IaaS.</p> <p>En las implementaciones empresariales de alta disponibilidad con un equilibrador de carga delante de varios hosts de Manager Service, esta entrada es el FQDN del equilibrador de carga.</p> | |
| Organización | Introduzca texto para representar el departamento o la unidad de negocio más grande. | |
| Unidad organizativa | Introduzca texto para representar el departamento o el grupo de trabajo más pequeño. | |
| Código de país | Introduzca una abreviatura para el país de operación. | |
| Serie | Identificador alfanumérico único | |
| Huella digital | Cadena alfanumérica única que se utiliza para identificar un certificado o comparar uno con otro | |

| Configuración | Descripción |
|---------------|---|
| Válido desde | Marca de hora después de la cual se puede utilizar el certificado |
| Válido hasta | Marca de hora después de la cual ya no se puede utilizar el certificado |

Equilibradores de carga

(Solo implementaciones empresariales) En la página Equilibradores de carga, tiene que hacer una pausa para configurar los equilibradores de carga del grupo correcto de los sistemas de miembros de vRealize Automation .

La lista de equilibradores de carga es meramente informativa. En función de las entradas del asistente anterior, presenta cada equilibrador de carga en su implementación junto con los miembros, su función de componente, el nombre de dominio completo y el número de puerto.

Ponga en pausa aquí y utilice la lista mientras inicia sesión en sus equilibradores de carga para agregar los miembros de vRealize Automation y abrir los puertos.

Validación

En la página Validación, compruebe que puede proceder con la instalación de vRealize Automation.

Para comprobar que todos los componentes, las funciones y las cuentas de vRealize Automation son correctos, y que los sistemas se pueden autenticar con otro, haga clic en **Validar**. El proceso puede durar media hora o más dependiendo de su entorno.

Si se producen errores, expanda el elemento de línea con errores y haga las correcciones necesarias en función del estado y los mensajes que se presentan. No puede continuar con la instalación de vRealize Automation hasta que se apruebe la validación.

Crear snapshots

En la página Crear Snapshots, puede realizar una pausa para tomar snapshots de máquina virtual de todos los componentes de vRealize Automation antes de continuar con la instalación.

Incluso después de aprobar la validación, se aconseja estar bien preparado para los problemas inesperados en torno a la instalación. Antes de iniciar la instalación, utilice el cliente de vSphere para tomar un snapshot de cada dispositivo de vRealize Automation y cada instancia de Windows Server de IaaS. De lo contrario, será necesario volver a introducir toda la configuración del asistente para regresar a este punto.

Si dispone de recursos suficientes, puede tomar snapshots de máquinas virtuales en ejecución. Una práctica conveniente es detenerlas primero.

- 1 En la parte superior derecha del asistente de instalación, haga clic en **Cerrar sesión**.

Importante Si cierra el asistente con otra opción que no sea **Cerrar sesión**, no podrá volver a abrir al asistente.

- 2 En vSphere, desconecte el sistema operativo invitado de cada dispositivo de vRealize Automation y cada instancia de Windows Server de IaaS.
- 3 Haga clic con el botón secundario en las máquinas virtuales y seleccione **Tomar snapshot**.
- 4 Asigne un nombre al snapshot.
- 5 Para incluir la memoria de la máquina en el snapshot, seleccione **Snapshot de memoria de la máquina virtual**.
- 6 Haga clic en **Aceptar**.
Espere a que se creen los snapshots.
- 7 Conecte el sistema operativo invitado de cada dispositivo de vRealize Automation y cada instancia de Windows Server de IaaS.
- 8 Inicie sesión nuevamente como usuario raíz para regresar a la página de snapshots del asistente de instalación.

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

Detalles de la instalación

En la página Detalles de la instalación, inicie la instalación de vRealize Automation o vuelva a intentarlo si se produjeron problemas.

Para iniciar la instalación, haga clic en **Instalar**. Según el entorno, la instalación puede demorar hasta una hora o más.

Durante la instalación o con posterioridad, puede hacer clic en el botón **Recopilar logs**.

- Al recopilar logs, aparece un vínculo de descarga de un archivo ZIP sobre la tabla de estado.
- Al recopilar logs más de una vez, cada recopilación sobrescribe la anterior.

Si desea ver los logs actuales, descárguelos antes de hacer clic **Recopilar logs** nuevamente.

Si se producen errores, el asistente interrumpirá la instalación y mostrará mensajes para ayudar a realizar correcciones. Después de evaluar los mensajes y tener en cuenta las correcciones necesarias, es posible que necesite o no los snapshots que creó.

No restaurar los snapshots

Si el asistente habilita **Error al reintentar**, puede realizar correcciones y volver a intentar la instalación sin revertir las máquinas a los snapshots.

Después de realizar las correcciones, haga clic en **Error al reintentar**.

Restaurar los snapshots de instancias de Windows Server de IaaS

Si el asistente habilita **Reintentar todos IaaS**, realice los siguientes pasos.

- 1 En vSphere, revierta todas las máquinas Windows de IaaS a los snapshots tomados en la página anterior del asistente.
- 2 Si los snapshots se tomaron después de un apagado, encienda los sistemas operativos invitados.

- 3 Si utilizó una instancia externa de SQL Server, elimine la base de datos SQL de vRealize Automation.
- 4 Realice las correcciones.
- 5 Haga clic en **Reintentar todos IaaS**.

Restaurar los snapshots de dispositivos e instancias de Windows Server de IaaS

Si el asistente muestra mensajes acerca del dispositivo de vRealize Automation, realice los siguientes pasos.

- 1 En vSphere, revierta todos los dispositivos de vRealize Automation y las máquinas Windows de IaaS a los snapshots tomados en la página anterior del asistente.
- 2 Si los snapshots se tomaron después de un apagado, encienda los sistemas operativos invitados.
- 3 Si utilizó una instancia externa de SQL Server, elimine la base de datos SQL de vRealize Automation.
- 4 Realice las correcciones.
- 5 Inicie sesión nuevamente como usuario raíz para regresar al asistente de instalación.
`https://vrealize-automation-appliance-FQDN:5480`
- 6 Regrese a la página Detalles de la instalación y haga clic en **Instalar**.

Licencias

En la página Licencias, introduzca una clave para activar el producto vRealize Automation instalado.

En **Nueva clave de licencia**, introduzca su clave y haga clic en **Enviar clave**. Puede enviar más de una clave por separado, incluidas las claves para instancias independientes de vRealize Automation, vRealize Suite, vRealize Business for Cloud y vRealize Code Stream.

En esta página, también puede seleccionar si desea habilitar vRealize Code Stream.

vRealize Code Stream no se admite en implementaciones de vRealize Automation de alta disponibilidad o de producción y requiere vRealize Code Stream Management Pack. Para obtener más información, consulte [Licencias de vRealize Code Stream](#).

Telemetría

En la página Telemetría, decide si vRealize Automation debe enviar o no estadísticas de uso a VMware como parte del programa de mejora de la experiencia de cliente.

Active o desactive la opción para unirse al programa de mejora de la experiencia de cliente (CEIP).

Para obtener más información, consulte [El programa de mejora de la experiencia de cliente](#).

Opciones posteriores a la instalación

En la página Opciones posteriores a la instalación, tiene opciones para crear nuevos datos de vRealize Automation o migrar datos de implementación antiguos a la nueva instalación.

- **Configurar contenido inicial** crea un nuevo usuario local del tenant predeterminado. Ese usuario local puede iniciar el proceso de configuración en el tenant predeterminado.

Para usar esta opción, es necesario haber añadido al menos un endpoint de vSphere anteriormente en la página Agentes del asistente de instalación.

- **Migrar una implementación** transfiere los datos de vRealize Automation antiguos a esta implementación recién instalada. La migración conserva los elementos esenciales como grupos, blueprints y endpoints.
- **Continuar** conduce al final del asistente de instalación.

Configuración de contenido inicial

En la página Configuración de contenido inicial, debe crear un nuevo usuario tenant predeterminado de vRealize Automation local que puede iniciar un flujo de trabajo de contenido para un endpoint de vSphere.

Nota Esta opción solo está disponible si se añadió al menos un endpoint de vSphere con anterioridad en la página Agentes.

El nuevo nombre de usuario local es configurationadmin. vRealize Automation concede los siguientes privilegios a configurationadmin.

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

Escriba y confirme una contraseña de inicio de sesión para configurationadmin. Para generar un elemento del catálogo y lograr que configurationadmin pueda iniciar el proceso de configuración después de iniciar sesión en el tenant predeterminado, haga clic en **Crear contenido inicial**.

Configuración de migración

En la página Configuración de migración, puede iniciar la transferencia de una implementación de vRealize Automation anterior a su implementación recién instalada.

Antes de migrar una implementación anterior, cumpla con las siguientes directrices.

- Revise cuidadosamente la guía de migración de vRealize Automation asociada con la versión de la implementación anterior. Los requisitos previos y otros detalles pueden variar.

- Migre los tenants y los almacenes de identidades anteriores a la instancia de VMware Identity Manager en la nueva implementación.
- Clone la base de datos SQL Server de IaaS anterior y restáurela en la base de datos de IaaS de la nueva implementación. Anote el nombre de la base de datos clonada.
- Obtenga y tome nota de la clave de cifrado de la base de datos SQL Server de IaaS anterior.
- Cree y tome nota de una nueva frase de contraseña para volver a cifrar los datos migrados.
- Anote el FQDN y las credenciales de inicio de sesión raíz del equilibrador de carga o del dispositivo de vRealize Automation anterior.
- Anote las nuevas credenciales de inicio de sesión raíz de la nueva implementación.

Las interfaces estándar de instalación de vRealize Automation

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 [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.

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 1-27. Lista de comprobación de implementación mínima

| Tarea | | Detalles |
|--------------------------|--|---|
| <input type="checkbox"/> | Planifique el entorno y compruebe que los requisitos previos de instalación se cumplen. | 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, cáncélelo 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 **Configuración de vRA > Configuración del host**.

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

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

Los certificados que importe deben ser de confianza y, asimismo, válidos para todas las instancias 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 | <ol 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 | <ol 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 | <ol style="list-style-type: none"> a Copie los valores de certificado desde BEGIN PRIVATE KEY a END PRIVATE KEY (encabezado y pie de página incluidos) y péguelos en el cuadro de texto Clave privada RSA. b Copie los valores de certificado desde BEGIN CERTIFICATE a END CERTIFICATE (encabezado y pie de página incluidos) y péguelos en el cuadro de texto Cadena de certificados. Si hay varios valores de certificado, incluya un encabezado BEGIN CERTIFICATE y un pie de página END CERTIFICATE por cada uno de ellos. <p>Nota En el caso de certificados encadenados, puede haber atributos adicionales disponibles.</p> <ol 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 **Configuración de vRA > Licencias**.
 - b Haga clic en **Licencias**.
 - c Introduzca la clave de licencia de vRealize Automation válida que obtuvo al descargar los archivos de instalación y haga clic en **Enviar clave**.

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

- 12 Seleccione si desea habilitar vRealize Code Stream e introduzca una licencia de vRealize Code Stream.

vRealize Code Stream no se admite en implementaciones de vRealize Automation de alta disponibilidad o de producción.

- 13 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`.

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 consola de administración 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**.

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**.

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 1-28. 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. | 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 |
| <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 [Complemento de VMware 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.

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 en clúster, la organización de certificados de vRealize Automation se ajusta en gran medida a la estructura formal en tres niveles de vRealize Automation. Los tres niveles son Dispositivo de vRealize Automation, los componentes de sitio web de IaaS y los componentes de Manager Service. En un sistema distribuido, cada máquina de hardware de un nivel particular comparte un certificado. Es decir, cada Dispositivo de vRealize Automation comparte un certificado común y cada máquina de Manager Service comparte el certificado común que se aplica a esa capa.

Se pueden usar certificados autofirmados que generen los usuarios o el sistema, o bien certificados que proporciona una CA con implementaciones distribuidas de vRealize Automation. A partir de vRealize Automation 7.0 y posterior, si el usuario no proporciona ningún certificado, el instalador genera automáticamente certificados autofirmados para todos los nodos correspondientes y los coloca en los almacenes de confianza adecuados.

Puede utilizar equilibradores de carga con componentes distribuidos de vRealize Automation para proporcionar alta disponibilidad y admitir la conmutación por error. VMware recomienda que las implementaciones de vRealize Automation utilicen una configuración de acceso directo (pass-through) para las implementaciones que usen equilibradores de carga. En una configuración de acceso directo, los equilibradores de carga pasan las solicitudes por los componentes adecuados en lugar de descifrarlas. Después, los servidores web de Dispositivo de vRealize Automation e IaaS deben realizar el descifrado que sea necesario.

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

Si proporciona o genera sus propios certificados mediante Openssl u otra herramienta, puede utilizar caracteres comodín o certificados de nombre alternativo del firmante (SAN). Tenga en cuenta que los certificados de IaaS deben usar certificados multiusuario.

Si proporciona certificados, debe obtener un certificado multiusuario que incluya el componente de IaaS del clúster y, a continuación, copiar el certificado en el almacén de confianza de cada componente. Si utiliza equilibradores de carga, debe incluir el FQDN del equilibrador de carga en la dirección de confianza del certificado multiusuario del clúster.

Si necesita actualizar los certificados autofirmados que ha generado el sistema con los certificados que haya proporcionado el usuario o CA, consulte [Actualización de certificados de vRealize Automation](#).

En la tabla Requisitos de confianza de certificados se resumen los requisitos que hay que cumplir para realizar un registro de confianza para los diversos certificados importados.

Tabla 1-29. Requisitos de confianza de certificados

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

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 1-30. 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 | | 123.234.1.105 |
| Solo como referencia; no introduzca direcciones IP | | |

Tabla 1-30. Dispositivo de vRealize Automation (Continuación)

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

Tabla 1-31. 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 |

Tabla 1-31. Servidores de Windows de IaaS (Continuación)

| Variable | Mi valor | Ejemplo |
|--|----------|-------------------------------|
| 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 |
| 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 1-32. 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 1-33. 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 |

Tabla 1-33. Distributed Execution Managers de IaaS (Continuación)

| Variable | Mi valor | Ejemplo |
|---|----------|---------------|
| 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 [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, cáncélelo 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 **Configuración de 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 el tipo de certificado en el menú **Acción de certificado**.

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

Los certificados que importe deben ser de confianza y, asimismo, válidos para todas las instancias 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. <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 Si la red o el equilibrador de carga lo requieren, copie el certificado importado o recién creado en el equilibrador de carga del dispositivo virtual.

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

a Si aún no ha iniciado sesión, iníciela en la consola de administración del dispositivo de vRealize Automation como usuario raíz.

b Haga clic en la pestaña **Administración**.

c Haga clic en el submenú **Administración**.

d Seleccione la casilla de verificación **Servicio SSH habilitado**.

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

e Seleccione la casilla de verificación **Inicio de sesión SSH de administrador habilitado**.

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

f Haga clic en **Guardar configuración**.

8 Defina la configuración de SSO.

9 Haga clic en **Servicios**.

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

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

10 Introduzca la información de licencia.

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

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

11 Seleccione si desea habilitar vRealize Code Stream e introduzca una licencia de vRealize Code Stream.

vRealize Code Stream no se admite en implementaciones de vRealize Automation de alta disponibilidad o de producción.

12 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.

13 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.

14 Haga clic en **Guardar configuración**.

15 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.

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 **Configuración de 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.

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 1-34. 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 1-35. 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 <i>db_server</i> 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). |
| <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. |

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 1-36. Valores de base de datos

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

- 5 Revise la configuración de la sección DB Settings de 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 consola de administración 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**.

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.

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 consola de administración 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 | <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> |

- 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 | <p>Escriba la frase de contraseña que creó anteriormente en los cuadros de texto Frase de contraseña y Confirmar.</p> |
| Si es la primera instalación | <p>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.</p> |

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](#).
- 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 consola de administración 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 | 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 primer componente del servidor web de IaaS, <i>web.mycompany.com:443</i> . No escriba las direcciones IP. |

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

- 22 En los cuadros de texto **Información 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 consola de administración 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 | <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.

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](#).
- 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 consola de administración 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.
- Si importó un certificado después de iniciar la instalación, haga clic en **Actualizar** para actualizar la lista.
 - Seleccione el certificado que quiera usar en **Certificados disponibles**.
 - 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](#).

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 consola de administración 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\Log*s.
- 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.

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 [Preparación de su entorno de SCVMM](#) y [Crear un endpoint de Hyper-V \(SCVMM\)](#).

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**.

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 1-37. 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 desaproveionarla. | Instalar el agente de EPI de Visual Basic Scripting |

Tabla 1-37. Elegir un escenario de agentes (Continuación)

| Escenario de integración | Procedimientos y requisitos de agente |
|---|---|
| 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.

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 1-38. 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 |
| Clúster de almacén de datos | Configurar un clúster de almacén de datos |
| Carpeta | Crear carpeta |

Tabla 1-38. Permisos necesarios para que el agente de vSphere administre una instancia de vCenter Server (Continuación)

| Valor de atributo | | Permiso |
|-------------------|---------------|--|
| | | Eliminar carpeta |
| Global | | Administrar atributos personalizados |
| | | Establecer atributo personalizado |
| Red | | Asignar red |
| Permisos | | Modificar permiso |
| Recurso | | Asignar máquina virtual a grupo de recursos |
| | | Migrar máquina virtual apagada |
| | | Migrar máquina virtual encendida |
| Máquina virtual | Inventario | Crear a partir de existente |
| | | Crear nueva |
| | | 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 |
| | | 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) |

Tabla 1-38. Permisos necesarios para que el agente de vSphere administre una instancia de vCenter Server (Continuación)

| Valor de atributo | Permiso |
|-------------------|--|
| Aprovisionar | Configuración |
| | Colocación de archivo de intercambio |
| | 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 consola de administración 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 | Instale agentes redundantes en distintos servidores. Configure los agentes redundantes de forma idéntica y asígneles el mismo nombre. |
| Agente independiente | Asigne un nombre único al agente. |

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 asígneles 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 consola de administración 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 | Instale agentes redundantes en distintos servidores. Configure los agentes redundantes de forma idéntica y asígneles el mismo nombre. |
| Agente independiente | Asigne un nombre único al agente. |

- 13 Indique el **Nombre de agente** al administrador de IaaS que configure los endpoints.

Para permitir el acceso y la recopilación de datos, el endpoint debe estar vinculado al agente que lo haya configurado.

14 Configure una conexión con el 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: XAdmin
```

- 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 consola de administración 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 | Instale agentes redundantes en distintos servidores. Configure los agentes redundantes de forma idéntica y asígneles el mismo nombre. |
| Agente independiente | Asigne un nombre único al agente. |

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 consola de administración 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 1-39. 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: |
| | <pre>help about_signing help Set-ExecutionPolicy</pre> |

Instalar el agente de Visual Basic Scripting

Los agentes de PowerShell de integración de aprovisionamiento externo (EPI) permiten integrar sistemas externos en el proceso de aprovisionamiento de máquinas. Utilice un agente de EPI para ejecutar scripts de Visual Basic a modo de pasos extra durante el proceso de aprovisionamiento.

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 consola de administración 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 | Instale agentes redundantes en distintos servidores. Configure los agentes redundantes de forma idéntica y asígneles el mismo nombre. |
| Agente independiente | Asigne un nombre único al agente. |

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 consola de administración 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

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.

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.

Archivo de respuesta de la instalación silenciosa de vRealize Automation

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 faltan. 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 registros 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 registros.

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
```

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

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

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 **Configuración de 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.

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.

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
```

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 la conmutación por error automática parece no funcionar, consulte [La conmutación por error automática de Manager Service no se activa](#) para obtener sugerencias de solución de problemas.

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 la base de datos está establecida en modo sincrónico en la configuración de vRA > Base de datos en 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 más información, consulte [Realizar una conmutación por error manual de la base de datos de dispositivo 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 [Actualización de certificados 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 [Configurar la base de datos de SQL para un nuevo nombre de host](#).
- 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. Restablezca 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.

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.

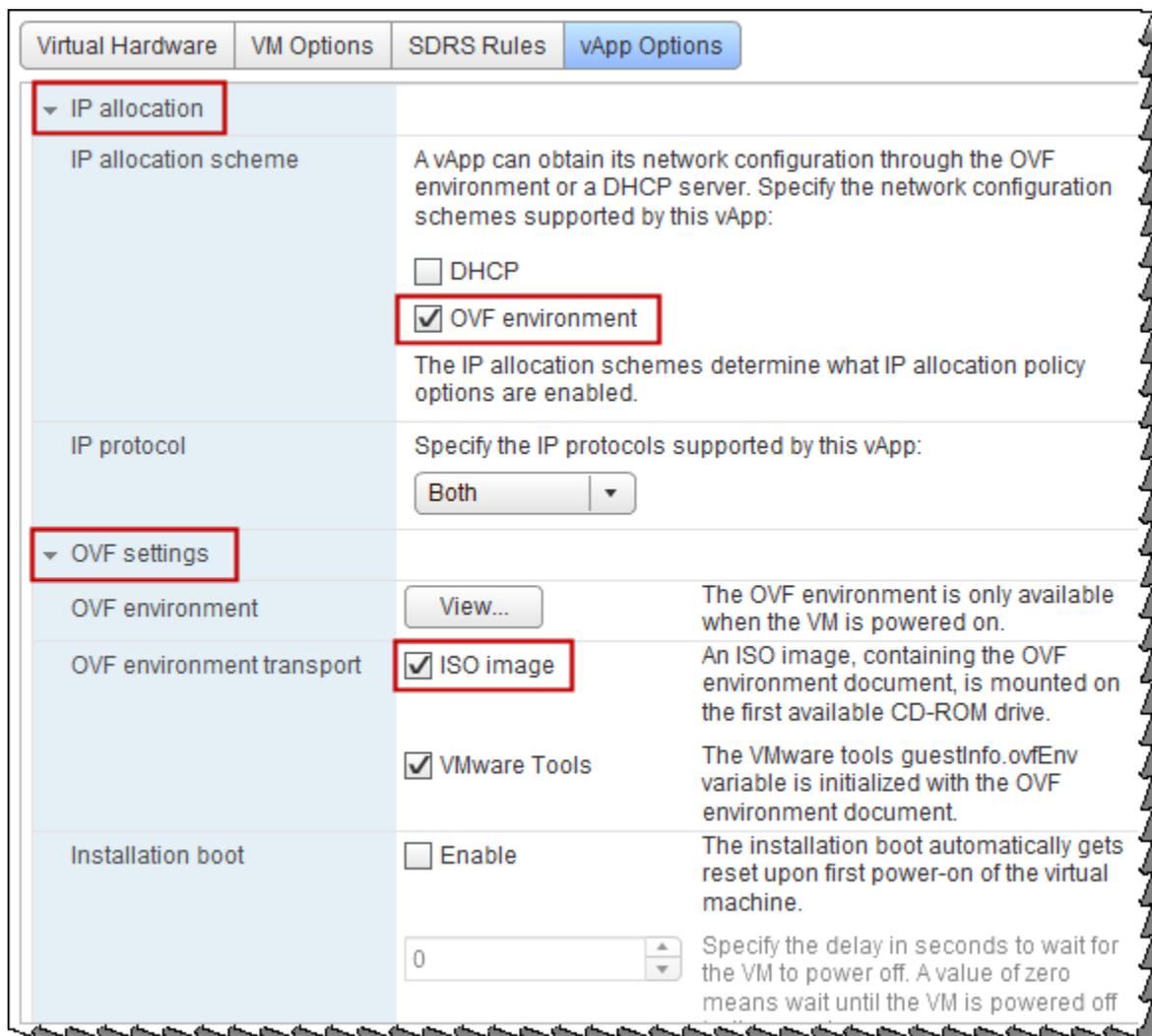
En todos los servidores de IaaS, repita el proceso para el archivo `Windows\system32\drivers\etc\hosts`.

- 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**.

Figura 1-16. Opciones de entorno de OVF e 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 conexión de la base de datos en **Configuración de vRA > Base de datos**
 - Estado de RabbitMQ en **Configuración de vRA > Mensajes**
 - Estado de Xenon en **Configuración de 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 más información, consulte [Actualización de certificados 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 1-40. 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 1-41. 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\DEM-name | 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\agent-name | VRMAgent.exe.config |

Tabla 1-42. 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\agent-name | 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 **Configuración de vRA > Configuración del host**, cambie **Nombre del host** a la instancia de CNAME que haya elegido.

Licencias de vRealize Code Stream

Puede habilitar vRealize Code Stream introduciendo una licencia de vRealize Code Stream en vRealize Automation.

Puede introducir la licencia de vRealize Code Stream en cualquiera de estas ubicaciones:

- En la página Licencias del asistente de instalación de vRealize Automation. Para obtener más información, consulte [Instalación de vRealize Code Stream](#).
- En la pestaña Licencias de la interfaz de administración de dispositivos de vRealize Automation. Para obtener más información, consulte [Aplicar una licencia de vRealize Code Stream a un dispositivo](#).

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 [documentación 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.

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 [Configurar una instancia de Active Directory mediante un vínculo LDAP/IWA](#).
- 2 Si se trata de un entorno de HA, debe seguir también los pasos que se describen en [Configurar la administración de directorios para alta disponibilidad](#).
- 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 Guarde y cierre `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 Vaya a **Configuración de 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 Vaya a **Configuración de vRA > Clúster** y compruebe que todos los nodos estén 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 1-43. 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.

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.

Requisitos previos

- Cree snapshots de todos los nodos de la instalación de vRealize Automation.

- Compruebe que todos los nodos de la instalación de vRealize Automation están en funcionamiento. Si intenta instalar o quitar una revisión sin que todos los nodos estén en ejecución, es posible que la interfaz de administración de dispositivos de vRealize Automation deje de responder. Si esto ocurre, póngase en contacto con el equipo de soporte técnico. No intente administrar revisiones por otros medios ni utilizar vRealize Automation hasta que se resuelva el problema.
- Si el entorno utiliza equilibradores de carga para alta disponibilidad, deshabilite el tráfico a los nodos secundarios hasta después de instalar o quitar las revisiones.
- Si se está instalando una nueva revisión, obtenga el archivo de revisión y cópielo en el sistema de archivos disponible para el navegador que utilice para la interfaz de administración de dispositivos de vRealize Automation.
- Compruebe [Base de conocimientos de VMware](#) para obtener información de última hora o recién publicada sobre revisiones.

Abra la base de conocimientos e introduzca *Aplicación de revisiones de vRealize Automation* en el cuadro de búsqueda. Por ejemplo, se realiza un seguimiento del [artículo 51708 de la base de conocimientos de VMware](#) y se actualiza con la información de la revisión de vRealize Automation 7.4 más reciente.

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 **Configuración de 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
```

Instalar una nueva revisión

Las nuevas revisiones de vRealize Automation se instalan a través de la interfaz de administración de dispositivos de vRealize Automation.

Requisitos previos

Compruebe los requisitos previos y desplácese hasta la interfaz de administración de revisiones. Consulte [Acceder a la administración de revisiones](#).

Procedimiento

- 1 Haga clic en **Nueva revisión**.
- 2 Haga clic en **Cargar revisión**.
- 3 Busque el archivo de revisión y selecciónelo.
- 4 Después de cargar la revisión, verifique los detalles de la revisión.
- 5 Si tiene la revisión incorrecta, haga clic en **Quitar** para cancelarla. Si la revisión es correcta, haga clic en **Instalar**.
- 6 Compruebe que se han cumplido los requisitos previos y haga clic en **Instalar**.
La instalación de la revisión puede tardar varios minutos.
- 7 Haga clic en **Listo**.

Si se produce un error en la instalación de la revisión, puede hacer clic en **Reintentar** para volver a intentarlo o en **Quitar** para cancelarla. Al cancelarla, se revierte vRealize Automation al estado que tenía antes de iniciar la instalación de la revisión.

Instalar la revisión actual en nuevos nodos

Puede añadir la revisión de vRealize Automation instalada más reciente a los nodos del clúster recién añadidos.

Requisitos previos

Compruebe los requisitos previos y desplácese hasta la interfaz de administración de revisiones. Consulte [Acceder a la administración de revisiones](#).

Procedimiento

- 1 Haga clic en **Revisiones instaladas**.
- 2 Seleccione la revisión más reciente.
- 3 Haga clic en **Instalar**.
- 4 Siga las indicaciones.

Quitar la revisión actual

Puede quitar la revisión instalada más reciente de vRealize Automation y revertir al nivel de revisión anterior.

Requisitos previos

Desplácese hasta la interfaz de administración de revisiones. Consulte [Acceder a la administración de revisiones](#).

Procedimiento

- 1 Haga clic en **Revertir**.
- 2 Seleccione la revisión más reciente.
- 3 Haga clic en **Revertir**.
- 4 Siga las indicaciones.

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 [Configurar las opciones de tenants](#).
- Los administradores de IaaS preparan los recursos externos para el aprovisionamiento. Consulte [Preparaciones externas para el aprovisionamiento](#)
- Si configuró Crear contenido inicial durante la instalación, el administrador de la configuración puede solicitar el elemento del catálogo Contenido inicial para rellenar en poco tiempo una prueba del concepto. Para ver un ejemplo de cómo solicitar el elemento y completar la acción de usuario manual, consulte [Escenario: Solicitar el contenido inicial para una implementación de prueba de concepto de Rainpole](#).

Solucionar problemas de instalación de vRealize Automation

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.

Ubicaciones de logs predeterminadas

Consulte los archivos log del producto y del sistema para obtener información acerca de los errores de instalación.

Nota Para la recopilación de logs, piense en aprovechar los vRealize Log Insight Content Pack de vRealize Automation y vRealize Orchestrator. Los Content Pack y Log Insight proporcionan un resumen unificado de los eventos de log de los componentes de vRealize Suite. Para obtener más información, consulte [VMware Solution Exchange](#).

Para obtener la lista más reciente de ubicaciones de logs, consulte [Artículo 2141175 de la base de conocimientos de VMware](#).

Logs de Windows

Busque los archivos log de los eventos de Windows en la siguiente ubicación.

| Log | Ubicación |
|--------------------------------------|---|
| Logs del Visor de eventos de Windows | Inicio > Panel de control > Herramientas administrativas > Visor de eventos |

Logs de instalación

Los logs de instalación se encuentran en las siguientes ubicaciones.

| Log | Ubicación predeterminada |
|-----------------------------|---|
| Logs de instalación | C:\Archivos de programa (x86)\vCAC\InstallLogs C:\Archivos de programa (x86)\VMware\vCAC\Server\ConfigTool\Log |
| Logs de instalación de WAPI | C:\Archivos de programa (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX> |

Logs de IaaS

Los logs de IaaS se encuentran en las siguientes ubicaciones.

| Log | Ubicación predeterminada |
|----------------------------|--|
| Logs de sitio web | C:\Archivos de programa (x86)\VMware\vCAC\Server\Website\Logs |
| Logs de repositorio | C:\Archivos de programa (x86)\VMware\vCAC\Server\Model Manager Web\Logs |
| Logs de Manager Service | C:\Archivos de programa (x86)\VMware\vCAC\Server\Logs |
| Logs de orquestaciones DEM | C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<system-name> DEO \Logs |
| Logs de agente | C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Agents\<agent-name>\logs |

Logs de marco de vRealize Automation

Las entradas de logs para los marcos vRealize Automation se encuentran en la siguiente ubicación.

| Log | Ubicación predeterminada |
|---------------|--------------------------|
| Logs de marco | /var/log/vmware |

Logs de aprovisionamiento de componentes de software

Los logs de aprovisionamiento de componentes de software se encuentran en la siguiente ubicación.

| Log | Ubicación predeterminada |
|---|--|
| Log de arranque de agente de software | /opt/vmware-appdirector (para Linux) o \opt\vmware-appdirector (para Windows) |
| Logs del script de ciclo de vida del software | /tmp/taskId (para Linux) \Users\darwin\AppData\Local\Temp\taskId (para Windows) |

Recopilación de logs en implementaciones distribuidas

Puede crear un archivo ZIP que empaquete todos los logs de los componentes en una implementación distribuida. .

Revertir una instalación fallida

Cuando se produce un error de instalación y esta se revierte, el administrador del sistema debe comprobar que se han desinstalado todos los archivos necesarios antes de iniciar una nueva instalación. Algunos archivos se deben desinstalar de forma manual.

Revertir una instalación mínima

Un administrador del sistema debe eliminar de forma manual algunos archivos y revertir la base de datos para desinstalar por completo una instalación de IaaS de vRealize Automation con errores.

Procedimiento

- 1 Si los siguientes componentes están presentes, desinstálelos mediante el programa de desinstalación de Windows.
 - Agentes de vRealize Automation
 - DEM de trabajo de vRealize Automation
 - DEM orquestador de vRealize Automation
 - Servidor de vRealize Automation
 - WAPI de vRealize Automation

Nota Si ve el siguiente mensaje, reinicie la máquina y, a continuación, siga los pasos de este procedimiento: Error al abrir el archivo de log de la instalación. Compruebe que la ubicación del archivo de log especificada existe y que se puede escribir en ella.

Nota Si el sistema Windows se ha revertido, o si ha desinstalado IaaS, debe ejecutar el comando `iisreset` antes de reinstalar el IaaS de vRealize Automation.

- 2 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 Sitio web predeterminado (o su sitio personalizado) y haga clic en **Enlaces**. Quite el enlace HTTPS (el valor predeterminado es 443).
- 4 Compruebe que se han eliminado el repositorio de aplicaciones, vRealize Automation y WAPI, y que los grupos de aplicaciones RepositoryAppPool, vCACAppPool y WapiAppPool también se han eliminado.

La instalación se ha eliminado por completo.

Revertir una instalación distribuida

Un administrador del sistema debe eliminar de forma manual algunos archivos y revertir la base de datos para desinstalar por completo una instalación de IaaS con errores.

Procedimiento

- 1 Si los siguientes componentes están presentes, desinstálelos mediante el programa de desinstalación de Windows.
 - Servidor de vRealize Automation
 - WAPI de vRealize Automation

Nota Si ve el siguiente mensaje, reinicie la máquina y, a continuación, siga este procedimiento: Error al abrir el archivo de log de la instalación. Compruebe que la ubicación del archivo de log especificada existe y que se puede escribir en ella.

Nota Si el sistema Windows se ha revertido, o si ha desinstalado IaaS, debe ejecutar el comando `iisreset` antes de reinstalar el IaaS de vRealize Automation.

- 2 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.

Tabla 1-44. 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 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 raíz y haga clic en **Configuración de vRA > Clúster**.
- 3 Haga clic en **Crear paquete de soporte**.
- 4 Haga clic en **Descargar** y guarde el paquete de soporte en el sistema.

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.

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.

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

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**).

Procedimiento

- 1 Seleccione **Herramientas > Configuración de Vista de compatibilidad**.
- 2 Desactive la opción **Mostrar sitios de la intranet en Vista de compatibilidad**.
- 3 Haga clic en **Cerrar**.

No se puede establecer una relación de confianza para el canal seguro SSL/TLS

Es posible que reciba el mensaje "No se puede establecer una relación de confianza para el canal seguro SSL/TLS al actualizar certificados de seguridad para vCloud Automation Center".

Problema

Si surge un problema de certificado con vcac-config.exe al actualizar un certificado de seguridad, puede ser que vea el siguiente mensaje:

```
Se ha terminado la conexión: No se puede establecer una relación de confianza para el canal seguro SSL/TLS
```

Si desea obtener más información sobre la causa del problema, siga el procedimiento que se describe a continuación.

Solución

- 1 Abra `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.

Si el problema persiste, repita el procedimiento y esta vez navegue a la dirección que necesita registrarse, es decir, la dirección de endpoint que usó en el registro con `vcac-config.exe`.

Conectarse a la red mediante un servidor proxy

Algunos sitios pueden conectarse a Internet mediante un servidor proxy.

Problema

Su implementación no puede conectarse a la Internet abierta. Por ejemplo, no puede acceder a sitios web, a las nubes públicas que administra ni a las direcciones de proveedores desde donde descarga software o actualizaciones.

Causa

Su sitio se conecta a Internet mediante un servidor proxy.

Solución

Requisitos previos

Solicítele al administrador de su sitio los nombres, números de puerto y credenciales del servidor proxy.

Procedimiento

- 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.

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

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.

Procedimiento

- 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/workfl
owexecutor.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/workfl
owexecutor.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.

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

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.

Procedimiento

- 1 Consulte el archivo de log `/var/log/vcac/catalina.out` y busque el mensaje `Cannot write to /etc/vcac/Encryption.key`.
- 2 Vaya al directorio `/etc/vcac/` y compruebe los permisos y propiedad del archivo `Encryption.key`. Debería ver una línea parecida a esta:

```
-rw----- 1 vcac vcac 48 Dec 4 06:48 encryption.key
```

Se necesitan permisos de lectura y escritura y el propietario y grupo del archivo debe ser `vcac`.

- 3 Si ve otra cosa, cambie los permisos o la propiedad del archivo según corresponda.

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.databasechangelock`, ejecute la siguiente consulta SQL.

```
select * from databasechangelock;
```

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.databasechangelock set locked=FALSE, lockgranted=NULL,
lockedby=NULL where id=1;
```

- 8 Desde `saas.databasechangelock`, ejecute la siguiente consulta SQL.

```
select * from databasechangelock;
```

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. Utilice la consola de administración de otro nodo para promocionar ese nodo como el nuevo principal, restaurando así el acceso de escritura a la base de datos de vRealize Automation.

Más adelante, volverá a conectar el nodo principal anterior, pero la pestaña Base de datos de su consola de administración seguirá mostrando el nodo como el principal, incluso cuando no lo sea. Los intentos que se hagan de utilizar la consola de administración de nodos para solucionar el problema promoviendo oficialmente el anterior nodo a principal fallarán.

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 consola de administración principal. Busque el nodo anterior que aparece como `invalid` en la pestaña Base de datos 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 o vuelva a unir correctamente un nodo principal anterior al clúster, no use su consola 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.

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.

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 msixexec 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, `c0DD0C01`.
- 3 Busque el código de referencia en el archivo log para ubicar la entrada asociada.
- 4 Para solucionar el problema, revise las entradas que aparecen por encima y por debajo de la entrada asociada.

La entrada de log asociada no señala específicamente el origen del problema.

Error al desinstalar un agente de proxy

Pueden producirse errores al quitar un agente de proxy si está habilitado el registro del programa de instalación de Windows.

Problema

Al intentar desinstalar un agente de proxy del Panel de control de Windows, la desinstalación no se realiza correctamente y aparece el siguiente error:

```
Error opening installation log file. Verify that the
specified log file location exists and is writable
```

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, vaya a **Inicio > Herramientas administrativas > Servicios de componentes**.

Nota Asegúrese de que todos los servidores de Windows tienen SID únicos en la configuración de MSDTC.

Además, el host de IaaS Manager Service debe poder resolver el nombre de NETBIOS del host de base de datos de SQL Server de IaaS. Si no se puede resolver el nombre de NETBIOS, agregue el nombre de NETBIOS de SQL Server al archivo /etc/hosts de la máquina de Manager Service y reinicie Manager Service.

- 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.

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

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.

Procedimiento

- 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.

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

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](#).

Procedimiento

- 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`

Actualizar vRealize Automation

Puede actualizar su entorno actual de vRealize Automation a la versión más reciente.

En función de su entorno actual de vRealize Automation, puede actualizar a la versión más reciente realizando una actualización local o una actualización en paralelo. Revise la información de esta página para determinar el mejor método de actualización para su entorno.

Una actualización local es un proceso compuesto por varios pasos. Los procedimientos se deben realizar siguiendo un orden determinado para actualizar los diversos componentes del entorno actual. Debe actualizar todos los componentes de producto a la misma versión. Solo puede realizar una actualización local para estas rutas.

- De vRealize Automation 6.2.5 a 7.4
- De vRealize Automation 7.1 a 7.4
- De vRealize Automation 7.2 a 7.4
- De vRealize Automation 7.3.x a 7.4

Con una actualización en paralelo se migran los datos de su entorno de vRealize Automation actual a un entorno de destino que esté implementado con la versión más reciente de vRealize Automation. Puede realizar una actualización en paralelo para estas rutas.

- De vRealize Automation 6.2.0 hasta 6.2.5 a 7.4
- De vRealize Automation 7.0 y 7.0.1 a 7.4
- De vRealize Automation 7.1, 7.2 y 7.3.x a 7.4

La migración no cambia su entorno actual. Si su entorno actual está integrado con vCloud Director, vCloud Air o tiene endpoints físicos, debe usar la migración para realizar una actualización. La migración elimina los endpoints no compatibles y todos los elementos asociados a estos en el entorno de destino.

Busque la versión actual de vRealize Automation en esta tabla. Use los documentos de la derecha para realizar una actualización del entorno de vRealize Automation a la versión más reciente.

Tabla 1-45. Rutas de actualización compatibles a vRealize Automation 7.4

| Versión que tiene instalada | Documentación para actualizaciones incrementales |
|---|--|
| vRealize Automation 7.1, 7.2 o 7.3.x | Consulte uno de estos temas. <ul style="list-style-type: none"> ■ Actualizar de vRealize Automation 7.1 o posterior a 7.4 ■ Migrar a vRealize Automation 7.4 |
| vRealize Automation 7.0 o 7.0.1 | Consulte Migrar a vRealize Automation 7.4 . |
| vRealize Automation 6.2.5 | Consulte uno de estos temas. <ul style="list-style-type: none"> ■ Actualizar de vRealize Automation 6.2.5 a 7.4 ■ Migrar a vRealize Automation 7.4 |
| vRealize Automation 6.2.0, 6.2.1, 6.2.2, 6.2.3, 6.2.4 | Consulte Migrar a vRealize Automation 7.4 |

Esta tabla proporciona información sobre la actualización desde una versión anterior de vCloud Automation Center. Debe actualizar a vRealize Automation 6.2.5 antes de actualizar a la versión más reciente de vRealize Automation. Encontrará vínculos a la documentación de las versiones 5.x y 6.x de vCloud Automation Center y vRealize Automation en <https://www.vmware.com/support/pubs/vcac-pubs.html>.

Tabla 1-46. Rutas de actualización compatibles a vRealize Automation 6.2.5

| Versión que tiene instalada | Documentación para actualizaciones incrementales |
|--------------------------------|--|
| vCloud Automation Center 6.0 | Realice actualizaciones en el siguiente orden: <ol style="list-style-type: none"> 1 <i>Actualización de vCloud Automation Center 6.0 a 6.0.1</i> 2 <i>Actualización a vCloud Automation Center 6.1</i> 3 <i>Actualización a vRealize Automation 6.2.x</i> |
| vCloud Automation Center 6.0.1 | Realice actualizaciones en el siguiente orden: <ol style="list-style-type: none"> 1 <i>Actualización a vCloud Automation Center 6.1</i> 2 <i>Actualización a vRealize Automation 6.2.x</i> |
| vCloud Automation Center 6.1.x | <i>Actualización a vRealize Automation 6.2.x</i> |
| vRealize Automation 6.2.x | Actualice directamente a la versión 6.2.5 como se describe en <i>Actualización a vRealize Automation 6.2.x</i> |

Nota vCloud Automation Center se ha rebautizado como vRealize Automation en la versión 6.2.0. Solo han cambiado la interfaz de usuario y los nombres de los servicios. Los nombres de directorios y los nombres de programas que contienen `vcac` no han cambiado.

Si está actualizando desde un entorno 6.2.x, revise estos elementos.

- La herramienta de evaluación para la actualización VMware vRealize Production Test analiza el entorno de vRealize Automation 6.2.x en busca de cualquier configuración de características que pueda causar problemas de actualización y, asimismo, comprueba que el entorno esté listo para la actualización. Para descargar esta herramienta y la documentación relacionada, vaya a la página de descarga del producto [Herramienta VMware vRealize Production Test](#).
- Al actualizar de un entorno 6.2.x a la versión más reciente de vRealize Automation, se introducen muchos cambios funcionales. Para obtener más información, consulte [Consideraciones sobre actualizar a esta versión de vRealize Automation](#).
- Si ha personalizado la implementación de vRealize Automation 6.2.x, póngase en contacto con el personal de soporte de CCE para obtener más información acerca de las consideraciones sobre la actualización.
- Los controles del diccionario de propiedades que no se admiten tras la actualización se pueden restaurar mediante las relaciones del diccionario de propiedades y vRealize Orchestrator.
- Si tiene flujos de trabajo en el entorno de origen que contienen código obsoleto, consulte la [guía de migración de extensibilidad de vRealize Automation](#), que incluye información sobre los cambios de código necesarios para la conversión a las suscripciones de agente de eventos.

Para evitar un problema conocido cuando se actualiza desde vRealize Automation 6.2.0, realice los siguientes pasos en cada nodo del sitio web de IaaS antes de iniciar la actualización. Este problema solo afecta a la versión 6.2.0. No afecta a otras versiones 6.2.x.

- 1 Abra el Bloc de notas con derechos administrativos. En Inicio, haga clic con el botón secundario en el icono de Bloc de notas y seleccione **Ejecutar como administrador**.
- 2 Abra el siguiente archivo:
`C:\Archivos de programa (x86)\VMware\VCAC\Server\Model Manager Web\web.config`

- 3 Encuentre la siguiente instrucción en el archivo:

```
<!-- add key="DisableMessageSignatureCheck" value="false"-->
```

- 4 Quite la marca de comentario de la declaración y cambie el valor de `false` a `true`.

```
<add key="DisableMessageSignatureCheck" value="true" />
```

- 5 Guarde el archivo.

Si el Bloc de notas le solicita la operación Guardar como, no ha abierto el Bloc de notas como Administrador y debe volver al paso 1.

- 6 Abra una ventana de Símbolo del sistema con derechos administrativos. En Inicio, haga clic con el botón secundario en el icono de Símbolo del sistema y seleccione **Ejecutar como administrador**.

- 7 Ejecute el restablecimiento.

- 8 Repita los pasos 1 a 7 para todos los nodos del sitio web.

Actualizar de vRealize Automation 7.1 o posterior a 7.4

Cuando se actualiza el entorno de vRealize Automation 7.1 o posterior a la versión más reciente, se siguen unos procedimientos de actualización específicos del entorno 7.1 o posterior.

Esta información es específica para la actualización de vRealize Automation 7.1 o posterior a la versión 7.4. Para obtener información sobre otras rutas de actualización admitidas, consulte [Actualizar vRealize Automation](#).

Actualizar vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4

Puede actualizar el entorno actual de vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4. Se utilizan los procedimientos de actualización específicos de esta versión para actualizar el entorno.

Una actualización local es un proceso compuesto de tres pasos. Los componentes se actualizan en el entorno actual en este orden.

- 1 Dispositivo de vRealize Automation
- 2 Servidor web de IaaS
- 3 vRealize Orchestrator

Debe actualizar todos los componentes de producto a la misma versión.

A partir de vRealize Automation 7.2, JFrog Artifactory Pro ya no se incluye en el paquete con el dispositivo de vRealize Automation. Si actualiza desde una versión anterior de vRealize Automation, el proceso de actualización elimina JFrog Artifactory Pro. Para obtener más información, consulte el artículo [2147237 de la Base de conocimientos](#).

Requisitos previos para actualizar vRealize Automation

Antes de ejecutar la actualización del entorno de vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4, revise estos requisitos previos.

Requisitos de configuración del sistema

Compruebe que se cumplan los siguientes requisitos previos antes de iniciar una actualización.

- Compruebe que todos los dispositivos y los servidores que forman parte de la implementación cumplen los requisitos del sistema para la versión más reciente. Consulte *Matriz de compatibilidad de vRealize Automation* en la documentación de [VMware vRealize Automation](#).
- Consulte la *Matriz de interoperabilidad de productos de VMware* en el sitio web de VMware para obtener información sobre la compatibilidad con otros productos de VMware.
- Verifique que la versión de vRealize Automation desde la que está actualizando esté en una condición de trabajo estable. Solucione los problemas que pudiera haber antes de la actualización.
- Compruebe que haya cambiado la configuración de tiempo de espera del equilibrador de carga de forma predeterminada a 10 minutos como mínimo.

Requisitos de configuración de hardware

Compruebe que el hardware de su entorno sea adecuado para vRealize Automation 7.4.

Consulte [Especificaciones del hardware y valores máximos de capacidad de vRealize Automation](#)

Compruebe que se cumplan los siguientes requisitos previos antes de iniciar una actualización.

- Debe tener como mínimo 18 GB de RAM, 4 CPU, disco 1 = 50 GB, disco 3 = 25 GB y disco 4 = 50 GB antes de ejecutar la actualización.

Si la máquina virtual se encuentra en vCloud Networking and Security, puede que deba asignar más espacio de RAM.

Aunque ya no se ofrece soporte general para vCloud Networking and Security, las propiedades personalizadas de VCNS siguen siendo válidas para los fines de NSX. Consulte el [artículo 2144733 de la base de conocimientos](#).

- Estos nodos deben tener al menos 5 GB de espacio de disco libre:
 - Sitio web de IaaS principal
 - Base de datos de Microsoft SQL
 - Model Manager
- En el nodo del sitio web de IaaS principal en el que están instalados los datos de Model Manager se debe haber instalado Java SE Runtime Environment 8, actualización 161 (64 bits) o posterior. Después de instalar Java, debe establecer la variable de entorno JAVA_HOME en la nueva versión.
- Para descargar y ejecutar la actualización, debe disponer de los siguientes recursos:
 - 5 GB en la partición raíz como mínimo
 - 5 GB en la partición /storage/db para el Dispositivo de vRealize Automation principal
 - 5 GB en la partición raíz para cada dispositivo virtual de réplica
- Compruebe la subcarpeta /storage/log y quite cualquier archivo ZIP guardado anterior para liberar espacio.

Requisitos previos generales

Compruebe que se cumplan los siguientes requisitos previos antes de iniciar una actualización.

- Debe instalar PowerShell 3.0 o una versión posterior en los sistemas IaaS de Windows antes de realizar la actualización. Se produce un error en la actualización si PowerShell 3.0 o una versión posterior no están instalados.
- Si Microsoft IIS está instalado, ejecute IISRESET en las máquinas web de IaaS y de Manager Service. La ejecución de IISRESET comprueba que no hay ningún servicio que dependa de IIS deshabilitado en el modo de inicio.
- Tiene acceso a todas las bases de datos y todos los equilibradores de carga a los que afecta la actualización de vRealize Automation o que participan en esta.
- El sistema no estará disponible para los usuarios mientras se lleva a cabo la actualización.
- Ha deshabilitado las aplicaciones que realizan consultas en vRealize Automation.
- Compruebe que el Coordinador de transacciones distribuidas de Microsoft (MSDTC) está habilitado en todos los servidores SQL asociados y de vRealize Automation. Para obtener instrucciones, consulte [el artículo 2089503 de la base de conocimientos](#).
- Haga lo siguiente si va a actualizar un entorno distribuido configurado con una base de datos de PostgreSQL integrada.
 - a Examine los archivos en el directorio pgdata del host principal antes de actualizar los hosts de réplica.
 - b Acceda a la carpeta de datos de PostgreSQL en el host principal en `/var/vmware/vpostgres/current/pgdata/`.
 - c Cierre los archivos que tenga abiertos en el directorio pgdata y quite los archivos que tengan el sufijo `.swp`.
 - d Compruebe que todos los archivos en este directorio tengan la propiedad correcta: `postgres:users`.

Además, debe comprobar que las propiedades personalizadas no tengan espacios en sus nombres.

Antes de actualizar a esta versión de vRealize Automation, elimine los caracteres de espacio que haya en los nombres de la propiedad personalizada (por ejemplo, puede reemplazar el espacio con un carácter de subrayado) para permitir que la propiedad personalizada se reconozca en la instalación de vRealize Automation actualizada. Los nombres de la propiedad personalizada de vRealize Automation no pueden contener espacios. Este problema puede afectar al uso de una instalación de vRealize Orchestrator actualizada que utiliza propiedades personalizadas que contenían espacios en las versiones anteriores de vRealize Automation o de vRealize Orchestrator o de ambos.

Lista de comprobación para actualizar vRealize Automation

Cuando se actualiza vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4, se actualizan todos los componentes de vRealize Automation en un orden específico.

El orden de la actualización varía en función de si está actualizando un entorno mínimo o un entorno distribuido con varios dispositivos de vRealize Automation.

Utilice las listas de comprobación para realizar un seguimiento de su trabajo a medida que se completa la actualización. Finalice las tareas en el orden en que aparecen.

Tabla 1-47. Lista de comprobación para actualizar un entorno mínimo de vRealize Automation

| Tarea | Instrucciones |
|--|--|
| <input type="checkbox"/> Ejecutar la recopilación de datos de inventario de red y seguridad de NSX antes de actualizar de vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4. Esta tarea solo es necesaria cuando vRealize Automation se integra con NSX. | Consulte Ejecutar la recopilación de datos del inventario de red y seguridad de NSX antes de actualizar vRealize Automation . |
| <input type="checkbox"/> Crear una copia de seguridad de la instalación actual. Este paso es crucial. | Para obtener más información sobre cómo crear una copia de seguridad del sistema y restaurarlo, consulte Crear copias de seguridad del entorno de vRealize Automation existente . Para obtener información general, consulte <i>Configurar la copia de seguridad y la restauración mediante Symantec Netbackup</i> en http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf . |
| <input type="checkbox"/> Descargar la actualización en el dispositivo de vRealize Automation. | Consulte Descargar actualizaciones del dispositivo de vRealize Automation . |
| <input type="checkbox"/> Instalar la actualización en el dispositivo y los componentes de IaaS de vRealize Automation. | Consulte Instalar la actualización en los componentes de IaaS y el dispositivo de vRealize Automation . |

Tabla 1-48. Lista de comprobación para actualizar un entorno distribuido de vRealize Automation

| Tarea | Instrucciones |
|--|--|
| <input type="checkbox"/> Ejecutar la recopilación de datos de inventario de red y seguridad de NSX antes de actualizar de vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4. Esta tarea solo es necesaria cuando vRealize Automation se integra con NSX. | Consulte Ejecutar la recopilación de datos del inventario de red y seguridad de NSX antes de actualizar vRealize Automation . |
| <input type="checkbox"/> Realizar una copia de la instalación actual. Este paso es crucial. | Para obtener más información sobre cómo crear una copia de seguridad del sistema y restaurarlo, consulte Crear copias de seguridad del entorno de vRealize Automation existente . Para obtener información detallada, consulte <i>Configurar la copia de seguridad y la restauración mediante Symantec Netbackup</i> en http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf . |
| <input type="checkbox"/> Deshabilitar la conmutación por error automática de PostgreSQL si se va a actualizar desde vRealize Automation 7.3.x. | Consulte Establecer el modo de replicación de PostgreSQL de vRealize Automation como asíncrono . |
| <input type="checkbox"/> Descargar actualizaciones en el dispositivo de vRealize Automation. | Consulte Descargar actualizaciones del dispositivo de vRealize Automation . |
| <input type="checkbox"/> Deshabilitar el equilibrador de carga. | Consulte la documentación del equilibrador de carga. |

Tabla 1-48. Lista de comprobación para actualizar un entorno distribuido de vRealize Automation (Continuación)

| Tarea | Instrucciones |
|---|---|
|  Instalar la actualización en el dispositivo principal y los componentes de IaaS de vRealize Automation. | Consulte Instalar la actualización en los componentes de IaaS y el dispositivo de vRealize Automation . |
| <p>Nota Instale la actualización en el dispositivo principal de un entorno distribuido.</p> | |
|  Habilitar el equilibrador de carga. | Configurar los equilibradores de carga |

Interfaces de usuario del entorno de vRealize Automation

El entorno de vRealize Automation se utiliza y administra con varias interfaces.

Interfaces de usuario

En estas tablas se describen las interfaces que se usan para administrar el entorno de vRealize Automation.

Tabla 1-49. Consola de administración de vRealize Automation

| Propósito | Acceso | Credenciales necesarias |
|--|---|--|
| La consola de vRealize Automation se emplea para las siguientes tareas de administrador del sistema. <ul style="list-style-type: none"> ■ Agregar tenants. ■ Personalizar la interfaz de usuario de vRealize Automation. ■ Configurar los servidores de correo electrónico. ■ Ver logs de eventos. ■ Configure vRealize Orchestrator. | <ol style="list-style-type: none"> 1 Inicie un navegador y abra la página de presentación del dispositivo de vRealize Automation con el nombre de dominio completo del dispositivo virtual: <code>https://vra-va-hostname.domain.name</code>. 2 Haga clic en Consola de vRealize Automation. También puede utilizar la siguiente dirección URL para abrir la consola de vRealize Automation: <code>https://vra-va-hostname.domain.name/vcac</code> 3 Inicie sesión. | Debe ser un usuario con la función de administrador del sistema. |

Tabla 1-50. Consola de tenant de vRealize Automation . Esta es la interfaz de usuario principal que se utiliza para crear y administrar servicios y recursos.

| Propósito | Acceso | Credenciales necesarias |
|---|---|---|
| <p>vRealize Automation se usa para las siguientes tareas.</p> <ul style="list-style-type: none"> ■ Solicitar nuevos blueprints de servicio de TI. ■ Crear y administrar recursos de TI y de nube. ■ Crear y administrar grupos personalizados. ■ Cree y administre grupos empresariales. ■ Asignar funciones a los usuarios. | <p>1 Inicie un navegador e introduzca la dirección URL de los tenants con el nombre de dominio completo del dispositivo virtual y el nombre de la URL de tenant:</p> <p><code>https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name</code> .</p> <p>2 Inicie sesión.</p> | <p>Debe ser un usuario con una o varias de las siguientes funciones:</p> <ul style="list-style-type: none"> ■ Arquitecto de aplicaciones ■ Administrador de aprobaciones ■ Administrador del catálogo ■ Administrador de contenedores ■ Arquitecto de contenedores ■ Consumidor de estado ■ Arquitecto de infraestructura ■ Consumidor de exportación segura ■ Arquitecto de software ■ Administrador de tenants ■ Arquitecto XaaS |

Tabla 1-51. Administración de dispositivos de vRealize Automation . Esta interfaz a veces se denomina interfaz de administración de dispositivos virtuales (Virtual Appliance Management Interface, VAMI).

| Propósito | Acceso | Credenciales necesarias |
|---|--|--|
| <p>La administración de dispositivos de vRealize Automation se usa para las siguientes tareas:</p> <ul style="list-style-type: none"> ■ Ver el estado de los servicios registrados. ■ Ver información del sistema y reiniciar o apagar el dispositivo. ■ Administrar la participación en el programa de mejora de la experiencia del cliente. ■ Ver el estado de la red. ■ Ver el estado de actualización e instalar actualizaciones. ■ Administrar la configuración de administración. ■ Administrar la configuración del host de vRealize Automation. ■ Administrar la configuración de SSO. ■ Administrar las licencias del producto. ■ Configurar la base de datos de Postgres de vRealize Automation. ■ Configurar la mensajería de vRealize Automation. ■ Configure el registro de vRealize Automation. ■ Instalar componentes de IaaS. ■ Migrar desde una instalación de vRealize Automation existente. ■ Administrar certificados de componentes de IaaS. ■ Configurar el servicio Xenon. | <ol style="list-style-type: none"> 1 Inicie un navegador y abra la página de presentación del dispositivo de vRealize Automation con el nombre de dominio completo del dispositivo virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Haga clic en Administración de dispositivos de vRealize Automation. También puede utilizar la siguiente dirección URL para abrir la administración de dispositivos de vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Inicie sesión. | <ul style="list-style-type: none"> ■ Nombre de usuario: raíz. ■ Contraseña: la contraseña que ha introducido al implementar el dispositivo de vRealize Automation. |

Tabla 1-52. Cliente de vRealize Orchestrator

| Propósito | Acceso | Credenciales necesarias |
|--|---|---|
| <p>El cliente de vRealize Orchestrator se usa para realizar las siguientes tareas:</p> <ul style="list-style-type: none"> ■ Desarrollar acciones. ■ Desarrollar flujos de trabajo. ■ Administrar políticas. ■ Instalar paquetes. ■ Administrar permisos de usuarios y de grupos de usuarios. ■ Asociar etiquetas a objetos de URI. ■ Ver el inventario. | <ol style="list-style-type: none"> 1 Inicie un navegador y abra la página de presentación de vRealize Automation con el nombre de dominio completo del dispositivo virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Para descargar el archivo <code>client.jnlp</code> en el equipo local, haga clic en Cliente de vRealize Orchestrator. 3 Haga clic con el botón derecho en el archivo <code>client.jnlp</code> y seleccione Iniciar. 4 En el cuadro de diálogo <i>¿Desea continuar?</i>, haga clic en Continuar. 5 Inicie sesión. | <p>Debe ser un usuario con la función de administrador del sistema o miembro del grupo <code>vcoadmins</code> configurado en los ajustes del proveedor de autenticación del centro de control de vRealize Orchestrator.</p> |

Tabla 1-53. Centro de control de vRealize Orchestrator

| Propósito | Acceso | Credenciales necesarias |
|--|---|--|
| <p>El centro de control de vRealize Orchestrator se emplea para editar la configuración de la instancia de vRealize Orchestrator predeterminada que está integrada en vRealize Automation.</p> | <ol style="list-style-type: none"> 1 Inicie un navegador y abra la página de presentación del dispositivo de vRealize Automation con el nombre de dominio completo del dispositivo virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Haga clic en Administración de dispositivos de vRealize Automation. También puede utilizar la siguiente dirección URL para abrir la administración de dispositivos de vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Inicie sesión. 4 Haga clic en Configuración de vRA > Orchestrator. 5 Seleccione la interfaz de usuario de Orchestrator. 6 Haga clic en Iniciar. 7 Haga clic en la URL de interfaz de usuario de Orchestrator. 8 Inicie sesión. | <p>Nombre de usuario</p> <ul style="list-style-type: none"> ■ Introduzca root (raíz) si no se configuró la autenticación basada en funciones. ■ Introduzca su nombre de usuario de vRealize Automation si está configurado para la autenticación basada en funciones. <p>Contraseña</p> <ul style="list-style-type: none"> ■ Escriba la contraseña que introdujo al implementar el dispositivo vRealize Automation si no se configuró la autenticación basada en funciones. ■ Introduzca la contraseña de su nombre de usuario si está configurado para la autenticación basada en funciones. |

Tabla 1-54. Símbolo del sistema de Linux

| Propósito | Acceso | Credenciales necesarias |
|---|--|---|
| <p>El símbolo del sistema de Linux se utiliza en un host, como el host del dispositivo de vRealize Automation, para realizar las siguientes tareas.</p> <ul style="list-style-type: none"> ■ Detener o iniciar servicios. ■ Editar archivos de configuración. ■ Ejecutar comandos. ■ Recuperar datos. | <p>1 En el host del dispositivo de vRealize Automation, abra un símbolo del sistema.</p> <p>Una forma de abrir el símbolo del sistema en el equipo local consiste en iniciar una sesión en el host mediante una aplicación como PuTTY.</p> <p>2 Inicie sesión.</p> | <ul style="list-style-type: none"> ■ Nombre de usuario: raíz. ■ Contraseña: la contraseña que ha creado al implementar el dispositivo de vRealize Automation. |

Tabla 1-55. Símbolo del sistema de Windows

| Propósito | Acceso | Credenciales necesarias |
|---|---|--|
| <p>Se puede utilizar un símbolo del sistema de Windows en un host, como el host de IaaS, para ejecutar scripts.</p> | <p>1 En el host de IaaS, inicie sesión en Windows.</p> <p>Una forma de iniciar sesión desde el equipo local consiste en iniciar una sesión de escritorio remoto.</p> <p>2 Abra el símbolo del sistema de Windows.</p> <p>Una forma de abrir el símbolo del sistema consiste en hacer clic con el botón derecho en el icono Inicio en el host y seleccionar Símbolo del sistema o Símbolo del sistema (administrador).</p> | <ul style="list-style-type: none"> ■ Nombre de usuario: usuario con privilegios administrativos. ■ Contraseña: contraseña del usuario. |

Actualización de productos de VMware integrados con vRealize Automation

Debe administrar todos los productos de VMware integrados con el entorno de vRealize Automation al actualizar vRealize Automation.

Si el entorno de vRealize Automation está integrado con uno o varios productos adicionales, deberá actualizar vRealize Automation antes de actualizar los productos adicionales. Si vRealize Business for Cloud está integrado con vRealize Automation, deberá anular el registro de vRealize Business for Cloud antes de actualizar vRealize Automation.

Siga el flujo de trabajo recomendado para la administración de productos integrados al actualizar vRealize Automation.

- 1 Actualice vRealize Automation.
- 2 Actualice VMware vRealize Operations Manager.
- 3 Actualice VMware vRealize Log Insight.
- 4 Actualice VMware vRealize Business for Cloud.

En esta sección, se proporcionan instrucciones adicionales para administrar vRealize Business for Cloud cuando se integra con el entorno de vRealize Automation.

Actualización de vRealize Operations Manager integrado con vRealize Automation

Actualice vRealize Operations Manager tras actualizar vRealize Automation.

Procedimiento

- 1 Actualice vRealize Automation.
- 2 Actualice vRealize Operations Manager. Para obtener información, consulte *Actualizar el software* en la documentación de [VMware vRealize Operations Manager](#).

Actualización de vRealize Log Insight integrado con vRealize Automation

Actualice vRealize Log Insight tras actualizar vRealize Automation.

Procedimiento

- 1 Actualice vRealize Automation.
- 2 Actualice vRealize Log Insight. Para obtener información, consulte *Actualizar vRealize Log Insight* en la documentación de [VMware vRealize Log Insight](#).

Actualización de vRealize Business for Cloud integrado con vRealize Automation

Cuando se actualiza el entorno de vRealize Automation, se debe cancelar el registro de la conexión con vRealize Business for Cloud, y luego volver a registrarla.

Realice este procedimiento para garantizar la continuidad del servicio con vRealize Business for Cloud al actualizar el entorno de vRealize Automation.

Procedimiento

- 1 Elimine el registro de vRealize Business for Cloud desde vRealize Automation. Consulte *Eliminar el registro de vRealize Business for Cloud desde vRealize Automation* en la documentación de [VMware vRealize Business for Cloud](#).
- 2 Actualice vRealize Automation.
- 3 Si es necesario, actualice vRealize Business for Cloud. Consulte *Actualizar vRealize Business for Cloud* en la documentación de [VMware vRealize Business for Cloud](#).
- 4 Registre vRealize Business for Cloud con vRealize Automation. Consulte *Registrar vRealize Business for Cloud con vRealize Automation* en la documentación de [VMware vRealize Business for Cloud](#).

Preparar la actualización de vRealize Automation

Complete estas tareas antes de actualizar vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4.

Realice estas tareas en el orden en que aparecen en la lista de comprobación. Consulte [Lista de comprobación para actualizar vRealize Automation](#).

Ejecutar la recopilación de datos del inventario de red y seguridad de NSX antes de actualizar vRealize Automation

Antes de actualizar vRealize Automation 7.1, 7.2 o 7.3.x a 7.4, debe ejecutar la recopilación de datos del inventario de red y seguridad de NSX en el entorno de vRealize Automation 7.1, 7.2 o 7.3.x.

Esta recopilación de datos es necesaria para que la acción de reconfiguración del equilibrador de carga funcione en vRealize Automation 7.4 para las implementaciones de 7.1, 7.2 o 7.3.x.

Procedimiento

- ◆ Ejecute la recopilación de datos del inventario de red y seguridad de NSX en vRealize Automation 7.1, 7.2 o 7.3.x antes de realizar la actualización a la versión 7.4. Consulte [Iniciar recopilación de datos de endpoint manualmente](#).

Pasos siguientes

[Prerrequisitos de copia de seguridad para actualizar vRealize Automation 7.1, 7.2 o 7.3 a 7.4](#).

Prerrequisitos de copia de seguridad para actualizar vRealize Automation 7.1, 7.2 o 7.3 a 7.4

Antes de comenzar la actualización, complete los prerrequisitos de copia de seguridad.

Requisitos previos

- Compruebe que el entorno de origen se ha instalado y configurado correctamente.
- Inicie sesión en vSphere Client y, para cada dispositivo en el entorno de origen, cree una copia de seguridad de todos los archivos de configuración del dispositivo de vRealize Automation en los directorios siguientes:
 - `/etc/vcac/`
 - `/etc/vco/`
 - `/etc/apache2/`
 - `/etc/rabbitmq/`
- Cree una copia de seguridad de la base de datos de Microsoft SQL Server de IaaS. Para obtener información, busque los artículos en [Microsoft Developer Network](#) sobre cómo crear una copia de seguridad completa de la base de datos de SQL Server.
- Cree una copia de seguridad de cualquier archivo que haya personalizado, como `DataCenterLocations.xml`.
- Cree un snapshot de cada dispositivo virtual y servidor de IaaS. Siga las directrices habituales para hacer una copia de seguridad del sistema completo en caso de que no se realice con éxito la actualización de vRealize Automation. Consulte [Copia de seguridad y recuperación de instalaciones de vRealize Automation](#).

Crear copias de seguridad del entorno de vRealize Automation existente

Antes de actualizar de vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4, apague cada servidor de IaaS de vRealize Automation en cada nodo de Windows y cada dispositivo de vRealize Automation en cada nodo de Linux, y cree un snapshot de ellos. Si la actualización no se realiza correctamente, use el snapshot para volver a la última configuración correcta conocida e intentar otra actualización.

Para obtener información sobre la forma de iniciar vRealize Automation, consulte [Iniciar vRealize Automation](#).

Requisitos previos

- [Prerrequisitos de copia de seguridad para actualizar vRealize Automation 7.1, 7.2 o 7.3 a 7.4](#).
- Desde vRealize Automation 7.0, la base de datos de PostgreSQL siempre está configurada en modo de alta disponibilidad. Inicie sesión en la consola de administración del dispositivo de vRealize Automation y seleccione **Configuración de vRA > Base de datos** para encontrar el nodo principal actual. Si la configuración de la base de datos aparece como una base de datos externa, cree una copia de seguridad manual de esta base de datos externa.
- Si la base de datos de Microsoft SQL de vRealize Automation no está alojada en el servidor de IaaS, cree un archivo de copia de seguridad de la base de datos.
- Compruebe que ha completado los requisitos previos de copia de seguridad para la actualización.
- Compruebe que ha tomado un snapshot del sistema mientras estaba desconectado. Es el método favorito para tomar un snapshot. Consulte la documentación de *vSphere 6.0*.

Nota Cuando realice copias de seguridad del dispositivo vRealize Automation y de los componentes de IaaS, deshabilite los snapshots en memoria y los snapshots en modo inactivo.

- Si modificó el archivo `app.config`, haga una copia de seguridad de ese archivo. Consulte [Restaurar cambios para iniciar sesión en el archivo app.config](#).
- Haga una copia de seguridad de los archivos de configuración del flujo de trabajo externo (xmldb). Consulte [Restaurar archivos de tiempo de espera de flujos de trabajo externos](#).
- Compruebe que exista una ubicación fuera de la carpeta actual donde puede almacenar el archivo de copia de seguridad. Consulte [Las copias de seguridad de archivos .xml hacen que el sistema agote el tiempo de espera](#).

Procedimiento

- 1 Inicie sesión en el cliente de vSphere.
- 2 Ubique cada máquina de Windows de IaaS de vRealize Automation y cada nodo del dispositivo de vRealize Automation.
- 3 Para cada máquina, haga clic en **Apagar invitado** en este orden.
 - a Máquinas de servidor Windows de IaaS
 - b Dispositivo de vRealize Automation.

- 4 Realice un snapshot de cada máquina de vRealize Automation.
- 5 Use el método de copia de seguridad que prefiera para crear una copia de seguridad completa de cada nodo del dispositivo.
- 6 Encienda el sistema. Consulte Iniciar vRealize Automation en *Administración de vRealize Automation*.

Si tiene un entorno de alta disponibilidad, siga estos pasos para encender los dispositivos virtuales.

- a Inicie el dispositivo de vRealize Automation principal.
- b Inicie sesión en la instancia de administración de dispositivos de vRealize Automation, haga clic en **Servicios** y espere hasta que el estado del servicio de licencias sea REGISTRADO.
- c Inicie el resto de dispositivos de vRealize Automation al mismo tiempo.
- d Inicie el nodo web principal y espere a que finalice el inicio.
- e Inicie la máquina principal de Manager Service, y espere entre 2 y 5 minutos.

El tiempo real dependerá de la configuración del sitio.

Nota En los equipos secundarios, no inicie ni ejecute el servicio de Windows, a menos que esté configurada la conmutación por error automática de Manager Service.

- f Inicie Distributed Execution Manager Orchestrator, los trabajos y todos los agentes de proxy de vRealize Automation.

Nota Puede iniciar estos componentes en cualquier orden. No es necesario que espere a que un componente finalice para iniciar otro.

- 7 Inicie sesión en cada consola de administración del dispositivo de vRealize Automation y compruebe que el sistema está totalmente operativo.
 - a Haga clic en **Servicios**.
 - b Compruebe que cada servicio está REGISTRADO.

Pasos siguientes

[Establecer el modo de replicación de PostgreSQL de vRealize Automation como asíncrono.](#)

Establecer el modo de replicación de PostgreSQL de vRealize Automation como asíncrono

Si actualiza desde un entorno distribuido de vRealize Automation que funciona en el modo de replicación sincrónico de PostgreSQL, debe cambiarlo al modo asíncrono antes de actualizar.

Requisitos previos

- Tiene un entorno distribuido de vRealize Automation que desea actualizar.
- Ha iniciado sesión como **raíz** en la instancia de administración de dispositivos de vRealize Automation en `https://vra-va-hostname.domain.name:5480`.

Procedimiento

- 1 Haga clic en **Configuración de vRA > Base de datos**.
- 2 Haga clic en **Modo asincrónico** y espere hasta que finalice la acción.
- 3 Compruebe que todos los nodos de la columna Estado de sincronización muestran el estado Asincrónico.

Pasos siguientes

[Descargar actualizaciones del dispositivo de vRealize Automation](#)

Descargar actualizaciones del dispositivo de vRealize Automation

Puede buscar actualizaciones en la consola de administración del dispositivo y descargarlas mediante uno de los siguientes métodos.

Para mejorar el rendimiento de la actualización, utilice el método de archivos ISO.

Para evitar posibles problemas al actualizar el dispositivo, o si surgen problemas durante la actualización del dispositivo, consulte el [artículo de la base de conocimientos de VMware Error en la actualización de vRealize Automation debido a duplicados en la base de datos de vRealize Orchestrator \(54987\)](#).

Descargar actualizaciones de dispositivo virtual para su uso con una unidad de CD-ROM

Su dispositivo virtual se puede actualizar desde un archivo ISO que el dispositivo lee desde la unidad de CD-ROM virtual. Este es el método preferido.

Descargue el archivo ISO y configure el dispositivo principal para utilizar este archivo en la actualización del dispositivo.

Requisitos previos

- Realice una copia de seguridad del entorno de vRealize Automation existente.
- Compruebe que estén habilitadas todas las unidades de CD-ROM que utiliza en la actualización antes de actualizar un dispositivo de vRealize Automation. Consulte la documentación de vSphere para obtener información sobre la forma de añadir una unidad de CD-ROM a una máquina virtual en el cliente de vSphere.

Procedimiento

- 1 Descargue el archivo ISO del repositorio de actualizaciones.
 - a Inicie un navegador y vaya a la [página del producto vRealize Automation](#) en www.vmware.com.
 - b Haga clic en los **recursos de descarga de vRealize Automation** para ir a la página de descarga de VMware.
 - c Descargue el archivo adecuado.
- 2 Busque el archivo descargado en el sistema para comprobar que el tamaño de archivo es el mismo que el del archivo de la página de descarga de VMware. Utilice las sumas de comprobación proporcionadas en la página de descarga para validar la integridad del archivo descargado. Para obtener información, consulte los vínculos de la parte inferior de la página de descarga de VMware.

- 3 Compruebe que el dispositivo virtual principal esté encendido.
- 4 Conecte la unidad de CD-ROM del dispositivo virtual principal al archivo ISO descargado.
- 5 En el dispositivo de vRealize Automation principal, inicie sesión en la Administración de dispositivos de vRealize Automation como **raíz** con la contraseña que introdujo al implementar el dispositivo de vRealize Automation.
- 6 Haga clic en la pestaña **Actualizar**.
- 7 Haga clic en **Configuración**.
- 8 En Repositorio de actualizaciones, seleccione **Usar actualizaciones de CDROM**.
- 9 Haga clic en **Guardar configuración**.

Descargar las actualizaciones del dispositivo de vRealize Automation desde un repositorio de VMware

Puede descargar la actualización del dispositivo de vRealize Automation de un repositorio público en el sitio web vmware.com.

Requisitos previos

- Realice una copia de seguridad del entorno de vRealize Automation existente.
- Compruebe que el dispositivo de vRealize Automation esté encendido.

Procedimiento

- 1 En el dispositivo de vRealize Automation principal, inicie sesión en la Administración de dispositivos de vRealize Automation como **raíz** con la contraseña que introdujo al implementar el dispositivo de vRealize Automation.
- 2 Haga clic en la pestaña **Actualizar**.
- 3 Haga clic en **Configuración**.
- 4 (opcional) Indique la frecuencia con la que se van a buscar actualizaciones en el panel Actualizaciones automáticas.
- 5 Seleccione **Usar repositorio predeterminado** en el panel Repositorio de actualizaciones.
El repositorio predeterminado se establece en la URL de vmware.com adecuada.
- 6 Haga clic en **Guardar configuración**.

Actualizar componentes de IaaS y dispositivo de vRealize Automation

Tras satisfacer los requisitos previos de actualización y descargar la actualización de dispositivo virtual, la actualización se instala en el dispositivo de vRealize Automation 7.1, 7.2 o 7.3.x para realizar la actualización a la versión 7.4.

En un entorno mínimo, la actualización se instala en el dispositivo de vRealize Automation. En un entorno distribuido, la actualización se instala en el nodo de dispositivo principal. El tiempo necesario para que la actualización finalice depende del entorno y de la red. Cuando la actualización finaliza, el sistema muestra los cambios realizados en la página de estado de la actualización de la administración de dispositivos de vRealize Automation. Cuando la actualización del dispositivo finalice, debe reiniciarlo. Cuando el dispositivo principal se reinicia en un entorno distribuido, el sistema reinicia cada nodo de réplica.

Después de reiniciar, aparece el mensaje Esperando a que se inicien los servicios del dispositivo virtual en la página de estado de la actualización. La actualización de IaaS arranca cuando el sistema se ha inicializado por completo y todos los servicios están en funcionamiento. En la página de estado de la actualización, puede seguir de cerca el progreso de la actualización de IaaS. El primer componente de servidor de IaaS puede tardar unos 30 minutos en finalizar. Durante la actualización, verá un mensaje parecido a Actualizando componentes de servidor del nodo web1-vra.mycompany.com.

Cada vez que un nodo de Manager Service termine de actualizarse, verá un mensaje parecido a Habilitando el modo de conmutación por error automática en el nodo mgr-vra.mycompany.com. A partir de vRealize Automation 7.3, el nodo de Manager Service activo cambia de una elección manual a una decisión de sistema sobre qué nodo se convierte en el servidor de conmutación por error. El sistema habilita esta función durante la actualización. Si tiene problemas con esta función, consulte [La actualización no puede actualizar al agente de administración](#).

Instalar la actualización en los componentes de IaaS y el dispositivo de vRealize Automation

La actualización se instala en el dispositivo virtual de vRealize Automation 7.1, 7.2 o 7.3.x para actualizar vRealize Automation y los componentes de IaaS a la versión 7.4.

No cierre la consola de administración mientras instala la actualización.

Si surge algún problema durante el proceso de actualización, consulte [Solucionar problemas de actualización de vRealize Automation](#).

Nota Durante la actualización del agente de administración en las máquinas virtuales de IaaS, se instala temporalmente un certificado público de VMware en el almacén de certificados Editores de confianza. El proceso de actualización del agente de administración utiliza un script de PowerShell que se firma con este certificado. Cuando finaliza la actualización, este certificado se elimina del almacén de certificados.

Requisitos previos

- Compruebe que ha seleccionado un método de descarga y que ha completado el procedimiento del método. Consulte [Descargar actualizaciones del dispositivo de vRealize Automation](#).
- Para todos los entornos de alta disponibilidad, consulte [Crear copias de seguridad del entorno de vRealize Automation existente](#).

- En entornos con equilibradores de carga, compruebe que ha deshabilitado todos los nodos redundantes y que ha eliminado los supervisores de estado. Para obtener más información, consulte la documentación del equilibrador de carga.
 - Dispositivo de vRealize Automation
 - Sitio web de IaaS
 - IaaS Manager Service
- En entornos con equilibradores de carga, compruebe que el tráfico se dirige solo al nodo principal.
- Realice los pasos siguientes para comprobar que el servicio de IaaS alojado en Microsoft Internet Information Services (IIS) está en ejecución:
 - a Inicie un navegador y escriba la URL **https://webhostname/Repository/Data/MetaModel.svc** para comprobar que se está ejecutando el repositorio web. Si es correcto, no se devolverán errores y verá una lista de modelos con formato XML.
 - b Inicie sesión en el sitio web de IaaS y compruebe que el archivo `Repository.Log` indica que el estado registrado es correcto. El archivo se encuentra en la carpeta de inicio de VCAC en `/Server/Model Manager Web/Logs/Repository.Log`.

Nota Para un sitio web de IaaS distribuido, inicie sesión en el sitio web secundario, sin MMD, y detenga Microsoft IIS temporalmente. Para asegurarse de que el tráfico del equilibrador de carga pasa únicamente por el nodo web principal, compruebe la conectividad de `MetaModel.svc` y reinicie Microsoft IIS.

- Compruebe que todos los nodos IaaS están en buen estado con los pasos siguientes:
 - a En el dispositivo virtual principal, inicie sesión en la administración de dispositivos de vRealize Automation como **raíz** con la contraseña que ha introducido al implementar el dispositivo de vRealize Automation.
 - b Seleccione **Configuración de vRA > Clúster**.
 - c En **Última conexión**, compruebe lo siguiente.
 - Los nodos de IaaS en la tabla tienen una hora de última conexión inferior a 30 segundos.
 - Los nodos del dispositivo virtual tienen una hora de última conexión inferior a 10 minutos.

Si no existe comunicación entre los nodos de IaaS y el dispositivo de vRealize Automation, se produce un error en la actualización.

Haga lo siguiente para diagnosticar problemas de conectividad entre el agente de administración y el dispositivo virtual.

- 1 Inicie sesión en cada nodo de IaaS que no aparezca o que tenga una hora de **Última conexión** superior a 30 segundos.
- 2 Compruebe los logs del agente de administración para ver si hay algún error registrado.
- 3 Si el agente de administración no se está ejecutando, reinícielo en la consola de servicios.

- d Observe si hay algún nodo huérfano en la tabla. Un nodo huérfano es un nodo duplicado del que se informa en el host pero que no existe en el host. Debe eliminar todos los nodos huérfanos. Para obtener más información, consulte [Eliminar nodos huérfanos en vRealize Automation](#).
- Si tiene un dispositivo virtual de réplica que ya no forme parte del clúster, debe eliminarlo de la tabla de clústeres. Si no elimina este dispositivo, el proceso de actualización muestra un mensaje de advertencia que indica que la actualización de réplica no ha podido llevarse a cabo.
- Compruebe que todas las solicitudes guardadas y en curso se hayan completado correctamente antes de la actualización.
- Si actualiza los componentes de IaaS manualmente después de actualizar el dispositivo de vRealize Automation 7.1, 7.2 o 7.3.x, consulte [Excluir la actualización de IaaS](#). Si tiene previsto actualizar IaaS manualmente, deberá detener también todos los servicios de IaaS (salvo el agente de administración) en cada nodo de IaaS.

Procedimiento

- 1 En el dispositivo de vRealize Automation principal, inicie sesión en la Administración de dispositivos de vRealize Automation como **raíz** con la contraseña que introdujo al implementar el dispositivo de vRealize Automation.

En un entorno distribuido, abra la consola de administración en el dispositivo principal.

- 2 Haga clic en **Servicios** y compruebe que se han registrado todos los servicios.
- 3 Seleccione **Configuración de vRA > Base de datos** y compruebe que se trata del dispositivo de vRealize Automation principal.

La actualización se instala solo en el dispositivo de vRealize Automation principal. Cada dispositivo de vRealize Automation de réplica se actualiza automáticamente junto con el dispositivo principal.

- 4 Seleccione **Actualizar > Estado**.
- 5 Haga clic en **Comprobar actualizaciones** para comprobar si hay alguna actualización accesible.
- 6 (opcional) Para las instancias del dispositivo de vRealize Automation, haga clic en **Detalles** en el área de versión de dispositivo para ver información sobre la ubicación de las notas de la versión.
- 7 Haga clic en **Instalar actualizaciones**.
- 8 Haga clic en **Aceptar**.

Aparece un mensaje que indica que hay una actualización en curso. El sistema muestra los cambios realizados durante una actualización en la página de resumen de la actualización. El tiempo necesario para que la actualización finalice depende del entorno y de la red.

- 9 (Opcional) Para supervisar la actualización con mayor detalle, utilice un emulador de terminal para iniciar sesión en el dispositivo principal. Consulte el archivo `updatecli.log` en `/opt/vmware/var/log/vami/updatecli.log`.

También se puede obtener información adicional sobre el progreso de la actualización en estos archivos.

- `/opt/vmware/var/log/vami/vami.log`
- `/var/log/vmware/horizon/horizon.log`
- `/var/log/bootstrap/*.log`

Si cierra sesión durante el proceso de actualización, puede seguir el progreso de la actualización en el archivo de log. El archivo `updatecli.log` puede mostrar información acerca de la versión de vRealize Automation desde la que está actualizando. La versión que se muestra cambia a la versión posterior adecuada durante el proceso de actualización.

- 10 Cuando finalice la actualización del dispositivo de vRealize Automation, haga clic en **Sistema > Reiniciar** en la consola de administración.

En un entorno distribuido, todos los nodos del dispositivo de réplica que se han actualizado correctamente se reinician cuando se reinicia el dispositivo principal.

La actualización de IaaS se inicia cuando el sistema se inicializa y todos los servicios están en funcionamiento. Haga clic en **Actualizar > Estado** para seguir de cerca el progreso de la actualización de IaaS.

- 11 Cuando la actualización de IaaS finalice, haga clic en **Clúster** en la consola de administración de dispositivos y confirme que el número de versión es la versión actual de todos los nodos y los componentes de IaaS.

- 12 Haga clic en **Telemetría** en la consola de administración del dispositivo. Lea la nota acerca de la participación en el Programa de mejora de la experiencia del cliente (CEIP) y decida si desea unirse o no al programa.

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>.

Para obtener más información sobre el programa de mejora de la experiencia del cliente, consulte [Unirse o abandonar el programa de mejora de la experiencia del cliente para vRealize Automation](#).

Pasos siguientes

Haga lo siguiente en caso de que se use un equilibrador de carga en la implementación.

- 1 Habilite las comprobaciones de estado de vRealize Automation del equilibrador de carga.
- 2 Vuelva a habilitar el tráfico del equilibrador de carga para todos los nodos de vRealize Automation.

Si los componentes de IaaS no se pueden actualizar, consulte [Actualizar los componentes de servidor de IaaS por separado cuando se produce un error en el proceso de actualización](#).

Actualizar los componentes de servidor de IaaS por separado cuando se produce un error en el proceso de actualización

Si se produce un error en el proceso de actualización automática, puede actualizar los componentes de IaaS por separado.

Si Manager Service y el sitio web de IaaS de vRealize Automation se actualizan correctamente, puede volver a ejecutar el script de actualización del shell de IaaS sin revertir a las snapshots que creó antes de la actualización. En ocasiones, un evento de reinicio pendiente generado al actualizar varios componentes de IaaS instalados en la misma máquina virtual puede ocasionar un error en la actualización. En este caso, intente reiniciar el nodo de IaaS manualmente y volver a ejecutar la actualización para solucionar el problema. Si se producen errores en la actualización de forma coherente, póngase en contacto con el soporte de VMware o intente realizar una actualización manual siguiendo los pasos que se indican a continuación.

- 1 Revierta el dispositivo de vRealize Automation a su estado previo a la actualización.
- 2 Ejecute un comando que excluya los componentes de IaaS del proceso de actualización. Consulte [Excluir la actualización de IaaS](#).
- 3 Ejecute el proceso de actualización en el dispositivo de vRealize Automation.
- 4 Actualice los componentes de IaaS por separado mediante el script de actualización de shell o el paquete msi del instalador de IaaS de vRealize Automation 7.4.

Actualizar los componentes de IaaS con el script de actualización del shell después de actualizar el dispositivo de vRealize Automation

Utilice el script de actualización del shell para actualizar los componentes de IaaS tras actualizar cada dispositivo de vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4.

El Dispositivo de vRealize Automation actualizado contiene un script de shell que sirve para actualizar cada nodo y componente de IaaS.

Puede ejecutar el script de actualización utilizando la consola de vSphere de la máquina virtual o utilizando una sesión de consola de SSH. Si utiliza la consola de vSphere, evitará problemas de conectividad de red intermitente que pueden interrumpir la ejecución del script.

Si detiene el script mientras está actualizando un componente, el script se detiene cuando finalice la actualización del componente. Si aún deben actualizarse otros componentes en el nodo, puede volver a ejecutar el script.

Cuando la actualización finalice, puede revisar el resultado de la actualización abriendo el archivo de log de actualización en `/opt/vmware/var/log/vami/upgrade-iaas.log`.

Requisitos previos

- Revise [Solucionar problemas de actualización de vRealize Automation](#).
- Compruebe que la actualización de todos los dispositivos de vRealize Automation se haya realizado correctamente.

- Si reinicia un servidor de IaaS después de actualizar todos los dispositivos de vRealize Automation, pero antes de actualizar los componentes de IaaS, detenga todos los servicios de IaaS en Windows, excepto el servicio de agente de administración.
- Antes de ejecutar el script de actualización de shell en el nodo principal de dispositivos de vRealize Automation, haga clic en **Servicios** en la consola de administración del dispositivo. Compruebe que todos los servicios, excepto `iaas-service`, tienen un estado REGISTRADO.
- Complete estos pasos para instalar el agente de administración de IaaS manualmente en cada nodo de IaaS.
 - a Abra el navegador y vaya a la página de instalación de IaaS de VMware vRealize Automation en el dispositivo, en `https://virtual_appliance_host_FQDN:5480/installer`.
 - b Descargue el instalador del agente de administración, `vCAC-iaasManagementAgent-Setup.msi`.
 - c Inicie sesión en cada máquina de IaaS de vRealize Automation y actualice el agente de administración con el instalador del agente de administración. Reinicie el servicio de agente de administración de Windows.
- Compruebe que el nodo de Model Manager y de sitio web de IaaS principal tiene instalado JAVA SE Runtime Environment 8, actualización 161 (64 bits) o posterior. Después de instalar Java, debe establecer la variable de entorno, `JAVA_HOME`, en la nueva versión en cada uno de los nodos de servidor.
- Inicie sesión en cada nodo del sitio web de IaaS y compruebe que la fecha de creación es anterior a la fecha de modificación del archivo `web.config`. Si la fecha de creación del archivo `web.config` es igual o posterior a la fecha de modificación, realice el procedimiento descrito en [Error en la actualización para el componente de sitio web de IaaS](#).
- Haga lo siguiente en cada nodo de IaaS para comprobar que en todos ellos hay un agente de administración actualizado de IaaS:
 - a Inicie sesión en la consola de administración del dispositivo de vRealize Automation.
 - b Seleccione **Configuración de vRA > Clúster**.
 - c Amplíe la lista de todos los componentes instalados en cada nodo de IaaS y localice el agente de administración de IaaS.
 - d Compruebe que la versión del agente de administración esté actualizada.
- [Excluir la actualización de IaaS](#).
- Compruebe que se puede acceder a la copia de seguridad de la base de datos Microsoft SQL Server de IaaS en caso de que necesite revertir los datos.
- Compruebe que los snapshots de los servidores de IaaS de la implementación estén disponibles.

Si la actualización no se ha realizado correctamente, regrese al snapshot y la copia de seguridad de la base de datos e intente realizar otra actualización.

Procedimiento

- 1 Abra una nueva sesión de consola en el host de Dispositivo de vRealize Automation. Inicie sesión con la cuenta raíz.
- 2 Cambie los directorios a `/usr/lib/vcac/tools/upgrade/`.

Es importante que todos los agentes de administración de IaaS estén actualizados y en buen estado antes de ejecutar el script de shell `./upgrade`. Si algún agente de administración de IaaS tiene un problema cuando se ejecuta el script para actualizar el shell, consulte [La actualización no puede actualizar al agente de administración](#).

- 3 Ejecute el script de actualización.
 - a En el símbolo del sistema, introduzca `./upgrade`.
 - b Pulse Entrar.

Para obtener una descripción del proceso de actualización de IaaS, consulte [Actualizar componentes de IaaS y dispositivo de vRealize Automation](#).

Si el script de actualización del shell no se ejecuta correctamente, revise el archivo `upgrade-iaas.log`.

Puede volver a ejecutar el script de actualización tras resolver un problema.

Pasos siguientes

- 1 [Restaurar el acceso al centro de control integrado de vRealize Orchestrator](#).
- 2 Si la implementación utiliza un equilibrador de carga, vuelva a habilitar los supervisores de estado de vRealize Automation y el tráfico a todos los nodos.

Para obtener más información, consulte *Equilibrio de carga de vRealize Automation*.

Actualizar componentes de IaaS con el archivo ejecutable del instalador de IaaS después de actualizar el dispositivo de vRealize Automation

Este método alternativo se puede utilizar para actualizar los componentes de IaaS después de actualizar el dispositivo de vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4.

Descargar el instalador de IaaS para actualizar los componentes de IaaS después de actualizar el dispositivo de vRealize Automation

Después de actualizar el dispositivo de vRealize Automation a la versión 7.4, descargue el instalador de IaaS en la máquina en la que están instalados los componentes de IaaS que desea actualizar.

Si aparecen advertencias de certificado durante el procedimiento, puede ignorarlos.

Nota Durante el proceso de actualización, el tipo de inicio de todos los servicios debe establecerse en Automático, excepto para las instancias de copia de seguridad pasiva de Manager Service. Si establece los servicios como Manual, se producirá un error en el proceso de actualización.

Requisitos previos

- Confirme que Microsoft .NET Framework 4.5.2 o una versión posterior esté instalado en la máquina de instalación de IaaS. El instalador de .NET se puede descargar de la página web del instalador de vRealize Automation. Si actualiza .NET a 4.5.2 después de desconectar los servicios y la máquina se reinicia como parte del proceso de instalación, deberá detener todos los servicios de IaaS excepto el agente de administración.
- Si usa Internet Explorer para la descarga, asegúrese de que la configuración de seguridad mejorada no está habilitada. Escriba `res://iesetup.dll/SoftAdmin.htm` en la barra de búsqueda y pulse Entrar.
- Inicie sesión como administrador local en el servidor de Windows en el que están instalados uno o más componentes de IaaS que desea actualizar.

Procedimiento

- 1 Inicie un navegador web.
- 2 Escriba la URL de la página de descarga del instalador de Windows.

Por ejemplo, `https://vcac-va-hostname.domain.name:5480/installer`, donde `vcac-va-hostname.domain.name` es el nodo principal de Dispositivo de vRealize Automation.

- 3 Haga clic en el vínculo **Instalador de IaaS**.
- 4 Cuando se le pida, guarde el archivo del instalador (`setup__vcac-va-hostname.domain.name@5480.exe`) en el escritorio.

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

Pasos siguientes

[Actualizar los componentes de IaaS después de actualizar vRealize Automation 7.1 o 7.2 a 7.3.](#)

Actualizar los componentes de IaaS después de actualizar vRealize Automation 7.1 o 7.2 a 7.3

Debe actualizar la base de datos de SQL y configurar todos los sistemas que tienen componentes de IaaS instalados. Puede usar estos pasos para instalaciones mínimas y distribuidas.

Nota El instalador de IaaS debe estar en la máquina que contiene los componentes de IaaS que desea actualizar. El instalador no se puede ejecutar desde una ubicación externa, excepto en el caso de la base de datos Microsoft SQL, que también se puede actualizar de forma remota desde el nodo web.

Compruebe que los snapshots de los servidores de IaaS de la implementación estén disponibles. Si la actualización no se realiza correctamente, puede volver al snapshot e intentar otra actualización.

Realice la actualización de forma que los servicios se actualicen en el siguiente orden:

- 1 Sitios Web de IaaS

Si está utilizando un equilibrador de carga, deshabilite el tráfico en todos los nodos no principales.

Finalice la actualización en un servidor antes de actualizar el siguiente servidor que esté ejecutando un servicio de sitio web. Empiece con el que tenga instalado el componente de datos de Model Manager.

Si realiza una actualización externa de la base de datos Microsoft SQL, deberá actualizar el SQL externo antes de actualizar el nodo web. Puede actualizar el SQL externo de forma remota desde el nodo web.

2 Manager Service

Actualice el servicio del administrador activo antes de actualizar el servicio del administrador pasivo.

Si el cifrado SSL no está habilitado en su instancia de SQL, desactive la casilla de verificación de cifrado SSL que se encuentra junto a la definición SQL en el cuadro de diálogo de configuración de la actualización de IaaS.

3 Orquestador de DEM y trabajos

Actualice todas las orquestaciones DEM y los trabajos. Finalice la actualización en un servidor antes de actualizar el siguiente servidor.

4 Agentes

Finalice la actualización en un servidor antes de actualizar el siguiente servidor que esté ejecutando un agente.

5 Agente de administración

Se actualiza automáticamente como parte del proceso de actualización.

Si está utilizando servicios diferentes en un servidor, la actualización actualiza los servicios en el orden correcto. Por ejemplo, si su sitio tiene un sitio web y servicios del administrador en el mismo servidor, seleccione ambos para la actualización. El instalador de actualización aplica las actualizaciones en el orden correcto. Debe completar la actualización en un servidor antes de iniciar una actualización en otro.

Nota Si su implementación utiliza un equilibrador de carga, el dispositivo principal debe estar conectado al equilibrador de carga. Todas las demás instancias de dispositivos de Dispositivo de vRealize Automation deben deshabilitarse para el tráfico del equilibrador de carga antes de la actualización para evitar errores de almacenamiento en caché.

Requisitos previos

- Realice una copia de seguridad del entorno de vRealize Automation existente.
- Si reinicia un servidor de IaaS después de actualizar todos los dispositivos de vRealize Automation, pero antes de actualizar los componentes de IaaS, detenga todos los servicios de Windows de IaaS en el servidor, excepto el servicio de agente de administración.
- [Descargar el instalador de IaaS para actualizar los componentes de IaaS después de actualizar el dispositivo de vRealize Automation.](#)

- Compruebe que su principal sitio web de IaaS, la base de datos de Microsoft SQL y el nodo de Model Manager tienen JAVA SE Runtime Environment 8, 64 bits, actualización 111 o una versión posterior instalada. Después de instalar Java, debe establecer la variable de entorno, JAVA_HOME, en la nueva versión en cada uno de los nodos de servidor.
- Compruebe que la fecha de creación sea anterior a la fecha de modificación del archivo web.config. Si la fecha de creación del archivo web.config es igual o posterior a la fecha de modificación, realice el procedimiento descrito en [Error en la actualización para el componente de sitio web de IaaS](#).
- Siga estos pasos para reconfigurar el Coordinador de transacciones distribuidas (DTC) de Microsoft.

Nota Incluso con el Coordinador de transacciones distribuidas habilitado, las transacciones distribuidas podrían no realizarse si el firewall está activado.

- a En el dispositivo de vRealize Automation, seleccione **Inicio > Herramientas administrativas > Servicios de componentes**.
- b Expanda **Servicios de componentes > Equipos > Mi PC > Coordinador de transacciones distribuidas**.
- c Elija la tarea correspondiente.
 - En el caso de un DTC independiente local, haga clic con el botón secundario en **DTC local** y seleccione **Propiedades**.
 - En el caso de un DTC agrupado, expanda **DTC agrupados**, haga clic con el botón secundario en el DTC agrupado con el nombre y seleccione **Propiedades**.
- d Haga clic en **Seguridad**.
- e Seleccione todas estas opciones.
 - **Acceso a DTC desde la red**
 - **Permitir clientes remotos**
 - **Permitir entrantes**
 - **Permitir salientes**
 - **Se requiere autenticación mutua**
- f Haga clic en **Aceptar**.

Procedimiento

- 1 Si está utilizando un equilibrador de carga, prepare su entorno.
 - a Compruebe que el nodo del sitio web de IaaS que contiene los datos de Model Manager esté habilitado para el tráfico del equilibrador de carga.

Puede identificar este nodo por la presencia de la carpeta `vCAC Folder\Server\ConfigTool`.
 - b Deshabilite los demás sitios web de IaaS y los servicios del administrador no principales para el tráfico del equilibrador de carga.

- 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 Escriba las credenciales del administrador para la implementación actual en la página de inicio de sesión.

El nombre de usuario es **root** y la contraseña es la que especificó al implementar el dispositivo.

- 6 Seleccione **Aceptar certificado**.
- 7 En la página **Tipo de instalación**, compruebe que se haya seleccionado **Actualizar**.
Si no se ha seleccionado **Actualizar**, los componentes de este sistema ya están actualizados para esta versión.
- 8 Haga clic en **Siguiente**.
- 9 Configure las opciones de actualización.

| Opción | Acción |
|--|--|
| Si está actualizando los datos de Model Manager | Active la casilla Datos de Model Manager en la sección del Servidor vCAC. La casilla de verificación está activada de forma predeterminada. Actualice los datos de Model Manager solo una vez. Si está ejecutando el archivo de configuración en varias máquinas para actualizar una instalación distribuida, los servidores web dejan de funcionar mientras hay una discrepancia de versión entre los servidores web y los datos de Model Manager. Cuando haya actualizado los datos de Model Manager y de los servidores web, todos los servidores web deberían funcionar. |
| Si no está actualizando los datos de Model Manager | Desactive la casilla Datos de Model Manager en la sección del Servidor vCAC. |
| Para preservar los flujos de trabajo personalizados como versión más reciente de los datos de Model Manager | Si está actualizando los datos de Model Manager, active la casilla Preservar mis versiones más recientes del flujo de trabajo en la sección de Flujos de trabajo de extensibilidad. La casilla de verificación está activada de forma predeterminada. Los flujos de trabajo personalizados siempre se preservan. La casilla solo determina el orden de la versión. Si ha utilizado vRealize Automation Designer para personalizar flujos de trabajo en Model Manager, seleccione esta opción para mantener la versión más reciente de cada flujo de trabajo personalizado antes de actualizar como la versión más reciente tras la actualización. Si no selecciona esta opción, la versión de cada flujo de trabajo proporcionado con vRealize Automation Designer se convierte en la más reciente tras la actualización y la versión más reciente antes de la actualización se convierte en la segunda más reciente. Para obtener información sobre vRealize Automation Designer, consulte Ampliar el ciclo de vida de la máquina usando vRealize Automation Designer . |
| Si está actualizando un Distributed Execution Manager o un agente de proxy | Introduzca las credenciales para la cuenta del administrador en la sección de Cuenta de servicio. Todos los servicios que actualiza se ejecutan en esta cuenta. |

| Opción | Acción |
|--|--|
| Para especificar su base de datos de Microsoft SQL Server | <p>Si está actualizando datos de Model Manager, introduzca los nombres del servidor de la base de datos y la instancia de la base de datos en el cuadro de texto Servidor en la sección de Información de instalación de la base de datos de Microsoft SQL Server. Introduzca un nombre de dominio completo (FQDN) para el nombre del servidor de la base de datos en el cuadro de texto Nombre de base de datos.</p> <p>Si la instancia de la base de datos está en un puerto SQL no predeterminado, incluya el número de puerto en la especificación de la instancia del servidor. El número de puerto predeterminado de Microsoft SQL es 1433.</p> <p>Cuando se actualizan los nodos del administrador, la opción SSL de MSSQL está seleccionada de forma predeterminada. Si la base de datos no utiliza SSL, desactive la opción Usar SSL para la conexión de la base de datos.</p> |

10 Haga clic en **Siguiente**.

11 Confirme que todos los servicios que se deben actualizar aparecen en la página Preparado para actualizar y haga clic en **Actualizar**.

Aparecerá la página Actualizando y un indicador de progreso. Cuando finalice el proceso de actualización, se habilitará el botón **Siguiente**.

12 Haga clic en **Siguiente**.

13 Haga clic en **Finalizar**.

14 Compruebe que se hayan reiniciado todos los servicios.

15 Repita estos pasos para cada servidor de IaaS en su implementación en el orden recomendado.

16 Cuando se hayan actualizado todos los componentes, inicie sesión en la consola de administración para el dispositivo y compruebe que todos los servicios, incluido IaaS, estén registrados ahora.

17 (Opcional) Habilite la conmutación por error automática de Manager Service. Consulte [Habilitar la conmutación por error automática de Manager Service después de actualizar](#).

Todos los componentes seleccionados se actualizan a la nueva versión.

Pasos siguientes

1 [Restaurar el acceso al centro de control integrado de vRealize Orchestrator](#).

2 Si la implementación utiliza un equilibrador de carga, actualice cada nodo del equilibrador de carga para que use las comprobaciones de estado de vRealize Automation y vuelva a habilitar el tráfico del equilibrador de carga para cualquier nodo desconectado.

Para obtener más información, consulte *Equilibrio de carga de vRealize Automation*.

Restaurar el acceso al centro de control integrado de vRealize Orchestrator

Después de actualizar los componentes del servidor de IaaS, debe restaurar el acceso a vRealize Orchestrator.

Cuando se actualiza de vRealize Automation 7.3 y versiones anteriores a la versión 7.4, debe realizar este procedimiento para incorporar la nueva característica de control de acceso basado en funciones. Este procedimiento se aplica a un entorno de alta disponibilidad.

Requisitos previos

Cree un snapshot del entorno vRealize Automation.

Procedimiento

1 Inicie sesión en la consola de administración de Dispositivo de vRealize Automation como usuario raíz utilizando el nombre de dominio totalmente cualificado de host del dispositivo, `https://va-hostname.domain.name:5480`.

2 Seleccione **Configuración de vRA > Base de datos**.

3 Identifique los nodos principal y de réplica.

4 En cada nodo de réplica, abra una sesión de SSH, inicie sesión como administrador y ejecute el siguiente comando:

```
service vco-server stop && service vco-configurator stop
```

5 En el nodo principal, abra una sesión de SSH, inicie sesión como administrador y ejecute el siguiente comando:

```
rm /etc/vco/app-server/vco-registration-id
```

6 En el nodo principal, cambie los directorios a `/etc/vco/app-server/`.

7 Abra el archivo `sso.properties`.

8 Si el nombre de la propiedad `com.vmware.o11n.sso.admin.group.name` contiene espacios o cualquier otro carácter Bash que se pueda aceptar como un carácter especial en un comando Bash, como un apóstrofo (') o un signo de dólar (\$), siga estos pasos.

a Copie la línea con la propiedad `com.vmware.o11n.sso.admin.group.name` e introduzca `AdminGroup` para el valor.

b Añada `#` al comienzo de la línea original con la propiedad `com.vmware.o11n.sso.admin.group.name` para comentar la línea.

c Guarde y cierre el archivo `sso.properties`.

9 Ejecute este comando:

```
vcac-vami vco-service-reconfigure
```

10 Abra el archivo `sso.properties`. Si el archivo ha cambiado, siga estos pasos.

a Quite el `#` del principio de la línea original con la propiedad `com.vmware.o11n.sso.admin.group.name` para eliminar el comentario de la línea.

b Elimine la copia de la línea con la propiedad `com.vmware.o11n.sso.admin.group.name`.

c Guarde y cierre el archivo `sso.properties`.

11 Ejecute este comando para reiniciar el servicio vco-server:

```
service vco-server restart
```

12 Ejecute este comando para reiniciar el servicio vco-configurator:

```
service vco-configurator restart
```

13 En la consola de administración de Dispositivo de vRealize Automation, haga clic en **Servicios** y espere hasta que todos los servicios del nodo principal estén REGISTRADOS.

14 Una vez que todos los servicios estén registrados, una los nodos de réplica de vRealize Automation al clúster de vRealize Automation para sincronizar la configuración de vRealize Orchestrator. Para obtener información, consulte [Reconfigurar la instancia integrada de vRealize Orchestrator para admitir la alta disponibilidad](#).

Pasos siguientes

[Actualizar vRealize Orchestrator tras actualizar vRealize Automation](#).

Actualizar vRealize Orchestrator tras actualizar vRealize Automation

Debe actualizar la instancia de vRealize Orchestrator cuando actualice vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4.

Con la publicación de vRealize Orchestrator 7.4, tiene dos opciones para actualizar vRealize Orchestrator cuando actualiza a vRealize Automation 7.4.

- Puede migrar el servidor externo de vRealize Orchestrator existente a la instancia de vRealize Orchestrator integrada que se incluye en vRealize Automation 7.4.
- Puede actualizar el servidor de vRealize Orchestrator independiente o en clúster para que funcione con vRealize Automation 7.4.

Migrar un servidor externo de vRealize Orchestrator a vRealize Automation

Puede migrar el servidor externo de vRealize Orchestrator existente a una instancia de vRealize Orchestrator integrada en vRealize Automation 7.4.

Puede implementar vRealize Orchestrator como instancia externa de servidor y configurar vRealize Automation para que funcione con esa instancia externa; también puede configurar y utilizar el servidor de vRealize Orchestrator que se incluye en Dispositivo de vRealize Automation.

VMware le recomienda que migre su vRealize Orchestrator externo al servidor de Orchestrator que está integrado en vRealize Automation. La migración de una instancia externa al Orchestrator integrado proporciona las siguientes ventajas:

- Reduce el coste total de propiedad.
- Simplifica el modelo de implementación.

- Mejora la eficiencia operativa.

Nota Considere utilizar un vRealize Orchestrator externo en los casos siguientes:

- Varios arrendatarios en el entorno de vRealize Automation
- Entorno geográficamente disperso
- Manejo de la carga de trabajo
- Uso de complementos específicos, como versiones anteriores del complemento de Site Recovery Manager Plug-in

Diferencias del Centro de control entre Orchestrator externo e integrado

Algunos de los elementos de menú que están disponibles en el Centro de control de un vRealize Orchestrator externo no se incluyen en la vista predeterminada del Centro de control correspondiente a una instancia de Orchestrator integrado.

En el Centro de control del servidor de Orchestrator integrado, algunas opciones están ocultas de forma predeterminada.

| Elemento de menú | Detalles |
|---|---|
| Licencias | El Orchestrator integrado está preconfigurado para usar vRealize Automation como proveedor de licencias. |
| Exportar o importar configuración | La configuración de Orchestrator integrado se incluye en los componentes de vRealize Automation exportados. |
| Configurar base de datos | El Orchestrator integrado utiliza la misma base de datos que vRealize Automation. |
| Programa de mejora de la experiencia de cliente | Puede unirse al Programa de mejora de la experiencia de cliente (CEIP) desde la interfaz de administración de dispositivos de vRealize Automation. Consulte <i>el Programa de mejora de la experiencia de cliente en Administración de vRealize Automation</i> . |

Otras opciones que están ocultas en la vista predeterminada del Centro de control son el cuadro de texto de la **dirección del host** y el botón de **cancelación de registro** de la página **Configurar proveedor de autenticación**.

Nota Para conocer todas las opciones del Centro de control de vRealize Orchestrator incorporadas en vRealize Automation, debe acceder a la página de administración avanzada de Orchestrator en la dirección https://vra-va-hostname.dominio.nombre_o_dirección_del_equilibrador_de_carga:8283/vco-controlcenter/#!/?advanced y hacer clic en el botón F5 del teclado para actualizar la página.

Migrar un vRealize Orchestrator 7.x externo a vRealize Automation 7.4

Puede exportar la configuración de la instancia externa de Orchestrator e importarla al servidor de Orchestrator que está integrado en vRealize Automation.

Nota Si tiene varios nodos de Dispositivo de vRealize Automation, realice el procedimiento de migración únicamente en el nodo principal de vRealize Automation.

Requisitos previos

- Actualice su vRealize Automation a la versión 7.4. Para obtener más información, consulte *Actualización de vRealize Automation en Instalación o actualización de vRealize Automation*.
- Detenga el servicio del servidor de Orchestrator del Orchestrator externo.
- Haga una copia de seguridad de la base de datos, incluido el esquema de base de datos, del servidor externo de Orchestrator.

Procedimiento

- 1 Exporte la configuración del servidor externo de Orchestrator.
 - a Inicie sesión en el centro de control del servidor externo de Orchestrator como **raíz** o como **administrador**, según la versión de origen.
 - b Detenga el servicio del servidor de Orchestrator desde la página **Opciones de inicio** para prevenir cambios no deseados en la base de datos.
 - c Vaya a la página **Exportar o importar configuración**.
 - d En la página **Exportar configuración**, seleccione **Exportar configuración de servidor**, **Empaquetar complementos** y **Exportar configuraciones de complementos**.

- 2 Migre la configuración exportada a la instancia integrada de Orchestrator.
 - a Cargue el archivo de configuración de Orchestrator exportado en el directorio `/usr/lib/vco/tools/configuration-cli/bin` de Dispositivo de vRealize Automation.
 - b Inicie sesión en Dispositivo de vRealize Automation sobre SSH como **raíz**.
 - c Detenga el servicio del servidor de Orchestrator y el servicio del centro de control del servidor integrado de vRealize Orchestrator.

```
service vco-server stop && service vco-configurator stop
```

- d Importe el archivo de configuración de Orchestrator en el servidor integrado de vRealize Orchestrator; para ello, ejecute el script `vro-configure` con el comando `import`.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-  
IP_dispositivo_orchestrator-fecha_hora.zip
```

- 3 Si el servidor externo de Orchestrator desde el que desea migrar utiliza la base de datos integrada de PostgreSQL, edite los archivos de configuración de la base de datos.
 - a En el archivo `/var/vmware/vpostgres/current/pgdata/postgresql.conf`, quite la marca de comentario de la línea `listen_addresses`.
 - b Establezca los valores de `listen_addresses` con un carácter comodín (*).

```
listen_addresses = '*'
```

- c Anexe una línea al archivo `/var/vmware/vpostgres/current/pgdata/pg_hba.conf`.

```
host all all vra-va-ip-address/32 md5
```

Nota El archivo `pg_hba.conf` requiere el uso de un formato de prefijo CIDR en lugar de una dirección IP y una máscara de subred.

- d Reinicie el servicio del servidor de PostgreSQL.

```
service vpostgres restart
```

- 4 Migre la base de datos a la base de datos interna de PostgreSQL; para ello, ejecute el script `vro-configure` con el comando `db-migrate`.

```
./vro-configure.sh db-migrate --sourceJdbcUrl URL_conexión_JDBC --sourceDbUsername usuario_base_datos --sourceDbPassword contraseña_usuario_base_datos
```

Nota Ponga las contraseñas que contienen caracteres especiales entre comillas simples.

La `URL_conexión_JDBC` depende del tipo de base de datos que utiliza.

```
PostgreSQL: jdbc:postgresql://host:puerto/nombre_base_datos
```

```
MSSQL: jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\; if using SQL authentication and
MSSQL: jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\;domain=dominio\;useNTLMv2=TRUE if
using Windows authentication.
```

```
Oracle: jdbc:oracle:thin:@host:puerto:nombre_base_datos
```

La información de inicio de sesión a la base de datos predeterminada es:

| | |
|---|--------|
| <code>nombre_de_base_de_datos</code> | vmware |
| <code>usuario_de_base_de_datos</code> | vmware |
| <code>contraseña_de_usuario_de_base_de_datos</code> | vmware |

- 5 Elimine todos los certificados del almacén de claves de la base de datos.

```
./vro-configuration.sh untrust --reset-db
```

- 6 Reinstale los complementos de Orchestrator.
 - a Inicie sesión en el centro de control como **raíz**.
 - b Haga clic en **Solución de problemas**.
 - c Haga clic en **Forzar reinstalación de complementos**.
- 7 Inicie el servicio del servidor de Orchestrator.

- 8 Regrese a la configuración predeterminada de los archivos `postgresql.conf` y `pg_hba.conf`.
 - a Reinicie el servicio del servidor de PostgreSQL.

Ha migrado correctamente una instancia externa del servidor de Orchestrator a una instancia de vRealize Orchestrator integrada en vRealize Automation.

Pasos siguientes

Configure el servidor integrado de vRealize Orchestrator. Consulte [Configure el servidor integrado de vRealize Orchestrator](#).

Configure el servidor integrado de vRealize Orchestrator

Después de exportar la configuración de un servidor externo de Orchestrator e importarla a vRealize Automation 7.4, debe configurar el servidor de Orchestrator integrado en vRealize Automation.

Requisitos previos

Migre la configuración del vRealize Orchestrator externo al interno.

Procedimiento

- 1 Inicie sesión en Dispositivo de vRealize Automation sobre SSH como **raíz**.
- 2 Inicie el servicio del centro de control y el servicio del servidor de Orchestrator en el servidor de vRealize Orchestrator integrado.

```
service vco-configurator start && service vco-server start
```

- 3 Inicie sesión en el centro del control del servidor integrado de Orchestrator como **administrador**.

Nota Si migra desde una instancia externa de vRealize Orchestrator 7.4, vaya directamente al paso 5.

- 4 Compruebe que Orchestrator esté configurado correctamente en la página **Validar configuración** del centro de control.
- 5 Si el Orchestrator externo se configuró para funcionar en modo de clúster, vuelva a configurar el clúster de Orchestrator en vRealize Automation.
 - a Diríjase a la página avanzada de **Administración de clústeres de Orchestrator** en `https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#/control-app/ha?remove-nodes`.

Nota Si no aparecen las casillas de verificación **Quitar** junto a los nodos existentes en el clúster, debe actualizar la página del navegador haciendo clic en el botón F5 del teclado.

- b Seleccione las casillas de verificación junto a los nodos de Orchestrator externos y haga clic en **Quitar** para excluirlos del clúster.

- c Para salir de la página de administración avanzada de clústeres, elimine la cadena de remove-nodes de la URL y actualice la página del navegador haciendo clic en el botón F5 del teclado.
- d En la página **Validar configuración** del centro de control, compruebe que Orchestrator está configurado correctamente.
- 6 (opcional) En la pestaña **Certificado de firma del paquete** de la página **Certificados**, genere un nuevo certificado de firma del paquete.
- 7 (opcional) Cambie los valores del **Arrendatario predeterminado** y del **Grupo de administradores** en la página **Configurar proveedor de autenticación**.
- 8 Compruebe que el servicio de vco-server aparece como REGISTRADO en la pestaña **Servicios** de la consola de administración de Dispositivo de vRealize Automation.
- 9 Seleccione los servicios de vco del servidor externo de Orchestrator y haga clic en **Eliminar del registro**.

Pasos siguientes

- Importe todos los certificados de confianza del servidor de Orchestrator externo al almacén de confianza del Orchestrator integrado.
- Una los nodos de réplica de vRealize Automation al clúster de vRealize Automation para sincronizar la configuración de Orchestrator.

Para obtener más información, consulte *Volver a configurar el vRealize Orchestrator integrado de destino para propiciar alta disponibilidad en la Instalación o actualización de vRealize Automation*.

Nota Las instancias de vRealize Orchestrator se agrupan en clústeres automáticamente y están disponibles para usarse.

- Reinicie el servicio de vco-configurator en todos los nodos del clúster.
- Actualice el terminal de vRealize Orchestrator para que apunte al servidor de Orchestrator integrado que se migró.
- Agregue el host de vRealize Automation y de IaaS al inventario del complemento vRealize Automation mediante la ejecución de los flujos de trabajo Añadir un host de vRA y Añadir un host de IaaS.

Actualizar un dispositivo independiente de vRealize Orchestrator para su uso con vRealize Automation

Si mantiene una instancia externa independiente de vRealize Orchestrator para usarla con vRealize Automation, deberá actualizar vRealize Orchestrator cuando actualice vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4.

Las instancias integradas de vRealize Orchestrator se actualizan como parte de la actualización del dispositivo de vRealize Automation. No hay que realizar ninguna otra acción para una instancia integrada.

Si va a actualizar un clúster de dispositivo de vRealize Orchestrator, consulte [Actualizar un clúster de dispositivo de vRealize Orchestrator para usarlo con vRealize Automation 7.4](#).

Requisitos previos

- [Instalar la actualización en los componentes de IaaS y el dispositivo de vRealize Automation](#).
- Desmonte todos los sistemas de archivos de red. Consulte *Administración de máquinas virtuales de vSphere* en la documentación de vSphere.
- Aumente la memoria del dispositivo de vSphere Orchestrator hasta por lo menos 6 GB. Consulte *Administración de máquinas virtuales de vSphere* en la documentación de vSphere.
- Tome un snapshot de la máquina virtual de vSphere Orchestrator. Consulte *Administración de máquinas virtuales de vSphere* en la documentación de vSphere.
- Si utiliza una base de datos externa, cree una copia de seguridad de la misma.
- Si utiliza la base de datos preconfigurada de PostgreSQL en vSphere Orchestrator, cree una copia de seguridad de la base de datos a través del menú **Exportar base de datos** del centro de control de vSphere.

Procedimiento

- ◆ Utilice uno de los métodos que se describen para actualizar su vRealize Orchestrator independiente.
 - [Actualizar Orchestrator Appliance mediante el repositorio predeterminado de VMware](#).
 - [Actualizar Orchestrator Appliance con una imagen ISO](#).
 - [Actualizar Orchestrator Appliance con un repositorio específico](#).

Actualizar Orchestrator Appliance mediante el repositorio predeterminado de VMware

Puede configurar Orchestrator para que descargue el paquete de actualización desde el repositorio predeterminado de VMware.

Requisitos previos

- Desmonte todos los sistemas de archivos de red. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente la memoria de Orchestrator Appliance hasta por lo menos 6 GB. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente el tamaño del disco de la máquina virtual de vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Asegúrese de que la partición raíz de Orchestrator Appliance tenga al menos 3 GB de espacio libre disponible. Para obtener más información sobre cómo aumentar el tamaño de una partición de disco, consulte el artículo de la base de conocimientos 1004071: <http://kb.vmware.com/kb/1004071>.
- Tome una snapshot de la máquina virtual de Orchestrator. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.

- Si utiliza una base de datos externa, cree una copia de seguridad de la misma.
- Si utiliza la base de datos preconfigurada en Orchestrator PostgreSQL, cree una copia de seguridad de la base de datos desde el menú **Exportar base de datos** del centro de control.

Procedimiento

- 1 Acceda a la Interfaz de administración de dispositivos virtuales (VAMI) en https://servidor_orchestrator:5480 e inicie sesión como **raíz**.
- 2 En la pestaña **Actualizar**, haga clic en **Configuración**.
Se selecciona el botón de opción junto a **Usar repositorio predeterminado**.
- 3 En la página **Estado**, haga clic en **Buscar actualizaciones**.
- 4 Si hay actualizaciones disponibles, haga clic en **Instalar actualizaciones**.
- 5 Acepte el contrato de licencia del usuario final de VMware y confirme que desea instalar la actualización.
- 6 Para completar la actualización, reinicie Orchestrator Appliance.
 - a Inicie sesión de nuevo en la Interfaz de administración de dispositivos virtuales (VAMI) como **raíz**.
- 7 (opcional) En la pestaña **Actualizar**, compruebe que se haya instalado correctamente la última versión del Orchestrator Appliance.
- 8 Inicie sesión en el centro de control como **raíz**.
- 9 Si tiene pensado crear un clúster de las instancias de Orchestrator, vuelva a configurar la configuración de los hosts.
 - a En la página **Configuración de hosts** del centro de control, haga clic en **CAMBIAR**.
 - b Introduzca el nombre del host del servidor del equilibrador de carga en lugar del nombre de Orchestrator Appliance de vRealize.

10 Vuelva a configurar la autenticación.

- a Si, antes de la actualización, el servidor de Orchestrator se configuró para que usara **LDAP** o **SSO (heredado)** como método de autenticación, configure **vSphere** o **vRealize Automation** como proveedor de autenticación.
- b Si la autenticación ya está establecida en **vSphere** o **vRealize Automation**, elimine la configuración del registro y vuelva a registrarla.

Nota Si, antes de la actualización, su instancia de Orchestrator ha utilizado **vSphere** como proveedor de autenticación y se ha configurado para conectarse al nombre de dominio completo o la dirección IP de vCenter Server, en caso de que tenga una instancia externa de Platform Services Controller, después de la actualización debe configurar Orchestrator para que se conecte al nombre de dominio completo o la dirección IP de la instancia de Platform Services Controller que contiene la instancia de vCenter Single Sign-On. También debe importar manualmente a Orchestrator los certificados de todas las instancias de Platform Services Controller que compartan el mismo dominio de vCenter Single Sign-On.

Ha actualizado correctamente Orchestrator Appliance.

Pasos siguientes

Compruebe que Orchestrator esté configurado correctamente en la página **Validar configuración** del centro de control.

Actualizar Orchestrator Appliance con una imagen ISO

Puede configurar Orchestrator para que descargue el paquete de actualización desde un archivo de imagen ISO montado en la unidad de CD-ROM del dispositivo.

Requisitos previos

- Desmonte todos los sistemas de archivos de red. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente la memoria de Orchestrator Appliance hasta por lo menos 6 GB. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente el tamaño del disco de la máquina virtual de vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Asegúrese de que la partición raíz de Orchestrator Appliance tenga al menos 3 GB de espacio libre disponible. Para obtener más información sobre cómo aumentar el tamaño de una partición de disco, consulte el artículo de la base de conocimientos 1004071: <http://kb.vmware.com/kb/1004071>.
- Tome una snapshot de la máquina virtual de Orchestrator. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Si utiliza una base de datos externa, cree una copia de seguridad de la misma.

- Si utiliza la base de datos preconfigurada en Orchestrator PostgreSQL, cree una copia de seguridad de la base de datos desde el menú **Exportar base de datos** del centro de control.

Procedimiento

- 1 Descargue el archivo VMware-vR0-Appliance-versión-número_compilación-updaterepo.iso del sitio oficial de descargas de VMware.
- 2 Conecte la unidad de CD-ROM de la máquina virtual de Orchestrator Appliance. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- 3 Monte el archivo de imagen ISO en la unidad de CD-ROM del dispositivo. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- 4 Acceda a la Interfaz de administración de dispositivos virtuales (VAMI) en https://servidor_orchestrator:5480 e inicie sesión como **raíz**.
- 5 En la pestaña **Actualizar**, haga clic en **Configuración**.
- 6 Seleccione el botón de opción junto a **Usar actualizaciones de CD-ROM**.
- 7 Vuelva a la página **Estado**.
Se mostrará la versión de la actualización disponible.
- 8 Haga clic en **Instalar actualizaciones**.
- 9 Acepte el contrato de licencia del usuario final de VMware y confirme que desea instalar la actualización.
- 10 Para completar la actualización, reinicie Orchestrator Appliance.
 - a Inicie sesión de nuevo en la Interfaz de administración de dispositivos virtuales (VAMI) como **raíz**.
- 11 (opcional) En la pestaña **Actualizar**, compruebe que se haya instalado correctamente la última versión del Orchestrator Appliance.
- 12 Inicie sesión en el centro de control como **raíz**.
- 13 Si tiene pensado crear un clúster de las instancias de Orchestrator, vuelva a configurar la configuración de los hosts.
 - a En la página **Configuración de hosts** del centro de control, haga clic en **CAMBIAR**.
 - b Introduzca el nombre del host del servidor del equilibrador de carga en lugar del nombre de Orchestrator Appliance de vRealize.

14 Vuelva a configurar la autenticación.

- a Si, antes de la actualización, el servidor de Orchestrator se configuró para que usara **LDAP** o **SSO (heredado)** como método de autenticación, configure **vSphere** o **vRealize Automation** como proveedor de autenticación.
- b Si la autenticación ya está establecida en **vSphere** o **vRealize Automation**, elimine la configuración del registro y vuelva a registrarla.

Nota Si, antes de la actualización, su instancia de Orchestrator ha utilizado **vSphere** como proveedor de autenticación y se ha configurado para conectarse al nombre de dominio completo o la dirección IP de vCenter Server, en caso de que tenga una instancia externa de Platform Services Controller, después de la actualización debe configurar Orchestrator para que se conecte al nombre de dominio completo o la dirección IP de la instancia de Platform Services Controller que contiene la instancia de vCenter Single Sign-On. También debe importar manualmente a Orchestrator los certificados de todas las instancias de Platform Services Controller que compartan el mismo dominio de vCenter Single Sign-On.

Ha actualizado correctamente Orchestrator Appliance.

Pasos siguientes

Compruebe que Orchestrator esté configurado correctamente en la página **Validar configuración** del centro de control.

Actualizar Orchestrator Appliance con un repositorio específico

Puede configurar Orchestrator para que utilice un repositorio local, en el que ha cargado el archivo de actualización.

Requisitos previos

- Desmonte todos los sistemas de archivos de red. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente la memoria de Orchestrator Appliance hasta por lo menos 6 GB. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente el tamaño del disco de la máquina virtual de vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Asegúrese de que la partición raíz de Orchestrator Appliance tenga al menos 3 GB de espacio libre disponible. Para obtener más información sobre cómo aumentar el tamaño de una partición de disco, consulte el artículo de la base de conocimientos 1004071: <http://kb.vmware.com/kb/1004071>.
- Tome una snapshot de la máquina virtual de Orchestrator. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Si utiliza una base de datos externa, cree una copia de seguridad de la misma.

- Si utiliza la base de datos preconfigurada en Orchestrator PostgreSQL, cree una copia de seguridad de la base de datos desde el menú **Exportar base de datos** del centro de control.

Procedimiento

- 1 Prepare el repositorio local para las actualizaciones.
 - a Instale y configure un servidor web local.
 - b Descargue el archivo VMware-vR0-Appliance-versión-número_compilación-updaterepo.zip del sitio oficial de descargas de VMware.
 - c Extraiga el archivo .ZIP en el repositorio local.
- 2 Acceda a la Interfaz de administración de dispositivos virtuales (VAMI) en `https://servidor_orchestrator:5480` e inicie sesión como **raíz**.
- 3 En la pestaña **Actualizar**, haga clic en **Configuración**.
- 4 Seleccione el botón de opción junto a **Usar repositorio especificado**.
- 5 Escriba la dirección URL del repositorio local que apunte al directorio Update_Repo.
`http://servidor_web_local:puerto/build/mts/release/bora-número_compilación/publish/exports/Update_Repo`
- 6 Si el repositorio local requiere autenticación, escriba el nombre de usuario y la contraseña.
- 7 Haga clic en **Guardar configuración**.
- 8 En la página **Estado**, haga clic en **Buscar actualizaciones**.
- 9 Si hay actualizaciones disponibles, haga clic en **Instalar actualizaciones**.
- 10 Acepte el contrato de licencia del usuario final de VMware y confirme que desea instalar la actualización.
- 11 Para completar la actualización, reinicie Orchestrator Appliance.
 - a Inicie sesión de nuevo en la Interfaz de administración de dispositivos virtuales (VAMI) como **raíz**.
- 12 (opcional) En la pestaña **Actualizar**, compruebe que se haya instalado correctamente la última versión del Orchestrator Appliance.
- 13 Inicie sesión en el centro de control como **raíz**.
- 14 Si tiene pensado crear un clúster de las instancias de Orchestrator, vuelva a configurar la configuración de los hosts.
 - a En la página **Configuración de hosts** del centro de control, haga clic en **CAMBIAR**.
 - b Introduzca el nombre del host del servidor del equilibrador de carga en lugar del nombre de Orchestrator Appliance de vRealize.

15 Vuelva a configurar la autenticación.

- a Si, antes de la actualización, el servidor de Orchestrator se configuró para que usara **LDAP** o **SSO (heredado)** como método de autenticación, configure **vSphere** o **vRealize Automation** como proveedor de autenticación.
- b Si la autenticación ya está establecida en **vSphere** o **vRealize Automation**, elimine la configuración del registro y vuelva a registrarla.

Nota Si, antes de la actualización, su instancia de Orchestrator ha utilizado **vSphere** como proveedor de autenticación y se ha configurado para conectarse al nombre de dominio completo o la dirección IP de vCenter Server, en caso de que tenga una instancia externa de Platform Services Controller, después de la actualización debe configurar Orchestrator para que se conecte al nombre de dominio completo o la dirección IP de la instancia de Platform Services Controller que contiene la instancia de vCenter Single Sign-On. También debe importar manualmente a Orchestrator los certificados de todas las instancias de Platform Services Controller que compartan el mismo dominio de vCenter Single Sign-On.

Ha actualizado correctamente Orchestrator Appliance.

Pasos siguientes

Compruebe que Orchestrator esté configurado correctamente en la página **Validar configuración** del centro de control.

Actualizar un clúster de dispositivo de vRealize Orchestrator para usarlo con vRealize Automation 7.4

Si utiliza un clúster de dispositivo de vRealize Orchestrator con vRealize Automation, debe actualizar el clúster de dispositivo de Orchestrator a la versión 7.4. Para ello, debe actualizar una única instancia y unir los nodos de 7.4 que se acaban de instalar con la instancia actualizada.

Para actualizar una única instancia de vRealize Orchestrator, consulte [Actualizar un dispositivo independiente de vRealize Orchestrator para su uso con vRealize Automation](#).

Requisitos previos

- [Instalar la actualización en los componentes de IaaS y el dispositivo de vRealize Automation](#).
- Configure un equilibrador de carga para distribuir el tráfico entre varias instancias de vRealize Orchestrator. Consulte la [guía de configuración del equilibrio de carga de vRealize Orchestrator](#).
- Tome una snapshot de todos los nodos de servidor de vRealize Orchestrator.
- Realice una copia de seguridad de la base de datos compartida de vRealize Orchestrator.

Procedimiento

- 1 Detenga los servicios de Orchestrator `vco-server` y `vco-configurator` en todos los nodos del clúster.

- 2 Actualice únicamente una de las instancias del servidor de Orchestrator en el clúster con uno de los procedimientos que se han descrito.
- 3 Implemente un nuevo Orchestrator Appliance en la versión 7.3.
 - a Configure el nuevo nodo con los ajustes de red de una instancia existente no actualizada que forme parte del clúster.
- 4 Acceda al centro de control del segundo nodo para iniciar el asistente para configuración.
 - a Vaya a `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter`.
 - b Inicie sesión como **raíz** con la contraseña que introdujo durante la implementación de OVA.
- 5 Seleccione el tipo de implementación **Orchestrator en clúster**.

Al seleccionar este tipo, hace que el nodo se una a un clúster de Orchestrator existente.
- 6 En el cuadro de texto **Nombre del host**, escriba el nombre del host o la dirección IP de la primera instancia del servidor de Orchestrator.

Nota Debe ser la IP local o el nombre de host de la instancia de Orchestrator a la que se une el segundo nodo. No debe usar la dirección del equilibrador de carga.

- 7 En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de raíz de la instancia del servidor de Orchestrator.
- 8 Haga clic en **Unir**. La instancia de Orchestrator clona la configuración del nodo, al cual se une. El servicio del servidor de Orchestrator de ambos nodos se reinicia automáticamente.
- 9 Acceda al Centro de Control del clúster actualizado de Orchestrator a través de la dirección del equilibrador de carga e inicie sesión como **administrador**.
- 10 En la página **Administración de clústeres de Orchestrator**, asegúrese de que las cadenas **Huella digital de configuración activa** y **Huella digital de configuración pendiente** de todos los nodos del clúster coincidan.

Nota Puede que necesite actualizar la página varias veces hasta que coincidan ambas cadenas.

- 11 Compruebe que el clúster de vRealize Orchestrator se haya configurado correctamente en la página **Validar configuración** del centro de control.
- 12 (opcional) Repita los pasos 3 a 8 con cada nodo adicional del clúster.

Ha actualizado correctamente el clúster de Orchestrator.

Pasos siguientes

[Configurar los equilibradores de carga.](#)

Configurar los equilibradores de carga

Si la implementación usa equilibradores de carga, vuelva a habilitar los nodos secundarios y las comprobaciones de estado, y revierta la configuración de tiempo de espera del equilibrador de carga.

Las comprobaciones de estado de vRealize Automation varían según la versión. Para obtener más información, consulte *Guía de configuración del equilibrio de carga de vRealize Automation* en la documentación de [VMware vRealize Automation](#).

Cambie la configuración de tiempo de espera del equilibrador de carga de 10 minutos al valor predeterminado.

Tareas posteriores a la actualización para actualizar vRealize Automation

Después de actualizar de vRealize Automation 7.1, 7.2 o 7.3.x a la versión 7.4, debe realizar tareas posteriores a la actualización obligatorias.

Actualizar agentes de software a TLS 1.2

Después de actualizar a vRealize Automation 7.4, debe realizar varias tareas para actualizar los agentes de software del entorno de vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 a TLS 1.2.

A partir de vRealize Automation 7.4, Transport Layer Security (TLS) 1.2 es el único protocolo TLS admitido para la comunicación de datos entre vRealize Automation y el navegador.

Tras la migración, debe actualizar las plantillas de máquina virtual existentes desde el entorno de vRealize Automation 7.1, 7.2, 7.3 o 7.3.1, así como cualquier máquina virtual existente.

Actualizar plantillas de máquina virtual de vRealize Automation

Las plantillas existentes se deben actualizar después de completar la actualización a vRealize Automation 7.4 para que los agentes de software usen el protocolo TLS 1.2.

El código de agente invitado y el de arranque de agente deben actualizarse en las plantillas de vRealize Automation 7.1, 7.2, 7.3 o 7.3.1. Si está utilizando una opción de clonación vinculada, es posible que deba volver a asignar las plantillas con las máquinas virtuales creadas recientemente y sus instantáneas.

Para actualizar las plantillas, complete estas tareas.

- 1 Inicie sesión en vSphere.
- 2 Convierta cada plantilla de vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 a una máquina virtual y encienda la máquina.
- 3 Importe el instalador de software adecuado y ejecute el instalador de software en cada máquina virtual.
- 4 Vuelva a convertir cada máquina virtual a una plantilla.

Utilice este procedimiento a fin de ubicar el instalador de software para Linux o Windows.

Requisitos previos

Haber actualizado a vRealize Automation 7.4 correctamente.

Procedimiento

- 1 Inicie un navegador y abra la página de presentación del dispositivo de vRealize Automation 7.4 con el nombre de dominio completo del dispositivo virtual: `https://vra-va-nombredelhost.dominio.nombre`.

- 2 Haga clic en la **página de agentes invitados y de software**.
- 3 Siga las instrucciones del instalador de software para Linux o Windows.

Pasos siguientes

[Identificar las máquinas virtuales que necesitan actualización del agente de software.](#)

Identificar las máquinas virtuales que necesitan actualización del agente de software

Puede utilizar el servicio de estado en vRealize Automation para identificar las máquinas virtuales que necesitan una actualización del agente de software a TLS 1.2.

Puede utilizar el servicio de estado para identificar las máquinas virtuales que necesitan una actualización del agente de software a TLS 1.2. Todos los agentes de software en el entorno de vRealize Automation 7.4 necesitan actualizarse para que pueda realizar procedimientos posteriores al aprovisionamiento, que requieren una comunicación segura entre el navegador y vRealize Automation.

Requisitos previos

- Ha actualizado correctamente a vRealize Automation 7.4.
- Ha iniciado sesión en vRealize Automation 7.4 en el dispositivo virtual principal como administrador de tenant.

Procedimiento

- 1 Haga clic en **Administración > Estado de mantenimiento**.
- 2 Haga clic en **Nueva configuración**.
- 3 En la página Detalles de la configuración, indique la información solicitada.

| Opción | Comentario |
|-------------|--|
| Nombre | Introduzca verificación de agente de software . |
| Descripción | Añada una descripción opcional, por ejemplo, Locate software agents for upgrade to TLS 1.2 (Buscar los agentes de software para actualización a TLS 1.2). |
| Producto | Seleccione vRealize Automation 7.4.0. |
| Programar | Seleccione Ninguno . |

- 4 Haga clic en **Siguiente**.
- 5 En la página Seleccionar conjuntos de pruebas, seleccione **Pruebas de sistema de vRealize Automation** y **Pruebas de Tenant de vRealize Automation**.
- 6 Haga clic en **Siguiente**.

7 En la página Configurar parámetros, indique la información solicitada.

Tabla 1-56. Dispositivo virtual de vRealize Automation

| Opción | Descripción |
|--|--|
| Dirección de servidor web pública | <ul style="list-style-type: none"> Es la dirección URL base para el host del dispositivo de vRealize Automation en una implementación mínima. Por ejemplo, <code>https://va-host.domain/</code>. Es la dirección URL base para el equilibrador de carga de vRealize Automation en una implementación de alta disponibilidad. Por ejemplo, <code>https://load-balancer-host.domain/</code>. |
| Dirección de la consola de SSH | Nombre de dominio completo del dispositivo de vRealize Automation. Por ejemplo, <code>va-host.domain</code> . |
| Usuario de la consola de SSH | root |
| Contraseña de la consola de SSH | Contraseña de la raíz. |
| Tiempo máximo de respuesta del servicio (ms) | Acepte el valor predeterminado: 2000 |

Tabla 1-57. Tenant del sistema de vRealize Automation

| Opción | Descripción |
|-------------------------------------|-------------------------------|
| Administrador de tenant del sistema | administrador |
| Contraseña de tenant del sistema | Contraseña del administrador. |

Tabla 1-58. Supervisión de espacio en disco de vRealize Automation

| Opción | Descripción |
|--------------------------------------|------------------------------------|
| Porcentaje del umbral de advertencia | Acepte el valor predeterminado: 75 |
| Porcentaje de umbral crítico | Acepte el valor predeterminado: 90 |

Tabla 1-59. Tenant de vRealize Automation

| Opción | Descripción |
|---|--|
| Tenant en prueba | Tenant seleccionado para las pruebas. |
| Nombre de usuario del administrador de tejido | Nombre de usuario del administrador de tejido. Por ejemplo, <code>admin@va-host.local</code> . Nota Este administrador de tejido también debe tener un administrador de tenant y una función de administrador de IaaS en orden para que se ejecuten todas las pruebas. |
| Contraseña del administrador de tejido | Contraseña del administrador de tejido. |

8 Haga clic en **Siguiente**.

9 En la página Resumen, revise la información y haga clic en **Finalizar**.

Finalizó la configuración de comprobación del agente de software.

10 En la tarjeta de verificación Agente de software, haga clic en **Ejecutar**.

- 11 Una vez completada la prueba, haga clic en el centro de la tarjeta de verificación Agente de software.
- 12 En la página de resultados de verificación del agente de software, explore los resultados de la prueba y busque la prueba Comprobar versión del agente de software, en la columna Nombre. Si se produce un error en el resultado de la prueba, haga clic en el vínculo de la **causa** en la columna Causa para ver las máquinas virtuales que tienen un agente de software desactualizado.

Pasos siguientes

Si tiene máquinas virtuales con un agente de software desactualizado, consulte [Actualizar los agentes de software en vSphere](#).

Actualizar los agentes de software en vSphere

Puede actualizar los agentes de software obsoletos en vSphere a TLS 1.2 después de la actualización mediante vRealize Automation Appliance Management.

Este procedimiento actualiza los agentes de software obsoletos a TLS 1.2 en las máquinas virtuales en un entorno actualizado. Se requiere para la actualización a vRealize Automation 7.4.

Requisitos previos

- Haber actualizado a vRealize Automation 7.4 correctamente.
- Ha usado el servicio de estado para identificar los dispositivos virtuales con agentes de software obsoletos.

Procedimiento

- 1 En el dispositivo de vRealize Automation principal, inicie sesión en la Administración de dispositivos de vRealize Automation como **raíz** con la contraseña que introdujo al implementar el dispositivo de vRealize Automation.

Para un entorno de alta disponibilidad, abra Appliance Management en el dispositivo principal.

- 2 Haga clic en **Configuración de vRA > Agentes de software**.
- 3 Haga clic en **Activar/desactivar TLS 1.0, 1.1**.

El estado de TLS v1.0, v1.1 es HABILITADO.

- 4 En las credenciales del tenant, escriba la información solicitada para el dispositivo vRealize Automation 7.4.

| Opción | Descripción |
|-------------------|---|
| Nombre de tenant | Nombre de tenant en el dispositivo vRealize Automation actualizado. Nota El usuario de tenant debe tener la función de arquitecto de software asignada. |
| Nombre de usuario | Nombre de usuario del administrador de tenant en el dispositivo vRealize Automation. |
| Contraseña | Contraseña de administrador de tenant. |

5 Haga clic en Probar conexión.

Si se establece una conexión, aparece un mensaje de confirmación.

6 Haga clic en Enumerar lotes.

Aparecerá la tabla de lista de opciones de lote.

7 Haga clic en Mostrar.

Aparece una tabla con una lista de las máquinas virtuales con agentes de software obsoletos.

8 Actualice el agente de software de las máquinas virtuales que estén en estado ACTUALIZABLE.

- Para actualizar el agente de software en una máquina virtual individual, haga clic en **Mostrar** para un grupo de máquinas virtuales, identifique la máquina virtual que desea actualizar y haga clic en **Ejecutar** para iniciar el proceso de actualización.
- Para actualizar al agente de software de un lote de máquinas virtuales, identifique el grupo que desea actualizar y haga clic en **Ejecutar** para iniciar el proceso de actualización.

Si tiene más de 200 máquinas virtuales para actualizar, puede controlar la velocidad del proceso de actualización por lotes; para ello, introduzca los valores de estos parámetros.

| Opción | Descripción |
|---------------------|--|
| Tamaño de lote | La cantidad de máquinas virtuales seleccionadas para la actualización por lotes. Puede cambiar este número para ajustar la velocidad de actualización. |
| Profundidad de cola | La cantidad de ejecuciones de actualización en paralelo que tienen lugar a la vez. Por ejemplo, 20. Puede cambiar este número para ajustar la velocidad de actualización. |
| Errores de lote | El recuento de errores de REST que hacen que el procesamiento por lotes se ralentice. Por ejemplo, si desea detener la actual actualización por lotes después de 5 errores para mejorar la estabilidad de la actualización, introduzca 5 en el campo de texto. |
| Fallos de lote | El número de actualizaciones fallidas del agente de software que hacen que el procesamiento por lotes se ralentice. Por ejemplo, si desea detener la actual actualización por lotes después de 5 errores para mejorar la estabilidad de la actualización, introduzca 5 en el campo de texto. |
| Sondeo de lote | Con qué frecuencia se sondea el proceso de actualización para comprobarlo. Puede cambiar este número para ajustar la velocidad de actualización. |

Si el proceso de actualización es demasiado lento o genera demasiadas actualizaciones incorrectas, puede ajustar estos parámetros para mejorar el rendimiento de la actualización.

Nota Al hacer clic en **Actualizar**, se borra la lista de lotes. No afecta el proceso de actualización. También se actualiza la información sobre si se ha establecido TLS 1.2 o no. Además, al hacer clic en **Actualizar**, también se realiza una comprobación de estado de los servicios de vRealize Automation. Si los servicios no se están ejecutando, el sistema muestra un mensaje de error y desactiva todos los otros botones de acción.

9 Haga clic en **Activar/desactivar TLS 1.0, 1.1**.

El estado de TLS v1.0, v1.1 es DESHABILITADO.

Actualizar agentes de software en Amazon Web Service o Azure

Puede actualizar manualmente los agentes de software obsoletos de las máquinas virtuales en Amazon Web Service (AWS) o Azure.

Requisitos previos

- Haber actualizado a vRealize Automation 7.4 correctamente.
- Un túnel de software está presente y se conoce la dirección IP de máquina virtual de túnel.

Procedimiento

- 1 Cree un archivo de nodo para cada nodo que se debe actualizar.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

Nota Para una actualización local, la instancia de `$DestinationVRAServer` es la misma que la de `$SourceVRAServer`.

- 2 Cree un archivo de plan para actualizar al agente de software en una máquina virtual de Linux o Windows.

- Modifique el archivo de parámetros de migración en `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}` para que contenga el valor de la dirección IP privada correspondiente al endpoint de AWS o Azure.

```
"key": "ipAddress",
  "value": {
    "type": "string",
    "value": "<$PrivateIp:$PrivatePort>"
  }
}
```

- Utilice este comando para actualizar una máquina de Linux.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL Software.LinuxAgentUpdate74 --
source_cloud_provider azure
```

- Utilice este comando para actualizar una máquina de Windows.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW Software.WindowsAgentUpdate74 --
source_cloud_provider azure
```

- Este comando ejecuta el archivo de plan.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

- 3 Utilice este comando para actualizar el agente de software con el archivo de nodo del paso 1 y luego con el archivo de plan del paso 2.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <
$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux
Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --
plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider
azure --action plan_batch -S <$SourceVRAServer>
```

Como alternativa, puede utilizar este comando para ejecutar un nodo a la vez desde el archivo del nodo proporcionando un índice de nodos.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <
$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux
Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --
plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider
azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

Cuando realice este procedimiento, puede seguir los registros del dispositivo virtual de vRealize Automation y la máquina de host para ver el proceso de actualización del agente de servidor.

Tras la actualización, el proceso de actualización importa un script de actualización de software para Windows o Linux en el dispositivo virtual de vRealize Automation 7.4. Puede iniciar sesión en el host de dispositivo virtual de vRealize Automation para asegurarse de que el componente de software se ha importado correctamente. Después de importar el componente, se envía una actualización de

software al evento Broker Service (EBS) anterior para retransmitir los scripts de actualización de software a las máquinas virtuales identificadas. Cuando la actualización y los agentes de software nuevos estén operativos, se enlazan al nuevo dispositivo virtual de vRealize Automation mediante el envío de una solicitud de ping.

Nota Archivos de registro útiles

- Salida de Catalina para instancia de origen de vRealize Automation: `/var/log/vcac/catalina.out`. En este archivo, puede ver las solicitudes de actualización que se envían al realizar las migraciones de agente. Esta actividad equivale a ejecutar una solicitud de aprovisionamiento de software.
- Salida de Catalina para instancia de destino de vRealize Automation: `/var/log/vcac/catalina.out`. En este archivo, verá las máquinas virtuales migradas informar aquí de sus solicitudes de ping para que incluyan los números de versión 7.4.0-SNAPSHOT. Puede hacerlas corresponder comparando los nombres de tema de EBS, por ejemplo, `sw-agent-UUID`.
- Carpeta de actualización del agente en el archivo de registro de actualización principal de máquina de destino
vRealize Automation: `/var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`. Puede seguir este archivo para ver qué operación de actualización está en curso.
- Registros individuales disponibles en las carpetas de tenant: `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`. Aquí se enumeran los nodos individuales como archivos de lote con errores y extensiones en curso.
- Máquinas virtuales migradas: `/opt/vmware-appdirector/agent/logs/darwin*.log`. Puede detectar esta ubicación que debería mostrar una lista con las solicitudes de actualización de software que se reciben, así como el posterior reinicio del agente `agent_bootstrap + software`.

Establecer el modo de replicación de PostgreSQL de vRealize Automation como sincrónico

Si establece el modo de replicación de PostgreSQL como asincrónico antes de la actualización, puede establecer el modo de replicación de PostgreSQL como sincrónico después de actualizar un entorno distribuido de vRealize Automation.

Requisitos previos

- Ha actualizado un entorno distribuido de vRealize Automation.
- Ha iniciado sesión como **raíz** en la instancia de administración de dispositivos de vRealize Automation adecuada en `https://vra-va-hostname.domain.name:5480`.

Procedimiento

- 1 Haga clic en **Configuración de vRA > Base de datos**.
- 2 Haga clic en **Modo sincrónico** y espere hasta que finalice la acción.
- 3 Compruebe que todos los nodos de la columna Estado de sincronización muestran el estado **Sincrónico**.

Pasos siguientes

[Ejecutar la conexión de prueba y comprobar los endpoints actualizados.](#)

Ejecutar la conexión de prueba y comprobar los endpoints actualizados

Al actualizar de vRealize Automation 7.3 o versiones anteriores a la versión 7.4, se modifican los endpoints del entorno de destino.

Después de actualizar a vRealize Automation 7.4, debe utilizar la acción **Probar conexión** para todos los endpoints aplicables. También es posible que tenga que realizar ajustes en algunos de los endpoints actualizados. Para obtener más información, consulte [Consideraciones al trabajar con endpoints actualizados o migrados](#).

La configuración de seguridad predeterminada relativa a endpoints actualizados o migrados consiste en no aceptar certificados que no sean de confianza.

Si usaba certificados que no eran de confianza, después de actualizar o migrar desde una instalación de vRealize Automation anterior, deberá hacer lo siguiente para que todos los endpoints de vSphere y de NSX permitan la validación de certificados. De lo contrario, las operaciones de endpoint generarán errores de certificado. Para obtener más información, consulte los artículos de la base de conocimientos de VMware *La comunicación del endpoint se interrumpe después de actualizar a vRA 7.3 (2150230)* en <http://kb.vmware.com/kb/2150230> y *Cómo descargar e instalar certificados raíz de vCenter Server para evitar advertencias de certificado del navegador web (2108294)* en <http://kb.vmware.com/kb/2108294>.

- 1 Después de la actualización o migración, inicie sesión en la máquina del agente de vSphere de vRealize Automation y reinicie los agentes de vSphere en la pestaña **Servicios**.

Es posible que no todos los agentes se reinicien con la migración, de modo que puede que sea necesario reiniciarlos manualmente.

- 2 Espere a que al menos un informe de ping finalice. Un informe de ping tarda uno o dos minutos en finalizar.
- 3 Cuando los agentes de vSphere hayan empezado a recopilar datos, inicie sesión en vRealize Automation como un administrador de IaaS.
- 4 Haga clic en **Infraestructura > Endpoints > Endpoints**.
- 5 Edite un endpoint de vSphere y haga clic en **Probar conexión**.
- 6 Si aparece un mensaje de certificado, haga clic en **Aceptar** para aceptar el certificado.

Si no aparece un mensaje de certificado, es posible que el certificado esté actualmente almacenado en una entidad raíz de confianza de la máquina de Windows que aloja el servicio del endpoint, por ejemplo, como una máquina de agente de proxy o una máquina de DEM.
- 7 Haga clic en **Aceptar** para confirmar la aceptación de certificado y guardar el endpoint.
- 8 Repita este procedimiento por cada endpoint de vSphere.
- 9 Repita este procedimiento por cada endpoint de NSX.

Si la acción **Probar conexión** finaliza correctamente, pero alguna de las operaciones de aprovisionamiento o de recopilación de datos genera errores, puede instalar el mismo certificado en todas las máquinas de agente que sirvan al endpoint y en todas las máquinas DEM. Si lo prefiere, puede desinstalar el certificado de las máquinas existentes y repetir el procedimiento anterior en el endpoint con el error.

Ejecutar la recopilación de datos del inventario de red y seguridad de NSX después de actualizar a partir de vRealize Automation

Después de actualizar desde vRealize Automation 7.1, 7.2 o 7.3.x a 7.4, debe ejecutar la recopilación de datos del inventario de seguridad y redes de NSX en el entorno de vRealize Automation 7.4.

Esta recopilación de datos es necesaria para que la acción de reconfiguración del equilibrador de carga funcione en vRealize Automation 7.4 para las implementaciones de 7.1, 7.2 o 7.3.x.

Requisitos previos

- [Ejecutar la recopilación de datos del inventario de red y seguridad de NSX antes de actualizar vRealize Automation.](#)
- Haber actualizado a vRealize Automation 7.4 correctamente.

Procedimiento

- ◆ Ejecute la recopilación de datos del inventario de red y seguridad de NSX en vRealize Automation 7.4 después de realizar la actualización. Consulte [Iniciar recopilación de datos de endpoint manualmente.](#)

Unión del dispositivo de réplica al clúster

Tras finalizar la actualización del dispositivo de vRealize Automation principal, cada nodo de réplica actualizado se une automáticamente al nodo principal. En el caso de que un nodo de réplica deba actualizarse por separado, utilice estos pasos para unir manualmente el nodo de réplica al clúster.

Acceda a la consola de administración del dispositivo del nodo de réplica que no está unido al clúster y lleve a cabo los siguientes pasos.

Procedimiento

- 1 Seleccione **Configuración de vRA > Clúster**.
- 2 Haga clic en **Unirse a clúster**.

Configurar puertos para implementaciones de alta disponibilidad

Tras finalizar una actualización en una implementación de alta disponibilidad, debe configurar el equilibrador de carga para que transfiera el tráfico del puerto 8444 al dispositivo de vRealize Automation para poder usar la funcionalidad de la consola remota.

Para obtener más información, consulte *Guía de configuración del equilibrio de carga de vRealize Automation* en la documentación de [vRealize Automation](#).

Reconfigurar la instancia integrada de vRealize Orchestrator para admitir la alta disponibilidad

En las implementaciones de alta disponibilidad, debe volver a unir cada dispositivo de vRealize Automation de réplica de destino manualmente al clúster para, de este modo, dar cabida a la alta disponibilidad en la instancia de vRealize Orchestrator integrada.

Requisitos previos

Inicie sesión en la consola de administración del dispositivo de vRealize Automation de réplica de destino.

- 1 Inicie el navegador y abra la consola de administración de vRealize Automation de réplica de destino usando el nombre de dominio completo (FQDN) del dispositivo virtual de réplica de destino:
`https://vra-va-hostname.domain.name:5480`.
- 2 Inicie sesión con el nombre de usuario **root** y la contraseña que especificó al implementar el dispositivo de vRealize Automation de réplica de destino.

Procedimiento

- 1 Seleccione **Configuración de vRA > Clúster**.
- 2 En el cuadro de texto **Nodo de clúster de encabezado**, introduzca el FQDN del dispositivo de vRealize Automation principal de destino.
- 3 Escriba la contraseña raíz en el cuadro de texto **Contraseña**.
- 4 Haga clic en **Unirse a clúster**.
Continúe aunque aparezcan advertencias de certificado. El sistema reinicia los servicios del clúster.
- 5 Compruebe que los servicios se están ejecutando.
 - a En la barra de pestañas superior, haga clic en **Servicios**.
 - b Haga clic en **Actualizar** para supervisar cómo se van iniciando los servicios.

Restaurar archivos de tiempo de espera de flujos de trabajo externos

Debe volver a configurar los archivos de tiempo de espera de flujos de trabajo externos de vRealize Automation debido a que el proceso de actualización sobrescribe los archivos xmldb.

Procedimiento

- 1 Abra los archivos de configuración del flujo de trabajo externo (xmldb) en su sistema desde el siguiente directorio.
`\VMware\vCAC\Server\ExternalWorkflows\xmldb\`.
- 2 Reemplace los archivos xmldb por los archivos a partir de los que ha creado copias de seguridad antes de la migración. Si no tiene archivos de copia de seguridad, vuelva a definir la configuración de tiempo de espera de flujos de trabajo externos.
- 3 Guarde la configuración.

Habilitar la acción de conexión a la consola remota para consumidores

La acción de consola remota para consumidores es compatible con dispositivos provisionados por vSphere en vRealize Automation.

Edite el blueprint después de actualizar la versión y seleccionar la acción **Conectar con la consola remota** en la pestaña **Acción**.

Para obtener más información, consulte el [artículo 2109706 de la Base de conocimientos](#).

Restaurar cambios para iniciar sesión en el archivo app.config

El proceso de actualización sobrescribe los cambios realizados que se registran en los archivos de configuración. Después de completar una actualización, debe restaurar los cambios realizados en el archivo `app.config` antes de la actualización.

Habilitar la conmutación por error automática de Manager Service después de actualizar

La conmutación por error automática de Manager Service se deshabilita de forma predeterminada cuando vRealize Automation se actualiza.

Siga estos pasos para habilitar la conmutación por error automática de Manager Service después de la actualización.

Procedimiento

- 1 Abra una ventana de símbolo del sistema como usuario raíz en el dispositivo de vRealize Automation.
- 2 Cambie los directorios a `/usr/lib/vcac/tools/vami/commands`.
- 3 Para habilitar la conmutación por error automática de Manager Service, ejecute el siguiente comando.

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

Para deshabilitar la conmutación por error automática en una implementación entera de IaaS, ejecute 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 automáticamente en una copia de seguridad si la instancia principal de Manager Service se detiene.

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 copia de seguridad. La conmutación por error automática de Manager Service se deshabilita de forma predeterminada cuando IaaS se actualiza con el script de actualización de shell o mediante el archivo ejecutable del instalador de IaaS.

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 característica de conmutación por error automática permite que los hosts se supervisen entre sí con transparencia y conmuten por error cuando sea necesario, pero para ello es necesario 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.

Solucionar problemas de actualización de vRealize Automation

En los temas de solución de problemas de actualización se ofrecen soluciones a los problemas que podría encontrar durante la actualización de vRealize Automation 7.1, 7.2 o 7.3 a la versión 7.4.

La conmutación por error automática de Manager Service no se activa

Sugerencias para solucionar problemas del comando `manager-service-automatic-failover`.

Solución

- El comando `manager-service-automatic-failover` no se ejecuta o muestra este mensaje durante más de dos minutos: **Habilitando el modo de conmutación por error automática de Manager Service en el nodo: `IAAS_MANAGER_SERVICE_NODEID`.**
 - a Inicie sesión en la administración del dispositivo de vRealize Automation en `https://va-hostname.domain.name:5480` con el nombre de usuario **host** y la contraseña que especificó al implementar el dispositivo.
 - b Seleccione **Configuración de vRA > Clúster**.
 - c Compruebe que el servicio del agente de administración se está ejecutando en todos los hosts de Manager Service.
 - d Compruebe que la hora de última conexión de todos los nodos de Manager Service en IaaS es inferior a 30 segundos.

Si observa algún problema de conectividad del agente de administración, resuélvalo manualmente e intente ejecutar de nuevo el comando para habilitar la conmutación por error automática de Manager Service.

- El comando `manager-service-automatic-failover` no habilita la conmutación por error en un nodo de Manager Service. Conviene volver a ejecutar el comando para solucionar este problema.

- Algunos hosts de Manager Service en la implementación de IaaS tienen habilitada la conmutación por error, mientras que otros no. Todos los hosts de Manager Service en la implementación de IaaS deben tener habilitada esta característica o no funcionarán. Para corregir este problema, tome una de las siguientes medidas:
 - Deshabilite la conmutación por error en todos los nodos de Manager Service y utilice en su lugar el método de conmutación por error manual. Ejecute la conmutación por error únicamente en un host cada vez.
 - Si, tras varios intentos, la característica no se puede habilitar en un nodo de Manager Service, detenga el servicio VMware vCloud Automation Center de Windows en este nodo y establezca el tipo de inicio del nodo en Manual hasta que resuelva el problema.
- Use Python para validar que la conmutación por error está habilitada en cada nodo de Manager Service.
 - a Inicie sesión como usuario **root** en el nodo de dispositivos de vRealize Automation mediante SSH.
 - b Ejecute `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover ENABLE`.
 - c Compruebe que el sistema devuelve este mensaje: Activación del modo de conmutación por error automática de Manager Service en el nodo:
`IAAS_MANAGER_SERVICE_NODEID` lista.
- Confirme que la conmutación por error está habilitada en cada nodo de Manager Service; para ello, examine el archivo de configuración de Manager Service.
 - a Abra un símbolo del sistema en un nodo de Manager Service.
 - b Desplácese hasta la carpeta de instalación de vRealize Automation y abra el archivo de configuración de Manager Service en `VMware\vCAC\Server\ManagerService.exe.config`.
 - c Confirme que los siguientes elementos están presentes en la sección `<appSettings>`.
 - `<add key="FailoverModeEnabled" value="True" />`
 - `<add key="FailoverPingIntervalMilliseconds" value="30000" />`
 - `<add key="FailoverNodeState" value="active" />`
 - `<add key="FailoverMaxFailedDatabasePingAttempts" value="5" />`
 - `<add key="FailoverMaxFailedRepositoryPingAttempts" value="5" />`
- Compruebe en el estado que el servicio VMware vCloud Automation Center de Windows está iniciado y que el tipo de inicio es automático.
- Use Python para validar que la conmutación por error está deshabilitada en cada nodo de Manager Service.
 - a Inicie sesión como usuario **root** en el nodo de dispositivos de vRealize Automation mediante SSH.

- b Ejecute `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover DISABLE`.
- c Compruebe que el sistema devuelve este mensaje: Desactivación del modo de conmutación por error automática de Manager Service en el nodo:
`IAAS_MANAGER_SERVICE_NODEID` lista.
- Confirme que la conmutación por error está deshabilitada en cada nodo de Manager Service; para ello, examine el archivo de configuración de Manager Service.
 - a Abra un símbolo del sistema en un nodo de Manager Service.
 - b Desplácese hasta la carpeta de instalación de vRealize Automation y abra el archivo de configuración de Manager Service en `VMware\vCAC\Server\ManagerService.exe.config`.
 - c Confirme que el siguiente elemento está presente en la sección `<appSettings>`.
 - `<add key="FailoverModeEnabled" value="False" />`
- Para crear un nodo de Manager Service de espera pasiva, establezca el estado del nodo del servicio VMware vCloud Automation Center de Windows en detenido y el tipo de inicio, en manual.
- En un nodo de Manager Service activo, el estado del servicio VMware vCloud Automation Center de Windows debe ser iniciado y el tipo de inicio, automático.
- El comando `manager-service-automatic-failover` utiliza el identificador interno de nodo de Manager Service (`IAAS_MANAGER_SERVICE_NODEID`). Para buscar el nombre de host correspondiente a este identificador interno, ejecute el comando `vra-command list-nodes` y busque el host de Manager Service cuyo valor de `Nodeld` sea `IAAS_MANAGER_SERVICE_NODEID`.
- Haga lo siguiente para encontrar el Manager Service que el sistema ha elegido automáticamente como servicio activo.
 - a Inicie sesión como usuario **root** en el nodo de dispositivos de vRealize Automation mediante SSH.
 - b Ejecute `vra-command list-nodes --components`.
 - Si la conmutación por error está habilitada, busque el nodo de Manager Service con estado activo.
 - Si la conmutación por error está deshabilitada, busque el nodo de Manager Service con estado iniciado.

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.

Error en la actualización para el componente de sitio web de IaaS

Se produce un error en la actualización de IaaS y no es posible continuar.

Problema

Se produce un error en la actualización de IaaS para el componente de sitio web. Los siguientes mensajes de error aparecen en el archivo de log del instalador.

- System.Data.Services.Client.DataServiceQueryException:
An error occurred while processing this request. --->
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- **Description:** An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.
- Warning: Non-zero return code. Error del comando.
- Done Building Project "C:\Archivos de programa (x86)\VMware\VCAC\Server\Model Manager Data\DeployRepository.xml" (InstallRepoModel target(s)) -- FAILED.

Los siguientes mensajes de error aparecen en el archivo de log del repositorio.

- [Error]: [sub-thread-Id="20" context="" token=""] Failed to start repository service. Reason:
System.InvalidOperationException: Configuration section encryptionKey is not protected
at
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration config)

```
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2
decryptFunc)
at
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object
sender, ObjectMaterializedEventArgs e)
at
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()
at
System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
at
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyValue(Core
ModelEntities
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String
coreModelConnectionString)
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().
```

Causa

Se produce un error en la actualización de IaaS cuando la fecha de creación del archivo `web.config` es igual o posterior a la fecha modificada.

Solución

- 1 En el host de IaaS, inicie sesión en Windows.
- 2 Abra el símbolo del sistema de Windows.
- 3 Cambie los directorios a la carpeta de instalación de vRealize Automation.
- 4 Inicie su editor de texto preferido con la opción **Ejecutar como administrador**.
- 5 Busque y seleccione el archivo `web.config` y guarde el archivo para cambiar la fecha de modificación del archivo.

- 6 Examine las propiedades del archivo `web.config` para confirmar que la fecha de modificación del archivo es posterior a la fecha de creación.
- 7 Actualice `laaS`.

Manager Service no se ejecuta debido a errores de validación de SSL durante el tiempo de ejecución

Manager Service no se ejecuta debido a errores de validación de SSL.

Problema

Manager Service no se ejecuta y muestra el siguiente mensaje en el registro:

```
[Info]: Thread-Id="6" - context="" token="" Error al conectar con la base de datos central; se volverá a intentar en 00:00:05. Detalles del error: La conexión con el servidor se ha establecido correctamente, pero se ha producido un error durante el proceso de inicio de sesión. (Proveedor: proveedor de SSL. Error: 0 - La cadena de certificados la proporciona una entidad que no es de confianza).
```

Causa

Durante el tiempo de ejecución, Manager Service no se ejecuta debido a errores de validación de SSL.

Solución

- 1 Abra el archivo de configuración `ManagerService.config`.
- 2 Actualice `Encrypt=False` en la siguiente línea:

```
<add name="vcac-repository" providerName="System.Data.SqlClient"
connectionString="Data Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated
Security=True;Pooling=True;Max Pool
Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

Error al iniciar sesión tras la actualización

Después de una actualización, debe salir del explorador y volver a iniciar sesión para las sesiones que usan cuentas de usuario sin sincronizar.

Problema

Al iniciar sesión después de actualizar vRealize Automation, el sistema deniega el acceso a las cuentas de usuario no sincronizadas.

Solución

Salga del explorador y vuelva a iniciar vRealize Automation.

Eliminar nodos huérfanos en vRealize Automation

Un nodo huérfano es un nodo duplicado del que se informa en el host pero que no existe en el host.

Problema

Cuando compruebe que todos los nodos de IaaS y del dispositivo virtual están en buen estado, podría descubrir que algún host tiene uno o varios nodos huérfanos. Debe eliminar todos los nodos huérfanos.

Solución

- 1 En el dispositivo de vRealize Automation principal, inicie sesión en la Administración de dispositivos de vRealize Automation como **raíz** con la contraseña que introdujo al implementar el dispositivo de vRealize Automation.
- 2 Seleccione **Configuración de vRA > Clúster**.
- 3 Haga clic en **Eliminar** en cada uno de los nodos huérfanos de la tabla.

Parece que el comando **Unirse a clúster** falla después de actualizar a un entorno de alta disponibilidad

Después de hacer clic en **Unirse a clúster** en la consola de administración en un nodo de clúster secundario, el indicador de progreso desaparece.

Problema

Cuando utiliza la consola de administración del dispositivo de vRealize Automation después de actualizar para unir un nodo de clúster secundario al nodo principal, el indicador de progreso desaparece y no se muestra ningún mensaje de error ni de ejecución correcta. Este comportamiento es un problema intermitente.

Causa

El indicador de progreso desaparece porque algunos navegadores se detienen al esperar una respuesta del servidor. Este comportamiento no detiene el proceso de unión a un clúster. Puede confirmar que el proceso de unión a un clúster se haya realizado correctamente si revisa el archivo de log en `/var/log/vmware/vcac/vcac-config.log`.

La combinación para la actualización de la base de datos de PostgreSQL no se realiza correctamente

La combinación de base de datos de PostgreSQL externa con la base de datos de PostgreSQL integrada no se realiza correctamente.

Problema

Si la combinación para la actualización de base de datos de PostgreSQL no se realiza correctamente, puede llevar a cabo una combinación manual.

Solución

- 1 Restaure el dispositivo virtual de vRealize Automation al snapshot que hizo antes de la actualización.

- 2 Inicie sesión en el dispositivo virtual de vRealize Automation y ejecute este comando para permitir que la actualización se complete si la combinación de base de datos no sale bien.

```
touch /tmp/allow-external-db
```

El comando no deshabilita la combinación automática.

- 3 En el host remoto de base de datos de PostgreSQL, conéctese a la base de datos de PostgreSQL mediante la herramienta psql y ejecute estos comandos.

```
CREATE EXTENSION IF NOT EXISTS "hstore";
```

```
CREATE EXTENSION IF NOT EXISTS "uuid-osspl";
```

```
CREATE SCHEMA saas AUTHORIZATION vcac;
```

El usuario de este comando es vcac. Si vRealize Automation se conecta a la base de datos externa con otro usuario, reemplace vcac en este comando con el nombre de ese usuario.

```
CREATE EXTENSION IF NOT EXISTS "citext" SCHEMA saas;
```

- 4 Ejecute la actualización.

Si esta se realiza correctamente, el sistema funcionará como se espera con la base de datos de PostgreSQL externa. Asegúrese de que la base de datos de PostgreSQL externa se ejecuta correctamente.

- 5 Inicie sesión en el dispositivo virtual de vRealize Automation virtual y ejecute estos comandos

```
/etc/bootstrap/postupdate.d/00-20-db-merge-external
```

```
/etc/bootstrap/postupdate.d/11-db-merge-external
```

Error al actualizar el dispositivo de réplica de vRealize Automation

El dispositivo de vRealize Automation de réplica no se actualiza durante la actualización principal del dispositivo.

Causa

Es posible que un dispositivo de réplica no se actualice correctamente debido a problemas de conectividad u otros errores. Si esto ocurre, aparecerá un mensaje de advertencia en la pestaña **Actualizar** del dispositivo de vRealize Automation principal que resaltará la réplica que no pudo actualizarse.

Solución

- 1 Revierta el snapshot del dispositivo virtual de réplica o una copia de seguridad al estado previo a la actualización y enciéndalo.

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

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

- 3 Haga clic en **Actualizar > Configuración**.

- 4 Seleccione la descarga de las actualizaciones desde un repositorio de VMware o un CD-ROM en la sección Repositorio de actualización.

- 5 Haga clic en **Estado**.

- 6 Haga clic en **Comprobar actualizaciones** para comprobar si hay alguna actualización accesible.

- 7 Haga clic en **Instalar actualizaciones**.

- 8 Haga clic en **Aceptar**.

Aparece un mensaje que indica que hay una actualización en curso.

- 9 Abra los archivos log para comprobar que la actualización se esté realizando correctamente.

- `/opt/vmware/var/log/vami/vami.log`
- `/var/log/vmware/horizon/horizon.log`

Si cierra sesión durante el proceso de actualización y después inicia sesión antes de que se acabe la actualización, puede seguir el proceso de actualización en el archivo de log. El archivo `updatecli.log` puede mostrar información acerca de la versión de vRealize Automation desde la que está actualizando. La versión que se muestra cambia a la versión posterior adecuada durante el proceso de actualización.

El tiempo necesario para que la actualización finalice depende del entorno.

- 10 Cuando la actualización haya finalizado, reinicie el dispositivo virtual.

- a Haga clic en **Sistema**.
- b Haga clic en **Reiniciar** y confirme la selección.

- 11 Seleccione **Configuración de vRA > Clúster**.

- 12 Introduzca el FQDN del dispositivo de vRealize Automation principal, y haga clic en **Unirse a un clúster**.

Las copias de seguridad de archivos .xml hacen que el sistema agote el tiempo de espera

vRealize Automation registra todos los archivos con una extensión .xml en el directorio `VMware\VCAC\Server\ExternalWorkflows\xml\db\`. Si este directorio contiene archivos de copia de seguridad con una extensión .xml, el sistema ejecuta flujos de trabajo duplicados que provocan que el sistema agote el tiempo de espera.

Solución

Solución alternativa: Cuando realice copias de seguridad de archivos en este directorio, traslade las copias de seguridad a otro directorio o cambie la extensión del nombre del archivo de copia de seguridad para que no contenga .xml.

Excluir la actualización de IaaS

Puede actualizar el dispositivo de vRealize Automation sin actualizar los componentes de IaaS.

Utilice este procedimiento cuando quiera actualizar el dispositivo de vRealize Automation sin actualizar los componentes de IaaS. Este procedimiento

- No detiene los servicios de IaaS.
- Omite la actualización de los agentes de administración.
- Impide la actualización automática de los componentes de IaaS después de las actualizaciones de dispositivos de vRealize Automation.

Procedimiento

- 1 Abra una conexión de Secure Shell con el nodo del dispositivo de vRealize Automation principal.
- 2 En el símbolo del sistema, ejecute este comando para crear el archivo de alternancia:

```
touch /tmp/disable-iaas-upgrade
```

- 3 Detenga los servicios de IaaS de forma manual.
 - a Inicie sesión en el servidor de Windows de IaaS.
 - b Seleccione **Inicio > Herramientas administrativas > Servicios**.
 - c Detenga los servicios en el siguiente orden.

Nota No desconecte el servidor de Windows de IaaS.

- 1 Cada agente de proxy de VMware vRealize Automation.
 - 2 Todos los trabajos de DEM de VMware.
 - 3 El orquestador de DEM de VMware.
 - 4 El servicio de VMware vCloud Automation Center.
- 4 Acceda a la consola de administración del dispositivo de vRealize Automation principal y actualice el dispositivo de vRealize Automation principal.

No se puede crear un nuevo directorio en vRealize Automation

Los intentos de agregar un nuevo directorio con el primer conector sincronizado no son correctos.

Problema

El problema se debe a un archivo `config-state.json` incorrecto ubicado en `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`.

Para obtener más información sobre cómo solucionar el problema, consulte el artículo [2145438 de la Base de conocimientos](#)

La actualización del dispositivo virtual de réplica de vRealize Automation agota el tiempo de espera

La actualización del dispositivo virtual de réplica de vRealize Automation agota el tiempo de espera cuando se actualiza el dispositivo virtual principal.

Problema

Al actualizar el dispositivo virtual principal, la pestaña de actualización de la consola de administración de vRealize Automation principal muestra un dispositivo virtual de réplica destacado que ha alcanzado el límite de tiempo de espera de actualización.

Causa

La actualización agota el tiempo de espera debido a un problema de rendimiento o de infraestructura.

Solución

- 1 Compruebe el progreso de actualización del dispositivo virtual de réplica.
 - a Vaya a la consola de administración del dispositivo virtual de réplica utilizando su nombre de dominio completo (FQDN), <https://va-hostname.domain.name:5480>.
 - b Inicie sesión con el nombre de usuario **root** y la contraseña que especificó cuando se implementó el dispositivo.
 - c Seleccione **Actualizar > Estado**, y compruebe el progreso de actualización.

Realice alguna de las siguientes acciones.

 - Si se produce un error en la actualización, siga los pasos del tema de solución de problemas [Error al actualizar el dispositivo de réplica de vRealize Automation](#).
 - Si la actualización del dispositivo virtual de réplica está en curso, espere hasta que finalice y vaya al paso 2.
- 2 Reinicie el dispositivo virtual.
 - a Haga clic en **Sistema**.
 - b Haga clic en **Reiniciar** y confirme la selección.
- 3 Seleccione **Configuración de vRA > Clúster**.
- 4 Introduzca el FQDN del dispositivo virtual de vRealize Automation principal, y haga clic en **Unirse a un clúster**.

En algunas máquinas virtuales, no se crea una implementación durante la actualización

Para las máquinas virtuales con el estado ausente en el momento de la actualización no se crea una implementación correspondiente en el entorno de destino.

Problema

Si una máquina virtual tiene el estado ausente en el entorno de origen durante la actualización, no se creará una implementación correspondiente en el entorno de destino. Si una máquina virtual sale del estado ausente después de la actualización, se podrá importar la máquina a la implementación de destino mediante la importación en bloque.

Error de certificado que no es de confianza

Al consultar la página Visor de logs de la infraestructura en la consola de Dispositivo de vRealize Automation, puede que vea un informe de error de conexión de endpoint que indique: `Certificate is not trusted`.

Problema

En la consola de Dispositivo de vRealize Automation, seleccione **Infraestructura > Supervisión > Log**. En la página Visor de logs, puede que vea un informe similar al siguiente:

Ha fallado la conexión con el endpoint. Para validar que se puede establecer una conexión segura con este endpoint, vaya al endpoint de vSphere en la página Endpoints y haga clic en el botón Probar conexión.

Excepción interna: El certificado no es de confianza (RemoteCertificateChainErrors). Subject: C=US, CN=vc6.mycompany.com Thumbprint: DC5A8816231698F4C9013C42692B0AF93D7E35F1

Causa

Al actualizar vRealize Automation 7.3 o versiones anteriores a la versión 7.4, se modifican los endpoints del entorno original. En los entornos actualizados recientemente a vRealize Automation 7.4, el administrador de IaaS debe revisar cada uno de los endpoints existentes que utilizan una conexión https segura. Si un endpoint presenta un error `Certificate is not trusted`, quiere decir que no funciona correctamente.

Solución

- 1 Inicie sesión en la consola de vRealize Automation como administrador de la infraestructura.
- 2 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 3 Siga estos pasos con cada endpoint que tenga una conexión segura.
 - a Haga clic en **Editar**.
 - b Haga clic en **Probar conexión**.
 - c Revise los detalles del certificado y haga clic en **Aceptar** si confía en él.
 - d Reinicie los servicios de Windows para todos los agentes de proxy de IaaS que usa este endpoint.
- 4 Compruebe que ya no aparecen más errores `Certificate is not trusted` en la página Visor de logs de la infraestructura.

Error al instalar o actualizar vRealize Automation

Al instalar o actualizar vRealize Automation, se produce un error y aparece un mensaje en el archivo de log.

Problema

Al instalar o actualizar vRealize Automation, se produce un error en el procedimiento. Por lo general, esto sucede cuando una corrección que se ha aplicado durante la instalación o la actualización no es correcta. Aparece un mensaje de error en el archivo de log similar al siguiente: Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.

Causa

El entorno de Windows tiene una política de grupo para la ejecución del script de PowerShell establecida en Habilitado.

Solución

- 1 En la máquina host de Windows, ejecute `gpedit.msc` para abrir el Editor de políticas de grupo local.
- 2 En el panel izquierdo, en la **configuración del equipo**, haga clic en el botón para expandir, de manera que se abra **Plantillas administrativas > Componentes de Windows > Windows PowerShell**.
- 3 Para **Activar la ejecución de scripts**, cambie el estado de Enabled a Not Configured.

No se pueden actualizar los componentes DEM y DEO

No se pueden actualizar los componentes DEM y DEO durante la actualización de vRealize Automation 7.2 a la versión 7.3.x.

Problema

Después de actualizar de vRealize Automation 7.2 a la versión 7.3.x, los componentes DEM y DEO instalados en la ruta personalizada (como la unidad D:) no se actualizan.

Consulte el [artículo 2150517 de la base de conocimientos](#).

La actualización no puede actualizar al agente de administración

Aparece un mensaje de error sobre el agente de administración cuando hace clic en **Instalar actualizaciones** en la página Estado de actualización de la consola de administración de Dispositivo de vRealize Automation.

Problema

El proceso de actualización no se realiza correctamente. Aparece el mensaje: No es posible actualizar el agente de administración en el nodo x. A veces, el mensaje muestra más de un nodo.

Causa

Este problema puede deberse a múltiples condiciones. El mensaje de error solo identifica el ID de nodo de la máquina afectada. Encontrará más información en el archivo All.log del agente de administración en la máquina donde el comando no se ejecuta correctamente.

Realice estas tareas en los nodos afectados según su situación:

Solución

- Si no se está ejecutando el servicio del agente de administración, inicie el servicio y reinicie la actualización en el dispositivo virtual.
- Si se está ejecutando el servicio del agente de administración y se actualiza el agente de administración, reinicie la actualización en el dispositivo virtual.
- Si se está ejecutando el servicio del agente de administración, pero no se actualiza el agente de administración, realice una actualización manual.
 - a Abra un navegador y vaya a la página de instalación de IaaS de vRealize Automation en el dispositivo vRealize Automation en `https:// va-hostname.domain.name:5480/install`.
 - b Descargue y ejecute el instalador del agente de administración.
 - c Reinicie el equipo del agente de administración.
 - d Reinicie la actualización en el dispositivo virtual.

La actualización del agente de administración no se realiza correctamente

La actualización del agente de administración no se realiza correctamente si se hace de vRealize Automation a la versión 7.2. o 7.3.x.

Problema

Si un incidente de conmutación por error ha intercambiado el host del agente de administración principal y secundario, la actualización no se realizará correctamente porque el proceso de actualización automatizado no puede encontrar el host esperado. Realice este procedimiento en cada nodo de IaaS en el que el agente de administración no esté actualizado.

Solución

- 1 Abra All.log en la carpeta de logs del agente de administración, situada en C:\Archivos de programa (x86)\VMware\VCAC\Management Agent\Log\.

La ubicación de la carpeta de instalación podría ser diferente a la ubicación predeterminada.

- 2 Busque en el archivo de log un mensaje sobre un dispositivo virtual apagado u obsoleto.

Por ejemplo, EXCEPCIÓN INTERNA: System.Net.WebException: No es posible conectar con el servidor remoto ---> System.Net.Sockets.SocketException: Se produjo un error durante el intento de conexión ya que la parte conectada no respondió adecuadamente tras un periodo de tiempo, o bien se produjo un error en la conexión establecida ya que el host conectado no ha podido responder.

Dirección_IP:5480

- 3 Edite el archivo de configuración del agente de administración en C:\Archivos de programa (x86)\VMware\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config para reemplazar el valor `alternativeEndpointaddress` existente con la URL del endpoint del dispositivo virtual principal.

La ubicación de la carpeta de instalación podría ser diferente a la ubicación predeterminada.

Ejemplo de `alternativeEndpointaddress` en `VMware.IaaS.Management.Agent.exe.config`.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="número de
miniatura" />
```

- 4 Reinicie el servicio Windows del agente de administración y compruebe el archivo `All.log` para verificar que esté trabajando.
- 5 Ejecute el procedimiento de actualización en el dispositivo de vRealize Automation principal.

Se produce un error de actualización de vRealize Automation debido a la configuración de tiempo de espera predeterminada

Si la configuración predeterminada de sincronización de bases de datos es demasiado limitada para el entorno, puede aumentar el ajuste de tiempo de actualización.

Problema

La configuración de tiempo de espera para el comando `SynchronizeDatabases` de `Vcac-Config` no es suficiente para algunos entornos en los que la sincronización de las bases de datos toma más que el valor predeterminado (3.600 segundos).

Los valores de propiedad `cafeTimeoutInSeconds` y `cafeRequestPageSize` del archivo `Vcac-Config.exe.config` rigen la comunicación entre la API y la herramienta de utilidad `Vcac-config.exe`. El archivo se encuentra en *Ubicación de instalación de IaaS\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config*.

Puede proporcionar un valor para estos parámetros opcionales para reemplazar el valor de tiempo de espera predeterminado de únicamente el comando `SynchronizeDatabases`.

| Parámetro | Nombre corto | Descripción |
|-------------------------------------|--------------------|--|
| <code>--DatabaseSyncTimeout</code> | <code>-dstm</code> | Establece el valor de tiempo de espera de solicitud HTTP en segundos solo para <code>SynchronizeDatabases</code> . |
| <code>--DatabaseSyncPageSize</code> | <code>-dsps</code> | Establece el tamaño de página de solicitud de sincronización solo para la sincronización de la reserva o de la política de reserva. El valor predeterminado es 10. |

Si no se establecen estos parámetros en el archivo `Vcac-Config.exe.config`, el sistema utiliza el valor de tiempo de espera predeterminado.

Error al actualizar IaaS en un entorno de alta disponibilidad

Se produce un error al ejecutar el proceso de actualización de IaaS en el nodo del servidor web principal con el equilibrio de carga habilitado. Es posible que aparezcan los siguientes mensajes de error: "System.Net.WebException: se agotó el tiempo de espera de la operación" o "401 - No autorizado: acceso denegado debido a credenciales no válidas".

Problema

Al actualizar IaaS con el equilibrio de carga habilitado, se puede producir un error intermitente. Cuando esto sucede, debe deshabilitar el equilibrio de carga y volver a ejecutar la actualización de vRealize Automation.

Solución

- 1 Revierta el entorno a los snapshots anteriores a la actualización.
- 2 Abra una conexión de escritorio remoto con el nodo del servidor web de IaaS principal.
- 3 Desplácese hasta el archivo de hosts de Windows en C:\windows\system32\drivers\etc.
- 4 Abra el archivo de hosts y añada esta línea para omitir el equilibrador de carga del servidor web.

dirección_IP_de_nodo_de_sitio_web_iaas_principal
FQDN_de_lb_de_sitio_web_iaas_de_vrealizeautomation

Ejemplo:

10.10.10.5 vra-iaas-web-lb.domain.com

- 5 Guarde el archivo de hosts y vuelva a intentar la actualización de vRealize Automation.
- 6 Cuando finalice la actualización de vRealize Automation, abra el archivo de hosts y quite la línea que añadió en el paso 4.

Solucionar problemas de actualización

Puede modificar el proceso de actualización para solucionar problemas de actualización.

Solución

Cuando experimente problemas al actualizar el entorno de vRealize Automation, utilice este procedimiento para modificar el proceso de actualización y seleccione una de las marcas disponibles.

Procedimiento

- 1 Abra una conexión de Secure Shell con el nodo del dispositivo de vRealize Automation principal.

- 2 En el símbolo del sistema, ejecute este comando para crear el archivo de alternancia:

touch available_flag

Por ejemplo: **touch /tmp/disable-iaas-upgrade**

Tabla 1-60. Marcas disponibles

| Marca | Descripción |
|-----------------------------|--|
| /tmp/disable-iaas-upgrade | <ul style="list-style-type: none"> ■ Impide el proceso de actualización de IaaS después de que se reinicia el dispositivo virtual. ■ Impide la actualización del agente de administración. ■ Impide las correcciones y comprobaciones de requisitos previos automáticas. ■ Impide la detención de los servicios de IaaS. |
| /tmp/do-not-upgrade-ma | Impide la actualización del agente de administración. Esta marca es adecuada cuando se actualiza el agente de administración de forma manual. |
| /tmp/skip-prereq-checks | Impide las correcciones y comprobaciones de requisitos previos automáticas. Esta marca es adecuada cuando hay un problema con las correcciones automáticas de requisitos previos y, en su lugar, las correcciones se han aplicado manualmente. |
| /tmp/do-not-stop-services | Impide la detención de los servicios de IaaS. La actualización no detiene los servicios de IaaS de Windows, como Manager Service, DEM y los agentes. |
| /tmp/do-not-upgrade-servers | <p>Impide la actualización automática de todos los componentes de IaaS de servidor, como la base de datos, el sitio web, la WAPI, el repositorio, los datos de Model Mfrontanager y Manager Service.</p> <p>Nota Esta marca también impide la habilitación del modo de conmutación por error automático de Manager Service.</p> |
| /tmp/do-not-upgrade-dems | Impide la actualización de DEM. |
| /tmp/do-not-upgrade-agents | Impide la actualización del agente de proxy de IaaS. |

3 Complete las tareas para la marca elegida.

Tabla 1-61. Tareas adicionales

| Marca | Tareas |
|-----------------------------|--|
| /tmp/disable-iaas-upgrade | <ul style="list-style-type: none"> ■ Actualice manualmente el agente de administración. ■ Aplique los requisitos previos de IaaS manualmente. ■ Detenga los servicios de IaaS de forma manual. <ol style="list-style-type: none"> a Inicie sesión en el servidor de Windows de IaaS. b Seleccione Inicio > Herramientas administrativas > Servicios. c Detenga los servicios en el siguiente orden. <p>Nota No desconecte el servidor de Windows de IaaS.</p> <ol style="list-style-type: none"> a Cada agente de proxy de VMware vRealize Automation. b Todos los trabajos de DEM de VMware. c El orquestador de DEM de VMware. d El servicio de VMware vCloud Automation Center. ■ Inicie la actualización de IaaS manualmente una vez completada la actualización del dispositivo virtual. |
| /tmp/do-not-upgrade-ma | Actualice manualmente el agente de administración. |
| /tmp/skip-prereq-checks | Aplique los requisitos previos de IaaS manualmente. |
| /tmp/do-not-stop-services | <p>Detenga los servicios de IaaS de forma manual.</p> <ol style="list-style-type: none"> 1 Inicie sesión en el servidor de Windows de IaaS. 2 Seleccione Inicio > Herramientas administrativas > Servicios. 3 Detenga los servicios en el siguiente orden. <p>Nota No desconecte el servidor de Windows de IaaS.</p> <ol style="list-style-type: none"> a Cada agente de proxy de VMware vRealize Automation. b Todos los trabajos de DEM de VMware. c El orquestador de DEM de VMware. d El servicio de VMware vCloud Automation Center. |
| /tmp/do-not-upgrade-servers | |
| /tmp/do-not-upgrade-dems | |
| /tmp/do-not-upgrade-agents | |

- 4 Acceda a la consola de administración del dispositivo de vRealize Automation principal y actualice el dispositivo de vRealize Automation principal.

Nota Debido a que cada marca permanece activa hasta que se la quita, ejecute este comando para quitar la marca elegida después de la actualización: `rm /flag_path/flag_name`. Por ejemplo, `rm /tmp/disable-iaas-upgrade`.

Actualizar de vRealize Automation 6.2.5 a 7.4

Cuando se actualiza el entorno de vRealize Automation 6.2.5 a la versión más reciente, se siguen unos procedimientos de actualización específicos del entorno 6.2.5.

Esta información es específica para la actualización de vRealize Automation 6.2.5 a la versión 7.4. Para obtener información sobre otras rutas de actualización admitidas, consulte [Actualizar vRealize Automation](#).

Actualizar de vRealize Automation 6.2.5 a 7.4

Puede realizar una actualización local del entorno actual de vRealize Automation 6.2.5 a la versión 7.4. Se utilizan los procedimientos de actualización específicos de esta versión para actualizar el entorno.

Una actualización local es un proceso compuesto de tres pasos. Los componentes se actualizan en el entorno actual en este orden.

- 1 Dispositivo de vRealize Automation
- 2 Servidor web de IaaS
- 3 vRealize Orchestrator

Debe actualizar todos los componentes de producto a la misma versión.

La herramienta de ayuda para la actualización vRealize Production Test analiza el entorno de vRealize Automation 6.2.x en busca de cualquier configuración de características que pueda causar problemas de actualización y, asimismo, comprueba que el entorno esté listo para la actualización. Para descargar esta herramienta y la documentación relacionada, vaya a la página de descarga del producto [Herramienta VMware vRealize Production Test](#).

Los controles del diccionario de propiedades que no se admiten tras la actualización se pueden restaurar mediante las relaciones del diccionario de propiedades y vRealize Orchestrator.

Si tiene flujos de trabajo en el entorno de origen que contienen código obsoleto, consulte la [guía de migración de extensibilidad de vRealize Automation](#), que incluye información sobre los cambios de código necesarios para la conversión a las suscripciones de agente de eventos.

A partir de vRealize Automation 7.2, JFrog Artifactory Pro ya no se incluye en el paquete con Dispositivo de vRealize Automation. Si actualiza desde una versión anterior de vRealize Automation, el proceso de actualización elimina JFrog Artifactory Pro. Para obtener más información, consulte el artículo [2147237 de la Base de conocimientos](#).

Nota Si ha personalizado el entorno actual de vRealize Automation 6.2.5, póngase en contacto con el personal de soporte de CCE para obtener más información acerca de la actualización.

Requisitos previos para actualizar vRealize Automation

Antes de actualizar desde vRealize Automation 6.2.5, revise los siguientes requisitos previos.

Requisitos de configuración del sistema

Compruebe que se cumplen los siguientes requisitos del sistema antes de iniciar una actualización.

- Compruebe que todos los dispositivos y los servidores que forman parte de la implementación cumplen los requisitos del sistema para la versión más reciente. Consulte *Matriz de compatibilidad de vRealize Automation* en la documentación de [VMware vRealize Automation](#).
- Consulte la *Matriz de interoperabilidad de productos de VMware* en el sitio web de VMware para obtener información sobre la compatibilidad con otros productos de VMware.
- Verifique que la versión de vRealize Automation desde la que está actualizando esté en una condición de trabajo estable. Solucione los problemas que pudiera haber antes de la actualización.
- Si actualiza desde vRealize Automation 6.2.5, registre la clave de licencia de vCloud Suite que utilice en su entorno de vRealize Automation actual. Al actualizar, las claves de licencia existentes se eliminan de la base de datos.
- Compruebe que haya cambiado la configuración de tiempo de espera del equilibrador de carga de forma predeterminada a 10 minutos como mínimo.

Requisitos de configuración de hardware

Compruebe que el hardware de su entorno sea adecuado para la versión de destino de vRealize Automation.

Consulte [Especificaciones del hardware y valores máximos de capacidad de vRealize Automation](#)

Compruebe que se cumplen los siguientes requisitos del sistema antes de iniciar una actualización.

- Debe configurar su hardware actual antes de descargar la actualización. Consulte [Aumentar los recursos de hardware de vCenter Server de vRealize Automation 6.2.5](#).
- Debe tener como mínimo 18 GB de RAM, 4 CPU, disco 1 = 50 GB, disco 3 = 25 GB y disco 4 = 50 GB antes de ejecutar la actualización.

Si la máquina virtual se encuentra en vCloud Networking and Security, puede que deba asignar más espacio de RAM.

Aunque ya no se ofrece soporte general para vCloud Networking and Security, las propiedades personalizadas de VCNS siguen siendo válidas para los fines de NSX. Consulte el [artículo 2144733 de la base de conocimientos](#).

- Estos nodos deben tener al menos 5 GB de espacio de disco libre:
 - Sitio web de IaaS principal
 - Base de datos de Microsoft SQL
 - Model Manager
- En el nodo del sitio web de IaaS principal en el que están instalados los datos de Model Manager se debe haber instalado Java SE Runtime Environment 8, actualización 161 (64 bits) o posterior. Después de instalar Java, debe establecer la variable de entorno JAVA_HOME en la nueva versión.
- Para descargar y ejecutar la actualización, debe disponer de los siguientes recursos:
 - 5 GB en la partición raíz como mínimo
 - 5 GB en la partición /storage/db para el Dispositivo de vRealize Automation principal
 - 5 GB en la partición raíz para cada dispositivo virtual de réplica
- Compruebe la subcarpeta /storage/log y quite cualquier archivo ZIP guardado anterior para liberar espacio.

Requisitos previos generales

Compruebe que se cumplen los siguientes requisitos del sistema antes de iniciar una actualización.

- Tiene acceso a una cuenta de Active Directory con el formato username@domain y con permisos para enlazar al directorio.
- Cumple las siguientes condiciones:
 - Tiene acceso a una cuenta con el formato nombreDeCuentaSAM.
 - Dispone de suficientes privilegios para unir el sistema al dominio (mediante la creación dinámica de un objeto informático) o para combinarlo en un objeto creado previamente.
- Tiene acceso a todas las bases de datos y todos los equilibradores de carga a los que afecta la actualización de vRealize Automation o que participan en esta.
- El sistema no estará disponible para los usuarios mientras se lleva a cabo la actualización.
- Ha deshabilitado las aplicaciones que realizan consultas en vRealize Automation.
- Compruebe que el Coordinador de transacciones distribuidas de Microsoft (MSDTC) está habilitado en todos los servidores SQL asociados y de vRealize Automation. Para obtener instrucciones, consulte [el artículo 2089503 de la base de conocimientos](#).
- Si el entorno tiene un dispositivo de vRealize Orchestrator externo y un dispositivo de vRealize Orchestrator externo conectados a Identity Appliance, actualice vRealize Orchestrator antes de actualizar vRealize Automation.

- Antes de la actualización, debe completar las tareas adicionales para preparar las máquinas virtuales de vRealize Automation. Antes de actualizar, revise el [artículo 51531 de la base de conocimientos](#).
- Compruebe que haya cambiado la configuración de tiempo de espera del equilibrador de carga de forma predeterminada a 10 minutos como mínimo.
- Si utiliza el complemento DynamicTypes, debe exportar las configuraciones del complemento DynamicTypes de vRealize Orchestrator como un flujo de trabajo del paquete.
`/Library/Dynamic Types/Configuration/Export Configuration As Package`
- Haga lo siguiente si va a actualizar un entorno distribuido configurado con una base de datos de PostgreSQL integrada.
 - a Examine los archivos en el directorio pgdata del host principal antes de actualizar los hosts de réplica.
 - b Acceda a la carpeta de datos de PostgreSQL en el host principal en `/var/vmware/vpostgres/current/pgdata/`.
 - c Cierre los archivos que tenga abiertos en el directorio pgdata y quite los archivos que tengan el sufijo `.swp`.
 - d Compruebe que todos los archivos en este directorio tengan la propiedad correcta: `postgres:users`.

Consideraciones sobre actualizar a esta versión de vRealize Automation

vRealize Automation 7 y las versiones posteriores incorporan una serie de cambios funcionales durante y después del proceso de actualización. Debe revisar los cambios antes de actualizar la implementación de vRealize Automation 6.2.5 a la nueva versión.

Revise estas consideraciones antes de actualizar.

Actualizar y especificaciones de Identity Appliance

Durante el proceso de actualización de vRealize Automation, hay que responder a algunos mensajes para actualizar Identity Appliance.

La implementación de destino usa VMware Identity Manager.

Actualización y licencias

Durante la actualización, se eliminan las licencias existentes de vRealize Automation 6.2.5 y cualquier licencia de vCloud Suite 6.x que tenga. Debe volver a introducir las licencias en la consola de administración de dispositivos de vRealize Automation 7.4.vRealize Automation

Ahora debe usar la licencia de vRealize Automation para dispositivos virtuales e IaaS introduciendo la información de la clave de licencia en el dispositivo de vRealize Automation. La información de licencia ya no está disponible en la interfaz de usuario de IaaS y IaaS ya no puede realizar comprobaciones de licencias. Los endpoints y las cuotas se aplican mediante los contratos de licencia para el usuario final (EULA).

Nota Anote su clave de licencia de vCloud Suite 6.x si la ha utilizado para vRealize Automation 6.2.5 antes de actualizar. Al actualizar, las claves de licencia existentes se eliminan de la base de datos.

Para obtener más información sobre cómo volver a introducir la información de licencia durante la actualización o después de esta, consulte [Actualizar la clave de licencia](#).

Conocer cómo se actualizan las funciones

Cuando se actualiza vRealize Automation, las asignaciones de función existentes de la organización se conservan. La actualización también crea algunas asignaciones de función para admitir las funciones de los arquitectos de blueprints adicionales.

Las siguientes funciones de los arquitectos se usan para admitir la definición de blueprints en el lienzo de diseño:

- Arquitecto de aplicaciones: ensambla componentes y blueprints existentes para crear blueprints compuestos.
- Arquitecto de infraestructura. Crea y administra blueprints de máquina virtual.
- Arquitecto de XaaS: crea y administra blueprints de XaaS.
- Arquitecto de software: crea y administra componentes de Software.

En vRealize Automation 7, los administradores de tenants y los administradores de grupo empresarial no pueden diseñar blueprints de forma predeterminada. A los administradores de tenants y los administradores de grupo empresarial actualizados se les asigna la función de arquitecto de infraestructura.

Los usuarios que pueden reconfigurar una máquina virtual en la versión de origen de vRealize Automation 6.2.x pueden cambiar la propiedad de la máquina virtual después de actualizar a la nueva versión.

Estas son las asignaciones de función que se realizan durante la actualización. Las funciones que no aparecen en la tabla se actualizan a la función con el mismo nombre en la implementación de destino.

Tabla 1-62. Funciones asignadas durante la actualización

| Función en la implementación de origen | Función en la implementación de destino |
|--|--|
| Administrador de tenants | Administrador de tenants y arquitecto de infraestructura |
| Administrador de grupo empresarial | Administrador de grupo empresarial y arquitecto de infraestructura |

Tabla 1-62. Funciones asignadas durante la actualización (Continuación)

| Función en la implementación de origen | Función en la implementación de destino |
|--|---|
| Arquitecto del servicio | Arquitecto de XaaS |
| Arquitecto de aplicaciones | Arquitecto de software |

Para obtener más información sobre las funciones, consulte [Tenant Roles and Responsibilities in vRealize Automation](#) (Funciones y responsabilidades de los tenants en vRealize Automation).

Conocer cómo se actualizan los blueprints

Como regla general, los blueprints publicados se actualizan como blueprints publicados.

No obstante, hay excepciones a esa regla. Los blueprints de varias máquinas se actualizan como blueprints compuestos que contienen componentes de blueprints. Los blueprints que contienen configuraciones no compatibles se actualizan como no publicados.

Nota vRealize Automation 7.x crea una snapshot del blueprint en la implementación. Si tiene problemas de reconfiguración al actualizar las propiedades de la máquina, como la CPU y la RAM en una implementación, consulte el artículo de la base de conocimientos [2150829: Creación de snapshots de blueprint vRA 7.x](#).

Para obtener más información sobre cómo se actualizan los blueprints, consulte [Actualizar y blueprints de vApp, endpoints de vCloud y reservas de vCloud](#) y [Conocer cómo se actualizan los blueprints de varias máquinas](#).

Actualizar y blueprints de vApp, endpoints de vCloud y reservas de vCloud

No puede actualizar una implementación que contenga endpoints de vApp (vCloud). La presencia de endpoints de vApp (vCloud) impide la actualización a esta versión de vRealize Automation.

La actualización no se produce en el dispositivo virtual principal si hay un endpoint de vApp (vCloud) en la implementación de origen. Aparece un mensaje tanto en el log como en la interfaz de usuario. Para averiguar si la implementación de origen contiene un endpoint de vApp (vCloud), inicie sesión en la consola de vRealize Automation como usuario administrador de IaaS. Seleccione **Infraestructura > Endpoints**. Si la lista de endpoints contiene endpoints de vApp (vCloud), no puede actualizar a esta versión de vRealize Automation.

Las vApps administradas para recursos de vCloud Air o vCloud Director no se admiten en el entorno de vRealize Automation de destino.

Nota Los siguientes tipos de política de aprobación están obsoletos. Si, al finalizar la actualización, figuran en la lista de tipos de políticas de aprobación disponibles, no se pueden usar.

- Catálogo de servicios - Solicitud de elemento del catálogo - vApp
- Catálogo de servicios - Solicitud de elemento del catálogo - Componente de vApp

Puede crear endpoints de vCloud Air y vCloud Director y reservas en la implementación de destino. También puede crear blueprints con componentes de máquina virtual de vCloud Air o vCloud Director.

Conocer cómo se actualizan los blueprints de varias máquinas

Puede actualizar el servicio administrado y los blueprints de varias máquinas desde una implementación de vRealize Automation 6.2.x compatible.

Cuando actualice un blueprint de varias máquinas, los blueprints de componentes se actualizarán como blueprints para una sola máquina. El blueprint de varias máquinas se actualiza como blueprint compuesto en el que están anidados sus blueprints secundarios como componentes de blueprint independientes.

La actualización crea un solo blueprint compuesto en la implementación de destino que contiene un componente de máquina virtual por cada blueprint de componente del blueprint de varias máquinas de origen. Si un blueprint tiene una configuración que no se admite en la nueva versión, dicho blueprint se actualiza y se establece en estado de borrador. Por ejemplo, si el blueprint de varias máquinas contiene un perfil de red privada, la actualización omite la configuración del perfil y el blueprint se actualiza y pone en un estado de borrador. El borrador del blueprint se puede editar para especificar información de perfil de red compatible y publicarlo.

Nota Si un blueprint publicado en la implementación de origen se actualiza al estado de borrador, este dejará de formar parte de un servicio o una autorización. Tras actualizar y publicar el blueprint en la versión actualizada de vRealize Automation, debe volver a crear las políticas de aprobación y las autorizaciones.

Algunas configuraciones de blueprint de varias máquinas no se admiten en la implementación de vRealize Automation de destino, incluidos los perfiles de red privados y los perfiles de red enrutados con configuraciones de PLR edge asociadas. Si ha usado una propiedad personalizada para especificar la configuración de PLR edge (`VCNS.LoadBalancerEdgePool.Names`), la propiedad personalizada se actualiza.

Puede actualizar un blueprint de varias máquinas con endpoints de vSphere y la configuración de red y seguridad de NSX. El blueprint actualizado contiene los componentes de red y seguridad de NSX en el lienzo de diseño.

Nota Las especificaciones de puerta de enlace enrutada de los blueprints de varias máquinas, tal como se definen en las reservas, se actualizan. Sin embargo, la implementación de vRealize Automation de destino no es compatible con las reservas de los perfiles enrutados que contienen configuraciones asociadas de PLR edge. Si la reserva de origen contiene un valor de puerta de enlace enrutada para un perímetro PLR, se actualizará, pero la configuración de puerta de enlace enrutada se omitirá. Como resultado, la actualización generará un mensaje de error en el archivo log y se deshabilitará la reserva.

Durante la actualización, los espacios y los caracteres especiales se eliminan de la red a la que se hace referencia y de los nombres de componentes de seguridad.

Nota vRealize Automation 7.x crea una snapshot del blueprint en la implementación. Si tiene problemas de reconfiguración al actualizar las propiedades de la máquina, como la CPU y la RAM en una implementación, consulte el artículo de la base de conocimientos [2150829: Creación de snapshots de blueprint vRA 7.x](#).

En función del tipo de configuración, la información de red y seguridad se plasmará como varias configuraciones distintas en el nuevo blueprint.

- Configuración del blueprint general en la página de propiedades. Esta información incluye el aislamiento de aplicaciones, la zona de transporte y la puerta de enlace enrutada o la información de la política de reserva del perímetro de NSX.
- Configuración disponible para los componentes de máquina virtual de vSphere en los componentes de red y seguridad de NSX en el lienzo de diseño.
- Configuración en las pestañas de red y seguridad de los componentes de máquina virtual de vSphere individuales en el lienzo de diseño.

Actualizar y reservas, blueprints y endpoints físicos

No puede actualizar una implementación que contenga endpoints físicos. Si hay endpoints físicos, el proceso de actualización de vRealize Automation no se lleva a cabo.

La actualización no se produce en el dispositivo virtual principal cuando la implementación de vRealize Automation 6.2.x tiene un endpoint físico. Aparece un mensaje de error tanto en el log como en la interfaz de migración. Para averiguar si la implementación de vRealize Automation 6.2.x tiene un endpoint físico, inicie sesión en vRealize Automation como un usuario administrador de IaaS. Seleccione **Infraestructura > Endpoints** y revise la lista de endpoints. Si la lista tiene un endpoint de Platform Type `Physical`, no puede actualizar a vRealize Automation 7,0 y versiones posteriores.

Los endpoints físicos, las reservas y los componentes de máquina virtual no son compatibles con vRealize Automation 7,0 y versiones posteriores.

Actualización y configuración del perfil de red

Los perfiles de red privada no son compatibles con vRealize Automation 7 y versiones posteriores. Estos perfiles se omitirán durante la actualización. Los perfiles de red enrutada con configuración de PLR edge asociada tampoco son compatibles con vRealize Automation 7 y versiones posteriores. Estos perfiles también se omitirán durante la actualización.

El tipo de perfil de red privada no es compatible con vRealize Automation 7 y versiones posteriores. Cuando el proceso de actualización de vRealize Automation detecta un perfil de red privada en la implementación de origen, lo omite. Los equilibradores de carga que hacen referencia a esas redes privadas también se ignoran durante la actualización. Las mismas condiciones de actualización son verdaderas para un perfil de red enrutado con una configuración de PLR edge asociada. Tampoco se actualiza la configuración del perfil de red.

Si una reserva contiene un perfil de red privada, la configuración de perfil de red privada se omite durante la actualización y la reserva se actualiza como deshabilitada en la implementación de destino.

Si una reserva contiene un perfil de red enrutada con una configuración de PLR edge asociada, la especificación de perfil de red enrutada se omite durante la actualización y la reserva se actualiza como deshabilitada en la implementación de destino.

Para obtener información sobre la actualización de un blueprint de varias máquinas que contiene una configuración de red, consulte [Conocer cómo se actualizan los blueprints de varias máquinas](#).

Actualizar y acciones autorizadas

Las acciones de máquina virtual no se pueden actualizar.

Las acciones que se pueden llevar a cabo en las máquinas virtuales aprovisionadas según las especificaciones del blueprint no se actualizan. Si desea volver a crear las acciones que se pueden realizar en una máquina virtual, personalice las autorizaciones de los blueprints para permitir solo ciertas acciones.

Para obtener más información relacionada, consulte [Actions in Entitlements](#) (Acciones en autorizaciones).

Actualizar y propiedades personalizadas

Todas las propiedades personalizadas que vRealize Automation proporciona están disponibles en la implementación actualizada. Se actualizan las propiedades personalizadas y los grupos de propiedades.

Terminología y cambios relacionados

Todos los perfiles de compilación que haya creado en la implementación de origen se actualizan como grupos de propiedades. El término *perfil de compilación* se ha retirado.

El término *grupo de propiedades* se ha retirado y los archivos del grupo de propiedades de CSV ya no están disponibles.

Distinción entre mayúsculas y minúsculas en los nombres de propiedades personalizadas

Antes de vRealize Automation 7.0, en los nombres de las propiedades personalizadas se distinguía entre mayúsculas y minúsculas. En vRealize Automation 7.0 y versiones posteriores, los nombres de las propiedades personalizadas distinguen mayúsculas de minúsculas. Durante la actualización, los nombres de las propiedades personalizadas deben coincidir exactamente. De esta forma, lo que se consigue es que los valores de propiedad no se reemplacen entre sí y que coincidan con las definiciones del diccionario de propiedades. Por ejemplo, una propiedad personalizada `hostname` y otra propiedad personalizada `HOSTNAME` serán propiedades personalizadas distintas en vRealize Automation 7.0 y versiones posteriores. La propiedad personalizada `hostname` y la propiedad personalizada `HOSTNAME` no se reemplazan entre sí durante la actualización.

Espacios en los nombres de las propiedades personalizadas

Antes de actualizar a esta versión de vRealize Automation, elimine los caracteres de espacio que haya en los nombres de la propiedad personalizada (por ejemplo, puede reemplazar el espacio con un carácter de subrayado) para permitir que la propiedad personalizada se reconozca en la instalación de vRealize Automation actualizada. Los nombres de la propiedad personalizada de vRealize Automation no pueden contener espacios. Este problema también puede afectar al uso de una instalación de vRealize Orchestrator actualizada que utiliza propiedades personalizadas que contenían espacios en las versiones anteriores de vRealize Automation o de vRealize Orchestrator o de ambos.

Nombres de propiedades reservados

Como ahora se reservan varias palabras clave, algunas propiedades actualizadas pueden verse afectadas. Algunas palabras clave que se utilizan en el código de blueprint se pueden importar, por ejemplo, mediante las funciones de importación de blueprint de vRealize CloudClient. Esas palabras clave se consideran reservadas y no están disponibles para propiedades que se están actualizando. Las palabras clave incluyen, entre otras, `cpu`, `storage` y `memory`.

Actualizar y servicios de aplicación

Application Services se puede actualizar en vRealize Automation 7 y las versiones posteriores.

Después de realizar correctamente la migración a vRealize Automation 7.4, puede utilizar la herramienta de migración de servicios de aplicación de vRealize Automation para actualizar sus servicios de aplicación. Siga estos pasos para descargar la herramienta.

- 1 Haga clic en [Descargar VMware vRealize Automation](#).
- 2 Seleccione **Controladores y herramientas > Herramienta de migración de VMware vRealize Application Services**.

Actualizar y diseño de servicios avanzado

Cuando vRealize Automation 7 o posterior se actualiza, los elementos de diseño de servicio avanzado se actualizan a elementos XaaS.

Los componentes de XaaS están disponibles para su uso en el lienzo de diseño.

Actualizar la información de precios de blueprint

A partir de la versión 7.0, los perfiles de precios de vRealize Automation ya no se admiten y no se migran a la implementación de destino durante la actualización. No obstante, puede usar la integración mejorada con vRealize Business for Cloud para gestionar los gastos de recursos de vRealize Automation.

vRealize Business for Cloud ahora está estrechamente integrado con vRealize Automation y admite las siguientes funciones de precios mejoradas.

- Ubicación unificada en vRealize Business for Cloud para definir las directivas de precios flexibles para:
 - Blueprints de recursos, máquinas y aplicaciones de infraestructura
 - Máquinas virtuales aprovisionadas en vRealize Automation para los endpoints admitidos, como vCenter Server, vCloud Director, Amazon Web Services, Azure y OpenStack.
 - Cualquier precio operativo, precio único y precio de las propiedades personalizadas de las máquinas virtuales aprovisionadas
 - Implementaciones, que incluyen el precio de las máquinas virtuales contenidas en las implementaciones.
- Informes de distribución de costes basados en funciones en vRealize Business for Cloud
- Aprovechamiento completo de las nuevas funciones de vRealize Business for Cloud

Antes de actualizar, puede exportar los informes de gastos existentes desde la instancia de vRealize Automation de origen como referencia. Tras completar la actualización, puede instalar y configurar vRealize Business for Cloud para gestionar los precios.

Nota vRealize Automation 7.4 solamente es compatible con vRealize Business for Cloud 7.4 y versiones posteriores.

Actualización y elementos de catálogo

Después de actualizar desde vRealize Automation 6.2. x a la versión más reciente, algunos elementos de catálogo aparecen en el catálogo de servicios pero no están disponibles para solicitarlos.

Después de migrar a la versión más reciente de vRealize Automation, los elementos de catálogo que utilizan estas definiciones de propiedades aparecen en el catálogo de servicios, pero no están disponibles para solicitarlos.

- Tipos de control: casilla de verificación o vínculo.
- Atributos: relación, expresiones regulares o diseños de propiedades.

En vRealize Automation 7.x, las definiciones de propiedad ya no utilizan estos elementos. Debe recrear la definición de propiedad o configurar la definición de propiedad para utilizar una acción de script de vRealize Orchestrator en lugar de los tipos de control incrustado o atributos. Para obtener más información, consulte [Los elementos del catálogo aparecen en el catálogo de servicios después de la actualización, pero no están disponibles para solicitarse](#).

Lista de comprobación para actualizar vRealize Automation

Cuando se actualiza vRealize Automation de la versión 6.2.5 a la 7.4, se actualizan todos los componentes de vRealize Automation en un orden específico.

Utilice las listas de comprobación para realizar un seguimiento de su trabajo a medida que se completa la actualización. Finalice las tareas en el orden en que aparecen.

Nota Debe actualizar todos los componentes en el orden establecido. Si sigue un orden distinto, podría provocar un comportamiento inesperado después de la actualización o la actualización podría no completarse correctamente.

El orden de la actualización varía en función de si está actualizando un entorno mínimo o un entorno distribuido con varios dispositivos de vRealize Automation.

Tabla 1-63. Lista de comprobación para actualizar un entorno mínimo de vRealize Automation

| Tarea | Instrucciones |
|--|--|
| <p> Realizar una copia de la instalación actual. Hacer esta copia de seguridad es una tarea crítica.</p> | <p>Para obtener más información sobre cómo crear una copia de seguridad del sistema y restaurarlo, consulte Hacer una copia de seguridad del entorno de vRealize Automation 6.2.5 existente.</p> <p>Para obtener información general, consulte <i>Configurar la copia de seguridad y la restauración mediante Symantec Netbackup</i> en http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf.</p> |
| <p> Prepare las máquinas virtuales de vRealize Automation 6.2.x para actualizarlas.</p> | <p>Debe revisar el artículo 51531 de la base de conocimientos y realizar las correcciones que correspondan a sus entornos antes de realizar la actualización.</p> |
| <p> Desconectar los servicios de Windows de vRealize Automation en el servidor de IaaS.</p> | <p>Consulte Detener los servicios de vRealize Automation en el servidor Windows de IaaS.</p> |
| <p> Si el Catálogo de componentes comunes está instalado, debe desinstalarlo antes de actualizar.</p> | <p>Para obtener información sobre cómo desinstalar componentes del Catálogo de componentes comunes, consulte la <i>guía de instalación del Catálogo de componentes comunes</i>.</p> <p>Si esta guía no está disponible, haga lo siguiente en cada nodo IaaS.</p> <ol style="list-style-type: none"> 1 Inicie sesión en el nodo de IaaS. 2 Haga clic en Iniciar. 3 Introduzca servicios en el cuadro de texto Buscar programas y archivos. 4 Haga clic en Servicios. 5 En el panel de la derecha de la ventana Servicios, haga clic con el botón derecho en cada servicio de IaaS y seleccione Detener para detener cada servicio. 6 Haga clic en Iniciar > Panel de control > Programas y características. 7 Haga clic con el botón derecho en cada componente del Catálogo de componentes comunes instalado y seleccione Desinstalar. 8 Haga clic en Iniciar > Símbolo del sistema. 9 En el símbolo del sistema, ejecute iisreset. |
| <p> Revisar las consideraciones de actualización a esta versión de vRealize Automation con objeto de saber qué se puede actualizar y qué no, así como las diferencias de comportamiento de los elementos actualizados.</p> <p>No todos los elementos, incluidos los blueprints, las reservas y los endpoints, pueden actualizarse. La presencia de algunas configuraciones no admitidas bloquea la actualización.</p> | <p>Consulte Consideraciones sobre actualizar a esta versión de vRealize Automation.</p> |
| <p> Configurar los recursos de hardware.</p> | <p>Consulte Aumentar los recursos de hardware de vCenter Server de vRealize Automation 6.2.5.</p> |

Tabla 1-63. Lista de comprobación para actualizar un entorno mínimo de vRealize Automation (Continuación)

| Tarea | Instrucciones |
|---|---|
| <input type="checkbox"/> Descargar actualizaciones en el dispositivo de vRealize Automation. | Consulte Descargar actualizaciones del dispositivo de vRealize Automation . |
| <input type="checkbox"/> Instalar la actualización en el dispositivo de vRealize Automation. | Consulte Instalar la actualización en el dispositivo de vRealize Automation . |
| <input type="checkbox"/> Actualizar la utilidad Single Sign-On a la utilidad VMware Identity Manager. | Consulte Actualizar la contraseña de Single Sign-On para VMware Identity Manager . |
| <input type="checkbox"/> Actualizar la clave de licencia. | Consulte Actualizar la clave de licencia . |
| <input type="checkbox"/> Migrar el almacén de identidades a VMware Identity Manager. | Migración de almacenes de identidades a VMware Identity Manager |
| <input type="checkbox"/> Actualizar los componentes de IaaS. | Consulte Actualizar los componentes del servidor de IaaS tras actualizar vRealize Automation . |
| <input type="checkbox"/> Actualizar la instancia externa de vRealize Orchestrator. | Consulte Actualizar el dispositivo independiente de vRealize Orchestrator para su uso con vRealize Automation . Consulte Actualizar el clúster de dispositivo externo de vRealize Orchestrator para su uso con vRealize Automation |
| <input type="checkbox"/> Añadir usuarios o grupos a una conexión de Active Directory. | Consulte Añadir usuarios o grupos a una conexión de Active Directory . |

Tabla 1-64. Lista de comprobación para actualizar un entorno distribuido de vRealize Automation

| Tarea | Instrucciones |
|---|---|
| <input type="checkbox"/> Realizar una copia de la instalación actual. Hacer esta copia de seguridad es una tarea crítica. | Para obtener más información sobre cómo crear una copia de seguridad del sistema y restaurarlo, consulte Hacer una copia de seguridad del entorno de vRealize Automation 6.2.5 existente . Para obtener información detallada, consulte <i>Configurar la copia de seguridad y la restauración mediante Symantec Netbackup</i> en http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf . |
| <input type="checkbox"/> Prepare las máquinas virtuales de vRealize Automation 6.2.x para actualizarlas. | Debe revisar el artículo 51531 de la base de conocimientos y realizar las correcciones que correspondan a sus entornos antes de realizar la actualización. |
| <input type="checkbox"/> Desconectar los servicios de vRealize Automation en los servidores de Windows de IaaS. | Consulte Detener los servicios de vRealize Automation en el servidor Windows de IaaS . |

Tabla 1-64. Lista de comprobación para actualizar un entorno distribuido de vRealize Automation (Continuación)

| Tarea | Instrucciones |
|---|--|
| <p> Si el Catálogo de componentes comunes está instalado, debe desinstalarlo antes de actualizar.</p> | <p>Para obtener información sobre cómo desinstalar componentes del Catálogo de componentes comunes, consulte la <i>guía de instalación del Catálogo de componentes comunes</i>.</p> <p>Si esta guía no está disponible, haga lo siguiente en cada nodo IaaS.</p> <ol style="list-style-type: none"> 1 Inicie sesión en el nodo de IaaS. 2 Haga clic en Iniciar. 3 Introduzca servicios en el cuadro de texto Buscar programas y archivos. 4 Haga clic en Servicios. 5 En el panel de la derecha de la ventana Servicios, haga clic con el botón derecho en cada servicio de IaaS y seleccione Detener para detener cada servicio. 6 Haga clic en Iniciar > Panel de control > Programas y características. 7 Haga clic con el botón derecho en cada componente del Catálogo de componentes comunes instalado y seleccione Desinstalar. 8 Haga clic en Iniciar > Símbolo del sistema. 9 En el símbolo del sistema, ejecute iisreset. |
| <p> Configurar los recursos del hardware para la actualización.</p> | <p>Consulte Aumentar los recursos de hardware de vCenter Server de vRealize Automation 6.2.5.</p> |
| <p> Deshabilitar los equilibradores de carga.</p> | <p>Deshabilite cada nodo secundario y quite los supervisores de estado de vRealize Automation de los siguientes elementos.</p> <ul style="list-style-type: none"> ■ Dispositivo de vRealize Automation ■ Sitio web de IaaS ■ IaaS Manager Service <p>Compruebe lo siguiente para confirmar que la actualización es correcta:</p> <ul style="list-style-type: none"> ■ El tráfico del equilibrador de carga se dirige únicamente al nodo principal. ■ Los supervisores de estado de vRealize Automation se han quitado del dispositivo, del sitio web y de Manager Service. |
| <p> Descargar actualizaciones en el dispositivo de vRealize Automation.</p> | <p>Consulte Descargar actualizaciones del dispositivo de vRealize Automation.</p> |
| <p> Instalar la actualización en el primer dispositivo de vRealize Automation de la instalación. Si ha designado un dispositivo como principal, en primer lugar actualice ese dispositivo.</p> | <p>Consulte Instalar la actualización en el dispositivo de vRealize Automation.</p> |
| <p> Actualizar la utilidad Single Sign-On a la utilidad VMware Identity Manager.</p> | <p>Consulte Actualizar la contraseña de Single Sign-On para VMware Identity Manager.</p> |
| <p> Actualizar la clave de licencia.</p> | <p>Consulte Actualizar la clave de licencia.</p> |

Tabla 1-64. Lista de comprobación para actualizar un entorno distribuido de vRealize Automation (Continuación)

| Tarea | Instrucciones |
|--|---|
| <input type="checkbox"/> Migrar el almacén de identidades a la utilidad VMware Identity Manager. | Migración de almacenes de identidades a VMware Identity Manager |
| <input type="checkbox"/> Instalar la actualización en el resto de dispositivos de vRealize Automation. | Instalar la actualización en dispositivos adicionales de vRealize Automation |
| <input type="checkbox"/> Actualizar los componentes de IaaS. | Consulte Actualizar los componentes del servidor de IaaS tras actualizar vRealize Automation . |
| <input type="checkbox"/> Actualizar la instancia externa de vRealize Orchestrator. | Consulte Actualizar el dispositivo independiente de vRealize Orchestrator para su uso con vRealize Automation . Consulte Actualizar el clúster de dispositivo externo de vRealize Orchestrator para su uso con vRealize Automation |
| <input type="checkbox"/> Habilitar los equilibradores de carga. | Configurar los equilibradores de carga |

Interfaces de usuario del entorno de vRealize Automation

El entorno de vRealize Automation se utiliza y administra con varias interfaces.

Interfaces de usuario

En estas tablas se describen las interfaces que se usan para administrar el entorno de vRealize Automation.

Tabla 1-65. Consola de administración de vRealize Automation

| Propósito | Acceso | Credenciales necesarias |
|---|---|---|
| <p>La consola de vRealize Automation se emplea para las siguientes tareas de administrador del sistema.</p> <ul style="list-style-type: none"> ■ Agregar tenants. ■ Personalizar la interfaz de usuario de vRealize Automation. ■ Configurar los servidores de correo electrónico. ■ Ver logs de eventos. ■ Configure vRealize Orchestrator. | <ol style="list-style-type: none"> 1 Inicie un navegador y abra la página de presentación del dispositivo de vRealize Automation con el nombre de dominio completo del dispositivo virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Haga clic en Consola de vRealize Automation. También puede utilizar la siguiente dirección URL para abrir la consola de vRealize Automation: <code>https://vra-va-hostname.domain.name/vcac</code> 3 Inicie sesión. | <p>Debe ser un usuario con la función de administrador del sistema.</p> |

Tabla 1-66. Consola de tenant de vRealize Automation . Esta es la interfaz de usuario principal que se utiliza para crear y administrar servicios y recursos.

| Propósito | Acceso | Credenciales necesarias |
|---|---|---|
| <p>vRealize Automation se usa para las siguientes tareas.</p> <ul style="list-style-type: none"> ■ Solicitar nuevos blueprints de servicio de TI. ■ Crear y administrar recursos de TI y de nube. ■ Crear y administrar grupos personalizados. ■ Cree y administre grupos empresariales. ■ Asignar funciones a los usuarios. | <ol style="list-style-type: none"> 1 Inicie un navegador e introduzca la dirección URL de los tenants con el nombre de dominio completo del dispositivo virtual y el nombre de la URL de tenant: <code>https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name .</code> 2 Inicie sesión. | <p>Debe ser un usuario con una o varias de las siguientes funciones:</p> <ul style="list-style-type: none"> ■ Arquitecto de aplicaciones ■ Administrador de aprobaciones ■ Administrador del catálogo ■ Administrador de contenedores ■ Arquitecto de contenedores ■ Consumidor de estado ■ Arquitecto de infraestructura ■ Consumidor de exportación segura ■ Arquitecto de software ■ Administrador de tenants ■ Arquitecto XaaS |

Tabla 1-67. Administración de dispositivos de vRealize Automation . Esta interfaz a veces se denomina interfaz de administración de dispositivos virtuales (Virtual Appliance Management Interface, VAMI).

| Propósito | Acceso | Credenciales necesarias |
|---|--|--|
| <p>La administración de dispositivos de vRealize Automation se usa para las siguientes tareas:</p> <ul style="list-style-type: none"> ■ Ver el estado de los servicios registrados. ■ Ver información del sistema y reiniciar o apagar el dispositivo. ■ Administrar la participación en el programa de mejora de la experiencia del cliente. ■ Ver el estado de la red. ■ Ver el estado de actualización e instalar actualizaciones. ■ Administrar la configuración de administración. ■ Administrar la configuración del host de vRealize Automation. ■ Administrar la configuración de SSO. ■ Administrar las licencias del producto. ■ Configurar la base de datos de Postgres de vRealize Automation. ■ Configurar la mensajería de vRealize Automation. ■ Configure el registro de vRealize Automation. ■ Instalar componentes de IaaS. ■ Migrar desde una instalación de vRealize Automation existente. ■ Administrar certificados de componentes de IaaS. ■ Configurar el servicio Xenon. | <ol style="list-style-type: none"> 1 Inicie un navegador y abra la página de presentación del dispositivo de vRealize Automation con el nombre de dominio completo del dispositivo virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Haga clic en Administración de dispositivos de vRealize Automation. También puede utilizar la siguiente dirección URL para abrir la administración de dispositivos de vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Inicie sesión. | <ul style="list-style-type: none"> ■ Nombre de usuario: raíz. ■ Contraseña: la contraseña que ha introducido al implementar el dispositivo de vRealize Automation. |

Tabla 1-68. Cliente de vRealize Orchestrator

| Propósito | Acceso | Credenciales necesarias |
|--|---|---|
| <p>El cliente de vRealize Orchestrator se usa para realizar las siguientes tareas:</p> <ul style="list-style-type: none"> ■ Desarrollar acciones. ■ Desarrollar flujos de trabajo. ■ Administrar políticas. ■ Instalar paquetes. ■ Administrar permisos de usuarios y de grupos de usuarios. ■ Asociar etiquetas a objetos de URI. ■ Ver el inventario. | <ol style="list-style-type: none"> 1 Inicie un navegador y abra la página de presentación de vRealize Automation con el nombre de dominio completo del dispositivo virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Para descargar el archivo <code>client.jnlp</code> en el equipo local, haga clic en Cliente de vRealize Orchestrator. 3 Haga clic con el botón derecho en el archivo <code>client.jnlp</code> y seleccione Iniciar. 4 En el cuadro de diálogo <i>¿Desea continuar?</i>, haga clic en Continuar. 5 Inicie sesión. | <p>Debe ser un usuario con la función de administrador del sistema o miembro del grupo <code>vcoadmins</code> configurado en los ajustes del proveedor de autenticación del centro de control de vRealize Orchestrator.</p> |

Tabla 1-69. Centro de control de vRealize Orchestrator

| Propósito | Acceso | Credenciales necesarias |
|--|---|--|
| <p>El centro de control de vRealize Orchestrator se emplea para editar la configuración de la instancia de vRealize Orchestrator predeterminada que está integrada en vRealize Automation.</p> | <ol style="list-style-type: none"> 1 Inicie un navegador y abra la página de presentación del dispositivo de vRealize Automation con el nombre de dominio completo del dispositivo virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Haga clic en Administración de dispositivos de vRealize Automation. También puede utilizar la siguiente dirección URL para abrir la administración de dispositivos de vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Inicie sesión. 4 Haga clic en Configuración de vRA > Orchestrator. 5 Seleccione la interfaz de usuario de Orchestrator. 6 Haga clic en Iniciar. 7 Haga clic en la URL de interfaz de usuario de Orchestrator. 8 Inicie sesión. | <p>Nombre de usuario</p> <ul style="list-style-type: none"> ■ Introduzca root (raíz) si no se configuró la autenticación basada en funciones. ■ Introduzca su nombre de usuario de vRealize Automation si está configurado para la autenticación basada en funciones. <p>Contraseña</p> <ul style="list-style-type: none"> ■ Escriba la contraseña que introdujo al implementar el dispositivo vRealize Automation si no se configuró la autenticación basada en funciones. ■ Introduzca la contraseña de su nombre de usuario si está configurado para la autenticación basada en funciones. |

Tabla 1-70. Símbolo del sistema de Linux

| Propósito | Acceso | Credenciales necesarias |
|---|--|---|
| <p>El símbolo del sistema de Linux se utiliza en un host, como el host del dispositivo de vRealize Automation, para realizar las siguientes tareas.</p> <ul style="list-style-type: none"> ■ Detener o iniciar servicios. ■ Editar archivos de configuración. ■ Ejecutar comandos. ■ Recuperar datos. | <p>1 En el host del dispositivo de vRealize Automation, abra un símbolo del sistema.</p> <p>Una forma de abrir el símbolo del sistema en el equipo local consiste en iniciar una sesión en el host mediante una aplicación como PuTTY.</p> <p>2 Inicie sesión.</p> | <ul style="list-style-type: none"> ■ Nombre de usuario: raíz. ■ Contraseña: la contraseña que ha creado al implementar el dispositivo de vRealize Automation. |

Tabla 1-71. Símbolo del sistema de Windows

| Propósito | Acceso | Credenciales necesarias |
|---|---|--|
| <p>Se puede utilizar un símbolo del sistema de Windows en un host, como el host de IaaS, para ejecutar scripts.</p> | <p>1 En el host de IaaS, inicie sesión en Windows.</p> <p>Una forma de iniciar sesión desde el equipo local consiste en iniciar una sesión de escritorio remoto.</p> <p>2 Abra el símbolo del sistema de Windows.</p> <p>Una forma de abrir el símbolo del sistema consiste en hacer clic con el botón derecho en el icono Inicio en el host y seleccionar Símbolo del sistema o Símbolo del sistema (administrador).</p> | <ul style="list-style-type: none"> ■ Nombre de usuario: usuario con privilegios administrativos. ■ Contraseña: contraseña del usuario. |

Actualización de productos de VMware integrados con vRealize Automation

Debe administrar todos los productos de VMware integrados con el entorno de vRealize Automation al actualizar vRealize Automation.

Si el entorno de vRealize Automation está integrado con uno o varios productos adicionales, deberá actualizar vRealize Automation antes de actualizar los productos adicionales. Si vRealize Business for Cloud está integrado con vRealize Automation, deberá anular el registro de vRealize Business for Cloud antes de actualizar vRealize Automation.

Siga el flujo de trabajo recomendado para la administración de productos integrados al actualizar vRealize Automation.

- 1 Actualice vRealize Automation.
- 2 Actualice VMware vRealize Operations Manager.
- 3 Actualice VMware vRealize Log Insight.
- 4 Actualice VMware vRealize Business for Cloud.

En esta sección, se proporcionan instrucciones adicionales para administrar vRealize Business for Cloud cuando se integra con el entorno de vRealize Automation.

Actualización de vRealize Operations Manager integrado con vRealize Automation

Actualice vRealize Operations Manager tras actualizar vRealize Automation.

Procedimiento

- 1 Actualice vRealize Automation.
- 2 Actualice vRealize Operations Manager. Para obtener información, consulte *Actualizar el software* en la documentación de [VMware vRealize Operations Manager](#).

Actualización de vRealize Log Insight integrado con vRealize Automation

Actualice vRealize Log Insight tras actualizar vRealize Automation.

Procedimiento

- 1 Actualice vRealize Automation.
- 2 Actualice vRealize Log Insight. Para obtener información, consulte *Actualizar vRealize Log Insight* en la documentación de [VMware vRealize Log Insight](#).

Actualización de vRealize Business for Cloud integrado con vRealize Automation

Cuando se actualiza el entorno de vRealize Automation, se debe cancelar el registro de la conexión con vRealize Business for Cloud, y luego volver a registrarla.

Realice este procedimiento para garantizar la continuidad del servicio con vRealize Business for Cloud al actualizar el entorno de vRealize Automation.

Procedimiento

- 1 Elimine el registro de vRealize Business for Cloud desde vRealize Automation. Consulte *Eliminar el registro de vRealize Business for Cloud desde vRealize Automation* en la documentación de [VMware vRealize Business for Cloud](#).
- 2 Actualice vRealize Automation.
- 3 Si es necesario, actualice vRealize Business for Cloud. Consulte *Actualizar vRealize Business for Cloud* en la documentación de [VMware vRealize Business for Cloud](#).
- 4 Registre vRealize Business for Cloud con vRealize Automation. Consulte *Registrar vRealize Business for Cloud con vRealize Automation* en la documentación de [VMware vRealize Business for Cloud](#).

Preparar la actualización de vRealize Automation

Debe realizar varias tareas y procedimientos antes de actualizar vRealize Automation 6.2.5 a la versión 7.4.

Realice las tareas en el orden en el que aparecen en la lista de comprobación de actualización. Consulte [Lista de comprobación para actualizar vRealize Automation](#).

Requisitos previos de copia de seguridad para actualizar vRealize Automation

Satisfaga los requisitos previos de copia de seguridad antes de actualizar vRealize Automation 6.2.5 a la versión 7.4.

Requisitos previos

- Compruebe que el entorno de origen se ha instalado y configurado correctamente.
- Para cada dispositivo del entorno de origen, cree una copia de seguridad de todos los archivos de configuración del dispositivo de vRealize Automation en los directorios siguientes.
 - `/etc/vcac/`
 - `/etc/vco/`
 - `/etc/apache2/`
 - `/etc/rabbitmq/`

- Realice una copia de seguridad de los archivos de configuración de flujos de trabajo externos (xmldb) de vRealize Automation en el sistema. Almacene los archivos de copia de seguridad en un directorio temporal. Estos archivos se encuentran en `\VMware\vCA\Server\ExternalWorkflows\xmldb\`. Debe restaurar los archivos xmldb en el nuevo sistema después de realizar la migración. Consulte [Restaurar archivos de tiempo de espera de flujos de trabajo externos](#).

Para obtener información sobre un problema relacionado, consulte [Las copias de seguridad de archivos .xml hacen que el sistema agote el tiempo de espera](#).

- Haga una copia de seguridad de la base de datos externa de PostgreSQL de vRealize Automation. Haga lo siguiente para saber si la base de datos de PostgreSQL es externa.
 - a Inicie sesión en la consola de administración de dispositivo de vRealize Automation usando el nombre de dominio completo, `https://va-hostname.domain.name:5480`.

En un entorno distribuido, inicie sesión en la consola de administración de dispositivo de vRealize Automation principal.
 - b Seleccione **Configuración de vRA > Base de datos**.
 - c Si el host del nodo de la base de datos de PostgreSQL de vRealize Automation es distinto del host de dispositivo de vRealize Automation, haga una copia de seguridad de la base de datos. Si el host del nodo de la base de datos es el mismo que el host de dispositivo, no es necesario hacer una copia de seguridad de la base de datos.

Para obtener información sobre la copia de seguridad de la base de datos de PostgreSQL, consulte <https://www.postgresql.org/>.
- Cree un snapshot de la configuración del tenant y los usuarios asignados.
- Cree una copia de seguridad de cualquier archivo que haya personalizado, como `DataCenterLocations.xml`.

- Cree un snapshot de cada dispositivo virtual y del servidor de IaaS. Siga las directrices habituales para hacer una copia de seguridad del sistema completo en caso de que no se realice con éxito la actualización de vRealize Automation. Consulte [Copia de seguridad y recuperación de instalaciones de vRealize Automation](#).

Hacer una copia de seguridad del entorno de vRealize Automation 6.2.5 existente

Antes de actualizar, apague los componentes del entorno de vRealize Automation 6.2.5 y realice un snapshot de estos.

Antes de actualizar, realice un snapshot de estos componentes mientras que su sistema se apaga.

- vRealize Automation servidores IaaS (nodos Windows)
- Dispositivos de vRealize Automation (nodos Linux)
- Nodos de identificación de vRealize Automation (SSO)

Si la actualización no se realiza correctamente, use el snapshot para volver a la última configuración conocida correcta e intentar otra actualización.

Requisitos previos

- Compruebe que la base de datos de PostgreSQL integrada está en el modo de alta disponibilidad. Si lo está, localice el nodo principal actual. Consulte el artículo de la base de conocimientos <http://kb.vmware.com/kb/2105809>.
- Si su entorno tiene una base de datos de PostgreSQL externa, cree una copia de seguridad de la base de datos.
- Si la base de datos de Microsoft SQL de vRealize Automation no está alojada en el servidor de IaaS, cree un archivo de copia de seguridad de la base de datos. Para obtener información, busque el artículo en [Microsoft Developer Network](#) sobre cómo crear una copia de seguridad completa de la base de datos de SQL Server.
- Compruebe que ha completado los requisitos previos de copia de seguridad para la actualización.
- Compruebe que ha tomado un snapshot del sistema mientras estaba desconectado. Es el método favorito para tomar un snapshot. Consulte la documentación de *vSphere 6.0*.

Nota Cuando realice copias de seguridad del dispositivo vRealize Automation y de los componentes de IaaS, deshabilite los snapshots en memoria y los snapshots en modo inactivo.

- Si modificó el archivo `app.config`, haga una copia de seguridad de ese archivo. Consulte [Restaurar cambios para iniciar sesión en el archivo app.config](#).
- Haga una copia de seguridad de los archivos de configuración del flujo de trabajo externo (xmldb). Consulte [Restaurar archivos de tiempo de espera de flujos de trabajo externos](#).
- Compruebe que exista una ubicación fuera de la carpeta actual donde puede almacenar el archivo de copia de seguridad. Consulte [Las copias de seguridad de archivos .xml hacen que el sistema agote el tiempo de espera](#).

Procedimiento

- 1 Inicie sesión en vCenter Server.
- 2 Busque estos componentes de vRealize Automation 6.2.5.
 - vRealize Automation servidores IaaS (nodos Windows)
 - Dispositivos de vRealize Automation (nodos Linux)
 - Nodos de identificación de vRealize Automation (SSO)
- 3 Para cada una de las siguientes máquinas virtuales, seleccione la máquina virtual, haga clic en **Apagar invitado** y espere a que la máquina virtual se detenga. Apague estas máquinas virtuales en el siguiente orden.
 - a Máquinas virtuales del agente de proxy de IaaS
 - b Máquinas virtuales del trabajo de DEM
 - c Máquina virtual del orquestador de DEM
 - d Máquina virtual de Manager Service
 - e Máquinas virtuales del servicio web
 - f Dispositivos virtuales de vRealize Automation secundarios
 - g Dispositivos virtuales de vRealize Automation principales
 - h Máquinas virtuales del administrador (si corresponde)
 - i Identity Appliance
- 4 Realice un snapshot de cada máquina virtual de vRealize Automation 6.2.5.
- 5 Clone cada nodo de dispositivo de vRealize Automation.
Realice la actualización en las máquinas virtuales clonadas.
- 6 Desconecte cada máquina virtual del dispositivo de vRealize Automation original antes de actualizar las máquinas virtuales clonadas.

Mantenga desconectadas las máquinas virtuales originales y utilícelas solo si tiene que restaurar el sistema.

Pasos siguientes

[Aumentar los recursos de hardware de vCenter Server de vRealize Automation 6.2.5.](#)

Aumentar los recursos de hardware de vCenter Server de vRealize Automation 6.2.5

Antes de actualizar desde vRealize Automation 6.2.5, debe aumentar los recursos de hardware en cada dispositivo de vRealize Automation.

En este procedimiento se da por hecho que se está usando la versión de Windows del cliente vCenter Server.

Requisitos previos

- Compruebe que posee un clon de cada dispositivo de vRealize Automation.
- Compruebe que tiene al menos 140 GB de espacio libre en vCenter Server para cada clon del dispositivo.
- Confirme que los dispositivos originales están apagados.

Procedimiento

- 1 Inicie sesión en vCenter Server.
- 2 Haga clic con el botón derecho en un icono de dispositivo de vRealize Automation clonado y seleccione **Editar configuración**.
- 3 Seleccione **Memoria** y establezca el valor en 18 GB.
- 4 Seleccione **CPU** y establezca el valor de **Número de sockets virtuales** en 4.
- 5 Extienda el tamaño del disco virtual 1 a 50 GB.
 - a Seleccione el disco 1.
 - b Cambie el tamaño a 50 GB.
 - c Haga clic en **Aceptar**.
- 6 Si no tiene el disco 3, realice los siguientes pasos para agregar un disco 3 con un tamaño de 25 GB.
 - a Haga clic en **Añadir** sobre la tabla Recursos para añadir un disco virtual.
 - b Seleccione **Disco duro** en **Tipo de dispositivo** y haga clic en **Siguiente**.
 - c Seleccione **Crear un nuevo disco virtual** y haga clic en **Siguiente**.
 - d Establezca el valor de **tamaño de disco** en 25 GB.
 - e Seleccione **Almacenar con la máquina virtual** y haga clic en **Siguiente**.
 - f Compruebe que la opción **Independiente** no esté seleccionada para **Modo** y que **SCSI (0:2)** esté seleccionado para **Modo de dispositivo virtual**. Haga clic en **Siguiente**.

Si recibe una solicitud para aceptar la configuración recomendada, acéptela.
 - g Haga clic en **Finalizar**.
 - h Haga clic en **Aceptar**.
- 7 Si hay un disco 4 virtual existente perteneciente a alguna versión anterior de vRealize Automation, realice estos pasos.
 - a Encienda el clon del dispositivo virtual principal y espere 1 minuto.
 - b Encienda el clon del dispositivo virtual secundario.
 - c En el clon de dispositivo virtual principal, abra un nuevo símbolo del sistema y desplácese a `/etc/fstab`.

- d En el clon del dispositivo virtual principal, abra el archivo `fstab` y quite las líneas que comiencen por `/dev/sdd`, que contienen los logs de escritura previa de `Wal_Archive`.
 - e En el clon del dispositivo virtual principal, guarde el archivo.
 - f En el clon del dispositivo virtual secundario, abra un nuevo símbolo del sistema y desplácese a `/etc/fstab`.
 - g En el clon del dispositivo virtual secundario, abra el archivo `fstab` y quite las líneas que comiencen por `/dev/sdd`, que contienen los logs de escritura previa de `Wal_Archive`.
 - h En el clon del dispositivo virtual secundario, guarde el archivo.
 - i Apague el clon del dispositivo virtual secundario y espere 1 minuto.
 - j Apague el clon del dispositivo virtual principal.
 - k Haga clic con el botón derecho en el icono de dispositivo principal de vRealize Automation clonado y seleccione **Editar configuración**.
 - l Elimine el disco 4 de la máquina del dispositivo virtual principal clonado.
 - m Haga clic con el botón derecho en el icono de dispositivo secundario de vRealize Automation clonado y seleccione **Editar configuración**.
 - n Elimine el disco 4 de la máquina del dispositivo virtual secundario clonado.
- 8 Realice los siguientes pasos para añadir un disco 4 con un tamaño de disco de 50 GB a las máquinas principal y secundaria clonadas del dispositivo virtual.
- a Haga clic en **Añadir** sobre la tabla Recursos para añadir un disco virtual.
 - b Seleccione **Disco duro** en **Tipo de dispositivo** y haga clic en **Siguiente**.
 - c Seleccione **Crear un nuevo disco virtual** y haga clic en **Siguiente**.
 - d Establezca el valor de **tamaño de disco** en 50 GB.
 - e Seleccione **Almacenar con la máquina virtual** y haga clic en **Siguiente**.
 - f Compruebe que la opción **Independiente** no esté seleccionada para **Modo** y que **SCSI (0:3)** esté seleccionado para **Modo de dispositivo virtual**. Haga clic en **Siguiente**.
Si recibe una solicitud para aceptar la configuración recomendada, acéptela.
 - g Haga clic en **Finalizar**.
 - h Haga clic en **Aceptar**.
- 9 Cree un snapshot de la máquina del dispositivo virtual principal clonado y de la máquina del dispositivo virtual secundario clonado.

Pasos siguientes

[Encender el sistema completo.](#)

Encender el sistema completo

Después de aumentar los recursos de hardware de vCenter para la actualización, debe encender el sistema antes de realizar la actualización.

Requisitos previos

- [Hacer una copia de seguridad del entorno de vRealize Automation 6.2.5 existente.](#)
- [Aumentar los recursos de hardware de vCenter Server de vRealize Automation 6.2.5.](#)

Procedimiento

- 1 Encienda el sistema completo.

Para obtener instrucciones, consulte la versión de vRealize Automation 6.2 del tema [Iniciar vRealize Automation](#).

Nota Si tiene un entorno de alta disponibilidad, utilice este procedimiento para encender los dispositivos virtuales.

- a Encienda el dispositivo virtual que apagó en último lugar.
- b Espere un minuto.
- c Encienda el resto de dispositivos virtuales.

- 2 Compruebe que el sistema funciona sin restricciones.

Pasos siguientes

[Detener los servicios de vRealize Automation en el servidor Windows de IaaS.](#)

Detener los servicios de vRealize Automation en el servidor Windows de IaaS

El siguiente procedimiento se puede usar para detener los servicios de vRealize Automation en cada servidor que ejecuta servicios de IaaS siempre que lo considere necesario.

Antes de iniciar la actualización, detenga los servicios de vRealize Automation en cada servidor de Windows de IaaS.

Nota Durante el proceso de actualización, el tipo de inicio de todos los servicios debe establecerse en Automático, excepto para las instancias de copia de seguridad pasiva de Manager Service. Si establece los servicios en Manual, se produce un error en el proceso de actualización.

Procedimiento

- 1 Inicie sesión en el servidor de Windows de IaaS.
- 2 Seleccione **Inicio > Herramientas administrativas > Servicios**.

- 3 Detenga los servicios en el siguiente orden. Asegúrese de no desconectar la máquina virtual.

Cada máquina virtual tiene un agente de administración, que debe detenerse con cada conjunto de servicios.

- a Todos los agentes de VMware vCloud Automation Center
- b Todos los trabajos de DEM de VMware
- c El orquestador de DEM de VMware
- d El servicio VMware vCloud Automation Center

- 4 Para implementaciones distribuidas con equilibradores de carga, deshabilite los nodos secundarios y quite los supervisores de estado de vRealize Automation para los siguientes elementos.

- a Dispositivo de vRealize Automation
- b Sitio web de IaaS
- c IaaS Manager Service

Compruebe que el tráfico de equilibradores de carga solo se dirija a los nodos principales, y que se eliminen los supervisores de estado de vRealize Automation del dispositivo, el sitio web y el servicio de administración. De lo contrario, la actualización no se realizará correctamente.

- 5 Realice los pasos siguientes para comprobar que el servicio IaaS alojado en Microsoft Internet Information Services (IIS) se ejecuta.

- a En su navegador, introduzca la URL **https://webhostname/Repository/Data/MetaModel.svc** para comprobar que el repositorio web se está ejecutando. Si es correcto, no se devolverán errores y verá una lista de modelos con formato XML.
- b Compruebe el estado registrado en el archivo `Repository.log` que se encuentra en el nodo web de la máquina virtual de IaaS para ver que el estado es correcto. El archivo se encuentra en la carpeta de inicio de VCAC en `/Server/Model Manager Web/Logs/Repository.log`.

Para un sitio web de IaaS distribuido, inicie sesión en el sitio web secundario, sin MMD, y detenga el servidor de Microsoft IIS temporalmente. Compruebe la conectividad de `MetaModel.svc`. Para comprobar que el tráfico del equilibrador de carga solo pasa por el nodo web principal, inicie el servidor de Microsoft IIS.

Pasos siguientes

[Descargar actualizaciones del dispositivo de vRealize Automation.](#)

Descargar actualizaciones del dispositivo de vRealize Automation

Puede buscar actualizaciones en la consola de administración del dispositivo y descargarlas mediante uno de los siguientes métodos.

Para mejorar el rendimiento de la actualización, utilice el método de archivos ISO.

Para evitar posibles problemas al actualizar el dispositivo, o si surgen problemas durante la actualización del dispositivo, consulte el [artículo de la base de conocimientos de VMware Error en la actualización de vRealize Automation debido a duplicados en la base de datos de vRealize Orchestrator \(54987\)](#).

- [Descargar las actualizaciones del dispositivo de vRealize Automation desde un repositorio de VMware](#)

Puede descargar la actualización del dispositivo de vRealize Automation de un repositorio público en el sitio web vmware.com.

- [Descargar actualizaciones de dispositivo virtual para su uso con una unidad de CD-ROM](#)

Su dispositivo virtual se puede actualizar desde un archivo ISO que el dispositivo lee desde la unidad de CD-ROM virtual. Este es el método preferido.

Descargar las actualizaciones del dispositivo de vRealize Automation desde un repositorio de VMware

Puede descargar la actualización del dispositivo de vRealize Automation de un repositorio público en el sitio web vmware.com.

Requisitos previos

- Realice una copia de seguridad del entorno de vRealize Automation existente.
- Compruebe que el dispositivo de vRealize Automation esté encendido.

Procedimiento

- 1 En el dispositivo de vRealize Automation principal, inicie sesión en la Administración de dispositivos de vRealize Automation como **raíz** con la contraseña que introdujo al implementar el dispositivo de vRealize Automation.
- 2 Haga clic en la pestaña **Actualizar**.
- 3 Haga clic en **Configuración**.
- 4 (opcional) Indique la frecuencia con la que se van a buscar actualizaciones en el panel Actualizaciones automáticas.
- 5 Seleccione **Usar repositorio predeterminado** en el panel Repositorio de actualizaciones.
El repositorio predeterminado se establece en la URL de vmware.com adecuada.
- 6 Haga clic en **Guardar configuración**.

Descargar actualizaciones de dispositivo virtual para su uso con una unidad de CD-ROM

Su dispositivo virtual se puede actualizar desde un archivo ISO que el dispositivo lee desde la unidad de CD-ROM virtual. Este es el método preferido.

Descargue el archivo ISO y configure el dispositivo principal para utilizar este archivo en la actualización del dispositivo.

Requisitos previos

- Realice una copia de seguridad del entorno de vRealize Automation existente.

- Compruebe que estén habilitadas todas las unidades de CD-ROM que utiliza en la actualización antes de actualizar un dispositivo de vRealize Automation. Consulte la documentación de vSphere para obtener información sobre la forma de añadir una unidad de CD-ROM a una máquina virtual en el cliente de vSphere.

Procedimiento

- 1 Descargue el archivo ISO del repositorio de actualizaciones.
 - a Inicie un navegador y vaya a la [página del producto vRealize Automation](#) en www.vmware.com.
 - b Haga clic en los **recursos de descarga de vRealize Automation** para ir a la página de descarga de VMware.
 - c Descargue el archivo adecuado.
- 2 Busque el archivo descargado en el sistema para comprobar que el tamaño de archivo es el mismo que el del archivo de la página de descarga de VMware. Utilice las sumas de comprobación proporcionadas en la página de descarga para validar la integridad del archivo descargado. Para obtener información, consulte los vínculos de la parte inferior de la página de descarga de VMware.
- 3 Compruebe que el dispositivo virtual principal esté encendido.
- 4 Conecte la unidad de CD-ROM del dispositivo virtual principal al archivo ISO descargado.
- 5 En el dispositivo de vRealize Automation principal, inicie sesión en la Administración de dispositivos de vRealize Automation como **raíz** con la contraseña que introdujo al implementar el dispositivo de vRealize Automation.
- 6 Haga clic en la pestaña **Actualizar**.
- 7 Haga clic en **Configuración**.
- 8 En Repositorio de actualizaciones, seleccione **Usar actualizaciones de CDROM**.
- 9 Haga clic en **Guardar configuración**.

Actualizar el dispositivo de vRealize Automation

Tras satisfacer los requisitos previos de actualización y descargar la actualización de dispositivo virtual, se actualiza el dispositivo de vRealize Automation 6.2.5 a la versión 7.4. También se vuelven a configurar algunas opciones del dispositivo principal de vRealize Automation.

Después de actualizar el dispositivo principal de vRealize Automation, los otros nodos del entorno se actualizan en el orden siguiente:

- 1 Dispositivos secundarios de vRealize Automation
- 2 Sitio web de IaaS
- 3 IaaS Manager Service
- 4 DEM de IaaS
- 5 Agente de IaaS

6 Actualizar o migrar cada instancia de vRealize Orchestrator externa

Instalar la actualización en el dispositivo de vRealize Automation

Instale la actualización de vRealize Automation en el dispositivo de vRealize Automation 6.2.5 y configure los parámetros del dispositivo.

A partir de la versión 7.1, vRealize Automation no admite la base de datos externa de PostgreSQL. El proceso de actualización combina los datos desde una base de datos externa de PostgreSQL ya existente con la base de datos interna de PostgreSQL que forma parte del Dispositivo de vRealize Automation.

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>.

No cierre la consola de administración mientras instala la actualización.

Si surge algún problema durante el proceso de actualización, consulte [Solucionar problemas de actualización de vRealize Automation](#).

Requisitos previos

- Compruebe que ha seleccionado el método de descarga y que ha descargado la actualización. Consulte [Descargar actualizaciones del dispositivo de vRealize Automation](#).
- Para implementaciones distribuidas de alta disponibilidad, consulte [Hacer una copia de seguridad del entorno de vRealize Automation 6.2.5 existente](#).
- Para las implementaciones con equilibradores de carga, compruebe que el tráfico se dirige solo al nodo principal y que los supervisores de estado están deshabilitados.
- Si hay un componente del Catálogo de componentes comunes instalado en su entorno, debe desinstalarlo antes de la actualización. Para obtener más información, consulte la *guía de instalación del Catálogo de componentes comunes*. Si la guía no está disponible, utilice el procedimiento alternativo de la [Lista de comprobación para actualizar vRealize Automation](#).
- Compruebe que la conexión de la base de datos jdbc:postgresql apunte a la dirección IP externa del nodo de PostgreSQL principal.
 - a En cada uno de los dispositivos de vRealize Automation, abra un nuevo símbolo del sistema.
 - b Vaya a `/etc/vcac/server.xml` y haga una copia de seguridad de `server.xml`.
 - c Abra `server.xml`.
 - d En caso necesario, edite la entrada jdbc:postgresql del archivo `server.xml` que apunta a la base de datos de Postgres y apunte a la dirección IP externa del nodo de PostgreSQL principal para el PostgreSQL externo o al dispositivo virtual principal para el PostgreSQL integrado.

Por ejemplo, `jdbc:postgresql://198.15.100.60:5432/vcac`
- Compruebe que todas las solicitudes guardadas y en curso se hayan completado correctamente antes de la actualización.

Procedimiento

- 1 Abra la consola de administración del dispositivo de vRealize Automation.
 - a En el dispositivo de vRealize Automation principal, inicie sesión en la Administración de dispositivos de vRealize Automation como **raíz** con la contraseña que introdujo al implementar el dispositivo de vRealize Automation.
 - b Inicie sesión con el nombre de usuario **root** y la contraseña que ha especificado al implementar el dispositivo.
- 2 Haga clic en **Servicios** y compruebe que cada servicio, excepto iaas-service, aparece como REGISTRADO.
- 3 Seleccione **Actualizar > Configuración**.
- 4 Seleccione una de las siguientes opciones:
 - **Usar repositorio predeterminado.**
 - **Usar actualizaciones de CDROM**
- 5 Haga clic en **Guardar configuración**.
- 6 Seleccione **Estado**.
- 7 Haga clic en **Comprobar actualizaciones** para comprobar si hay alguna actualización accesible.
- 8 (opcional) Para las instancias del dispositivo de vRealize Automation, haga clic en **Detalles** en el área de versión de dispositivo para ver información sobre la ubicación de las notas de la versión.
- 9 Haga clic en **Instalar actualizaciones**.
- 10 Haga clic en **Aceptar**.

Aparece un mensaje que indica que hay una actualización en curso.
- 11 (Opcional) Si no ha ajustado el tamaño del disco 1 a 50 GB manualmente, realice los siguientes pasos.
 - a Cuando el sistema le solicite reiniciar el dispositivo virtual, haga clic en **Sistema** y luego en **Reiniciar**.

Durante el reinicio, el sistema ajusta el espacio necesario para la actualización.
 - b Una vez que se reinicia el sistema, vuelva a iniciar sesión en la consola de administración del dispositivo de vRealize Automation, compruebe que cada servicio (excepto iaas-service) aparece como REGISTRADO, y seleccione **Actualizar > Estado**.
 - c Haga clic en **Comprobar actualizaciones** y en **Instalar actualizaciones**.
- 12 Para ver el progreso de la actualización, abra los siguientes archivos de log.
 - `/opt/vmware/var/log/vami/updatecli.log`
 - `/opt/vmware/var/log/vami/vami.log`
 - `/var/log/vmware/horizon/horizon.log`

- `/var/log/bootstrap/*.log`

Si cierra sesión durante el proceso de actualización y después inicia sesión antes de que se acabe la actualización, puede seguir el proceso de actualización en el archivo de log. El archivo `updatecli.log` puede mostrar información acerca de la versión de vRealize Automation desde la que está actualizando. La versión que se muestra cambia a la versión posterior adecuada durante el proceso de actualización.

El tiempo necesario para que la actualización finalice depende del entorno.

- 13 Haga clic en **Telemetría** en la consola de administración del dispositivo. Lea la nota acerca de la participación en el Programa de mejora de la experiencia del cliente (CEIP) y decida si desea unirse o no al programa.

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>.

Para obtener más información sobre el programa de mejora de la experiencia del cliente, consulte [Unirse o abandonar el programa de mejora de la experiencia del cliente para vRealize Automation](#).

Pasos siguientes

[Actualizar la contraseña de Single Sign-On para VMware Identity Manager.](#)

Actualizar la contraseña de Single Sign-On para VMware Identity Manager

Después de instalar las actualizaciones, deberá actualizar la contraseña de Single Sign-On para VMware Identity Manager.

VMware Identity Manager los componentes de SSO de Identity Appliance y vSphere.

Procedimiento

- 1 Cierre la sesión de la consola de administración del dispositivo de vRealize Automation, cierre el explorador, vuelva a abrirlo e inicie sesión de nuevo.
- 2 Seleccione **Configuración de vRA > SSO**.
- 3 Especifique una nueva contraseña de VMware Identity Manager y haga clic en **Guardar configuración**.

No utilice contraseñas sencillas. Puede hacer caso omiso del mensaje de error `El servidor SSO no está conectado`. Los servicios podrían tardar varios minutos en reiniciarse.

Se acepta la contraseña.

Para una implementación de alta disponibilidad, la contraseña se aplica al primer nodo del dispositivo de vRealize Automation y se propaga a todos los nodos secundarios del dispositivo de vRealize Automation.

- 4 Reinicie el dispositivo virtual.
 - a Haga clic en la pestaña **Sistema**.
 - b Haga clic en **Reiniciar** y confirme la selección.

- 5 Compruebe que se están ejecutando todos los servicios.
 - a Inicie sesión en la consola de administración del dispositivo de vRealize Automation.
 - b Haga clic en la pestaña **Servicios** en la consola.
 - c Haga clic en la pestaña **Actualizar** para ver el progreso del inicio de los servicios.
Debería ver un mínimo de 35 servicios.
- 6 Compruebe que todos los servicios estén registrados excepto iaas-service.
El servicio release-management no se inicia sin una clave de licencia de vRealize Code Stream.

Pasos siguientes

[Actualizar la clave de licencia.](#)

Actualizar la clave de licencia

Debe actualizar su clave de licencia para usar la versión más reciente del dispositivo de vRealize Automation.

Procedimiento

- 1 Vaya a la consola de administración de su dispositivo virtual, utilizando su nombre de dominio completo, `https://va-hostname.domain.name:5480`.
- 2 Inicie sesión con el nombre de usuario **root** y la contraseña que especificó cuando se implementó el dispositivo.
- 3 Seleccione **Configuración de vRA > Licencias**.
Si la pestaña **Licencias** no está disponible, realice los siguientes pasos y repita el procedimiento.
 - a Cierre sesión en la consola de administración.
 - b Borre la caché del navegador.
- 4 Introduzca su nueva clave de licencia en el cuadro de texto **Nueva clave de licencia**.
Los endpoints y las cuotas se marcarán de acuerdo con su contrato de licencia para el usuario final (EULA).
- 5 Haga clic en **Enviar clave**.

Pasos siguientes

[Migración de almacenes de identidades a VMware Identity Manager.](#)

Migración de almacenes de identidades a VMware Identity Manager

Cuando se actualiza de vRealize Automation 6.2.5 a la versión actual, se deben migrar los almacenes de identidades.

Tal como se requiere en los siguientes procedimientos, consulte el snapshot de la información de configuración del tenant de la versión 6.2.5.

Nota Tras migrar los almacenes de identidades, los usuarios de vRealize Code Stream deben reasignar manualmente las funciones de vRealize Code Stream.

Procedimiento

1 Crear una cuenta de usuario local para los tenants

Debe configurar un tenant con una cuenta de usuario local y asignar privilegios de administrador de tenants a dicha cuenta.

2 Sincronizar usuarios y grupos para un vínculo de Active Directory

Para importar sus usuarios y grupos en vRealize Automation mediante la capacidad Administración de directorios, se debe conectar a su vínculo Active Directory.

3 Migrar grupos personalizados a la instancia de VMware Identity Manager de destino

Debe migrar todos los grupos personalizados del entorno de origen a VMware Identity Manager (vIDM) en la implementación de destino.

4 Migrar varios administradores de tenants e IaaS

En los tenants de vRealize Automation con administradores de tenants o de IaaS, debe eliminar y restaurar cada administrador manualmente.

Crear una cuenta de usuario local para los tenants

Debe configurar un tenant con una cuenta de usuario local y asignar privilegios de administrador de tenants a dicha cuenta.

Repita este procedimiento para cada uno de los tenants.

Requisitos previos

Compruebe que ha establecido una nueva contraseña para VMware Identity Manager. Consulte [Actualizar la contraseña de Single Sign-On para VMware Identity Manager](#).

Procedimiento

- 1 Inicie sesión en la consola de vRealize Automation con el nombre de usuario del administrador del sistema predeterminado (**administrator**) y la contraseña.

La ubicación de la consola es `https://vra-appliance/vcac/`.

- 2 Haga clic en el tenant.

Por ejemplo, en el caso del tenant predeterminado, haga clic en **vsphere.local**.

- 3 Seleccione la pestaña **Usuarios locales**.

- 4 Haga clic en **Nuevo**.

5 Cree una cuenta de usuario local.

Asigne la función de administrador de tenants a este usuario. Compruebe que el nombre de usuario local es único en el directorio activo vsphere.local.

6 Haga clic en **Aceptar**.

7 Haga clic en **Administradores**.

8 Escriba el nombre de usuario local en el cuadro de búsqueda **Administradores de tenants** y pulse Entrar.

9 Haga clic en **Finalizar**.

10 Cierre sesión en la consola.

Pasos siguientes

[Sincronizar usuarios y grupos para un vínculo de Active Directory.](#)

Sincronizar usuarios y grupos para un vínculo de Active Directory

Para importar sus usuarios y grupos en vRealize Automation mediante la capacidad Administración de directorios, se debe conectar a su vínculo Active Directory.

Siga este procedimiento para cada uno de los tenants.

Requisitos previos

Compruebe que tiene privilegios de acceso a Active Directory.

Procedimiento

1 Inicie sesión en la consola de vRealize Automation en:

`https://vra-appliance/vcac/org/tenant_name`.

2 Seleccione **Administración > Administración de directorios > Directorios**.

3 Haga clic en **Añadir directorio** y seleccione **Añadir Active Directory en LDAP/IWA**.

4 Introduzca la configuración de su cuenta de Active Directory.

◆ Active Directory no nativo

| Opción | Entrada de muestra |
|--|--|
| Nombre de directorio | Escriba un nombre de directorio único. Seleccione Active Directory en LDAP si utiliza Active Directory no nativo. |
| Este directorio es compatible con servicios DNS | Anule la selección de esta opción. |
| DN de la base | Escriba el nombre distintivo (DN) del punto de inicio de las búsquedas en el servidor de directorios. Por ejemplo, cn=users,dc=rainpole,dc=local . |

| Opción | Entrada de muestra |
|-----------------------------------|--|
| DN de enlace | Escriba el nombre distintivo (DN) completo, incluido el nombre común (CN), de una cuenta de usuario de Active Directory que tenga privilegios para buscar usuarios. Por ejemplo, cn=config_admin infra,cn=users,dc=rainpole,dc=local . |
| Contraseña de DN de enlace | Escriba la contraseña de Active Directory para la cuenta que puede buscar usuarios. |

◆ Active Directory nativo

| Opción | Entrada de muestra |
|--|--|
| Nombre de directorio | Escriba un nombre de directorio único. Seleccione Active Directory (Autenticación de Windows integrada) si usa Active Directory nativo. |
| Nombre de dominio | Escriba el nombre del dominio al que desea unirse. |
| Nombre de usuario del administrador del dominio | Escriba el nombre de usuario del administrador del dominio. |
| Contraseña del administrador del dominio | Escriba la contraseña de usuario del administrador del dominio. |
| UPN del usuario de enlace | Utilice este formato de dirección de correo electrónico para introducir el nombre del usuario que puede autenticar el dominio. |
| Contraseña de DN de enlace | Escriba la contraseña de la cuenta de enlace de Active Directory para la cuenta que puede buscar usuarios. |

- 5 Haga clic en **Probar conexión** para probar la conexión al directorio configurado.
- 6 Haga clic en **Guardar y Siguiente**.
Aparece la página **Seleccione los dominios** y se muestra la lista de dominios.
- 7 Acepte la configuración de dominio predeterminada y haga clic en **Siguiente**.
- 8 Compruebe que los nombres de atributo estén asignados a los atributos de Active Directory correctos y haga clic en **Siguiente**.
- 9 Seleccione los grupos y los usuarios que desea sincronizar.
 - a Haga clic en el icono **Nuevo**.
 - b Escriba el dominio de usuario y haga clic en **Buscar grupos**.
Por ejemplo, introduzca **dc=vcac,dc=local**.
 - c Para seleccionar los grupos que desea sincronizar, haga clic en **Seleccionar** y en **Siguiente**.
 - d En la página **Select Users** (Seleccionar usuarios) elija los usuarios que desea sincronizar y haga clic en **Siguiente**.
- 10 Revise los usuarios y los grupos que se sincronizarán con el directorio y haga clic en **Sincronizar directorio**.

La sincronización de directorios tarda un poco y se ejecuta en segundo plano.

- 11 Seleccione **Administración > Administración de directorios > Proveedores de identidades** y haga clic en el nuevo proveedor de identidades.

Por ejemplo, **WorkspaceIDP__1**.

- 12 Desplácese a la parte inferior de la página y actualice el valor para que la propiedad IdP Hostname apunte al FQDN para el equilibrador de carga de vRealize Automation.

- 13 Haga clic en **Guardar**.

- 14 Repita los pasos 11 a 13 para cada tenant y proveedor de identidad.

- 15 Tras actualizar todos los nodos de vRealize Automation, inicie sesión en cada tenant y seleccione **Administración > Administración de directorios > Proveedores de identidad**.

Cada proveedor de identidad tiene todos los conectores de vRealize Automation agregados.

Por ejemplo, si su implementación tiene dos dispositivos de vRealize Automation, el proveedor de identidad tiene dos conectores asociados.

Migrar grupos personalizados a la instancia de VMware Identity Manager de destino

Debe migrar todos los grupos personalizados del entorno de origen a VMware Identity Manager (vIDM) en la implementación de destino.

Complete este procedimiento para migrar los grupos personalizados.

Requisitos previos

- [Crear una cuenta de usuario local para los tenants](#).
- Asegúrese de que el servicio horizon-workspace se está ejecutando en el dispositivo virtual de vRealize Automation.

Procedimiento

- 1 Inicie una sesión de SSH en el dispositivo virtual de vRealize Automation.
- 2 En el símbolo del sistema, inicie sesión como **root** con la contraseña que ha creado al instalar el dispositivo virtual de vRealize Automation.
- 3 Ejecute el siguiente comando:

```
vcac-config migrate-custom-groups
```

- Cuando se completa la migración, aparece este mensaje: La migración de los grupos personalizados se ha completado correctamente.
- Si no hay grupos personalizados en el entorno de origen, aparece este mensaje: No se han encontrado grupos personalizados en la base de datos de vRA. Se omitirá el proceso de migración.

Nota Si se produce un error durante la migración de grupos personalizados, consulte el archivo de log en `/var/log/vmware/vcac/vcac-config.log` para obtener más detalles.

Migrar varios administradores de tenants e IaaS

En los tenants de vRealize Automation con administradores de tenants o de IaaS, debe eliminar y restaurar cada administrador manualmente.

Realice el siguiente procedimiento en cada tenant de la consola de vRealize Automation.

Requisitos previos

Inicie sesión en la consola de vRealize Automation en el dispositivo virtual actualizado.

- 1 Abra la consola de vRealize Automation en el dispositivo virtual actualizado utilizando su nombre de dominio completo, https://va-hostname.domain_name/vcac.

En un entorno distribuido, abra la consola en el dispositivo virtual principal.

- 2 Seleccione el dominio **vsphere.local**.
- 3 Inicie sesión con el nombre de usuario **administrator** y la contraseña que especificó al implementar el dispositivo.

Procedimiento

- 1 Seleccione **Administración > Tenants**.
- 2 Haga clic en un nombre de tenant.
- 3 Haga clic en **Administradores**.
- 4 Confeccione una lista de todos los nombres de usuario y nombres de administrador de tenants e IaaS.
- 5 Seleccione cada administrador y haga clic en el icono de eliminación (✖) hasta eliminar todos los administradores.
- 6 Haga clic en **Finalizar**.
- 7 En la página Tenants, vuelva a hacer clic en el nombre del tenant.
- 8 Haga clic en **Administradores**.
- 9 Escriba en el cuadro de búsqueda correspondiente el nombre de cada usuario eliminado y presione Entrar.
- 10 Haga clic en el nombre del usuario que proceda en los resultados de la búsqueda para volver a añadirlo como administrador.

Cuando termine, la lista de administradores de tenants y administradores de IaaS tiene el mismo aspecto que la lista de los administradores que ha eliminado.

- 11 Haga clic en **Finalizar**.

Pasos siguientes

Actualice los dispositivos secundarios. Consulte [Instalar la actualización en dispositivos adicionales de vRealize Automation](#).

Instalar la actualización en dispositivos adicionales de vRealize Automation

En un entorno de alta disponibilidad, el dispositivo virtual principal es el nodo que ejecuta la base de datos de PostgreSQL integrada en el modo principal. Los otros nodos del entorno ejecutan la base de datos de PostgreSQL integrada en el modo de réplica. Durante la actualización, la réplica de un dispositivo virtual 6.2.5 no requiere cambios en la base de datos.

No cierre la consola de administración mientras instala la actualización.

Requisitos previos

- Compruebe si ha descargado las actualizaciones de dispositivos virtuales. Consulte [Descargar actualizaciones del dispositivo de vRealize Automation](#).
- Compruebe que la conexión de la base de datos jdbc:postgresql apunte a la dirección IP externa del nodo de PostgreSQL principal.
 - a En el dispositivo de vRealize Automation, abra un nuevo símbolo del sistema.
 - b Desplácese hasta `/etc/vcac/server.xml` y haga una copia de seguridad del archivo `server.xml`.
 - c Abra el archivo `server.xml`.
 - d Si es necesario, edite la entrada `jdbc:postgresql` del archivo `server.xml` para indicar la base de datos de PostgreSQL que desea utilizar.
 - Para una base de datos de PostgreSQL externa, introduzca la dirección IP externa del nodo de PostgreSQL principal.
 - Para la base de datos de PostgreSQL integrada, introduzca la dirección IP del dispositivo virtual principal.

Por ejemplo, `jdbc:postgresql://198.15.100.60:5432/vcac`

Procedimiento

- 1 Abra la consola de administración del dispositivo de vRealize Automation para la actualización.
 - a En cada dispositivo de vRealize Automation secundario, inicie sesión en la administración de dispositivos de vRealize Automation como **raíz** con la contraseña que ha especificado al implementar el dispositivo de vRealize Automation.
 - b Inicie sesión con el nombre de usuario **root** y la contraseña que ha especificado al implementar el dispositivo.
 - c Haga clic en **Actualizar**.
- 2 Haga clic en **Configuración**.
- 3 Seleccione la descarga de las actualizaciones desde un repositorio de VMware o un CD-ROM en la sección Repositorio de actualización.
- 4 Haga clic en **Estado**.
- 5 Haga clic en **Comprobar actualizaciones** para comprobar si hay alguna actualización accesible.

6 Haga clic en **Instalar actualizaciones**.

7 Haga clic en **Aceptar**.

Aparece un mensaje que indica que hay una actualización en curso.

8 (Opcional) Si no ha ajustado el tamaño del disco de 1 a 50 GB de forma manual, realice los pasos siguientes.

a Cuando el sistema le solicite reiniciar el dispositivo virtual, haga clic en **Sistema** y luego en **Reiniciar**.

Durante el reinicio, el sistema ajusta el espacio en el disco 1 necesario para la actualización.

b Después de que se haya reiniciado el sistema, cierre sesión en la consola de administración de Dispositivo de vRealize Automation, vuelva a iniciarla y seleccione **Actualizar > Estado**.

c Haga clic en **Comprobar actualizaciones** y en **Instalar actualizaciones**.

9 Para comprobar que la actualización se esté realizando correctamente, abra los archivos de log.

- /opt/vmware/var/log/vami/vami.log
- /opt/vmware/var/log/vami/updatecli.log
- /var/log/vmware/horizon/horizon.log
- /var/log/bootstrap/*.log

Si cierra sesión durante el proceso de actualización y después inicia sesión, puede seguir el proceso de actualización en el archivo de log /opt/vmware/var/log/vami/updatecli.log.

El tiempo necesario para que la actualización finalice depende del entorno.

10 Cuando la actualización haya finalizado, cierre sesión en la consola de administración de Dispositivo de vRealize Automation, borre la caché del navegador web e inicie sesión en la consola de administración de Dispositivo de vRealize Automation.

11 Reinicie el dispositivo virtual.

a Haga clic en **Sistema**.

b Haga clic en **Reiniciar** y confirme la selección.

12 Tras reiniciar el dispositivo virtual, inicie sesión en la consola de administración de Dispositivo de vRealize Automation de réplica.

13 Seleccione **Configuración de vRA > Clúster**.

14 Escriba el nombre de usuario y la contraseña del Dispositivo de vRealize Automation principal.

15 Haga clic en **Unirse a clúster**.

16 Haga clic en **Servicios** y compruebe que cada servicio, excepto iaas-service, aparece como REGISTRADO.

Pasos siguientes

[Actualizar los componentes del servidor de IaaS tras actualizar vRealize Automation.](#)

Actualizar los componentes del servidor de IaaS tras actualizar vRealize Automation

Tras actualizar vRealize Automation 6.2.5 a la versión 7.4, un administrador del sistema actualiza los componentes de servidor de IaaS, incluida la base de datos de Microsoft SQL Server.

Tiene dos opciones para actualizar los componentes del servidor de IaaS.

- Use el script de actualización automatizada del shell de IaaS.
- Utilice el archivo ejecutable del instalador de IaaS de vRealize Automation 7.4.

Si hay un componente del Catálogo de componentes comunes instalado, debe desinstalarlo antes de la actualización. Una vez finalizada la actualización, puede reinstalar el componente con la versión correcta. Para obtener más información, consulte la *Guía de instalación del catálogo de componentes comunes*. Si la guía no está disponible, utilice el procedimiento alternativo de la [Lista de comprobación para actualizar vRealize Automation](#).

Actualizar los componentes de IaaS mediante el script de actualización del shell

Utilice el script de actualización del shell para actualizar los componentes de IaaS tras actualizar cada dispositivo de vRealize Automation 6.2.5 a la versión 7.4.

El Dispositivo de vRealize Automation principal actualizado contiene un script de shell que permite actualizar cada nodo y componente de IaaS.

Puede ejecutar el script de actualización utilizando la consola de vSphere de la máquina virtual o utilizando una sesión de consola de SSH. Si utiliza la consola de vSphere, evitará problemas de conectividad de red intermitente que pueden interrumpir la ejecución del script.

Si detiene el script mientras está actualizando un componente, el script se ejecuta hasta que finalice la actualización del componente. Si algún componente del nodo no se actualiza, debe volver a ejecutar el script.

Cuando la actualización finalice, puede revisar el resultado de la actualización abriendo el archivo de log de actualización en `/usr/lib/vcac/tools/upgrade/upgrade.log`.

Requisitos previos

- Compruebe que la actualización de todos los dispositivos de vRealize Automation se haya realizado correctamente.
- Si reinicia un servidor de IaaS después de actualizar todos los dispositivos de vRealize Automation, tendrá que detener los servicios Windows de IaaS. Antes de actualizar los componentes de IaaS, detenga todos los servicios Windows de IaaS, a excepción del servicio de agente de administración, en el servidor.
- Antes de ejecutar el script del shell de actualización en el nodo de Dispositivo de vRealize Automation principal, compruebe que cada servicio está REGISTRADO.
 - a Vaya a la consola de administración de su dispositivo, utilizando su nombre de dominio completo, `https://va-hostname.domain.name:5480`.

- b Inicie sesión con el nombre de usuario **root** y la contraseña que especificó cuando se implementó el dispositivo.
- c Haga clic en **Servicios**.
- d Compruebe que todos los servicios, excepto `iaas-service`, tienen un estado REGISTRADO.
- Actualice el agente de administración en cada máquina virtual de IaaS de vRealize Automation.
 - a Abra un navegador y vaya a la página de instalación de IaaS de VMware vRealize Automation en el dispositivo de vRealize Automation usando el nombre de dominio completo, `https://virtual_appliance_host:5480/installer`.
 - b Haga clic en **Instalador del agente de administración**.
El instalador se descarga en la carpeta de descargas de forma predeterminada.
 - c Inicie sesión en cada máquina virtual de IaaS de vRealize Automation y actualice el agente de administración con el archivo del **instalador del agente de administración**.
- Compruebe que, en el nodo de sitio web de IaaS principal en el que están instalados los datos de Model Manager, se ha instalado Java SE Runtime Environment 8 de 64 bits (actualización 161) o posterior. Después de instalar Java, debe establecer la variable de entorno, `JAVA_HOME`, en la nueva versión.
- Inicie sesión en cada nodo del sitio web de IaaS y compruebe que la fecha de creación es anterior a la fecha de modificación del archivo `web.config`. Si la fecha de creación del archivo `web.config` es igual o posterior a la fecha de modificación, realice el procedimiento descrito en [Error en la actualización para el componente de sitio web de IaaS](#).
- Haga lo siguiente en cada nodo de IaaS para comprobar que en todos ellos hay un agente de administración actualizado de IaaS.
 - a Inicie sesión en la consola de administración del dispositivo de vRealize Automation.
 - b Seleccione **Configuración de vRA > Clúster**.
 - c Amplíe la lista de todos los componentes instalados en cada nodo de IaaS y localice el agente de administración de IaaS.
 - d Compruebe que la versión del agente de administración esté actualizada.
- Compruebe que se puede acceder a la copia de seguridad de la base de datos Microsoft SQL Server de IaaS en caso de que necesite revertir los datos.
- Elimine todos los nodos huérfanos de IaaS. Consulte [Eliminar nodos huérfanos en vRealize Automation](#).
- Compruebe que los snapshots de los servidores de IaaS de la implementación estén disponibles.
Si la actualización no se ha realizado correctamente, regrese al snapshot y la copia de seguridad de la base de datos e intente realizar otra actualización.

Procedimiento

- 1 Abra una nueva sesión de consola en el nodo principal o maestro de Dispositivo de vRealize Automation e inicie sesión con la cuenta raíz.

Si desea ejecutar el script de actualización mediante SSH, abra una sesión de consola de SSH.

- 2 Cambie los directorios a `/usr/lib/vcac/tools/upgrade/`.
- 3 En el símbolo del sistema, ejecute este comando para crear el archivo `upgrade.properties`.
`./generate_properties`
- 4 Abra el archivo `upgrade.properties` e introduzca todos los valores obligatorios.

En esta tabla se muestran los valores obligatorios, que varían en función del entorno. Por ejemplo, en un nodo que contiene un trabajo de DEM o un orquestador de DEM, las credenciales de DEM son obligatorias.

| Valor obligatorio | Descripción | Formato de credencial | Valor de ejemplo |
|---------------------|--|-----------------------|-----------------------|
| web_username | Nombre de usuario para el nodo web principal. Solo se requiere una vez. | Dominio\Usuario | iaasDomain\webuser |
| web_password | Contraseña para el nodo web principal. Solo se requiere una vez. | Contraseña | pa\$\$w0rd! |
| dem_username | Nombre de usuario para el trabajo de DEM o el orquestador de DEM. Se requiere para cada nodo donde se ha instalado un componente de DEM. | Dominio\Usuario | iaasDomain\demuser |
| dem_password | Contraseña para el trabajo de DEM o el orquestador de DEM. Se requiere para cada nodo donde se ha instalado un componente de DEM. | Contraseña | pa\$\$w0rd! |
| agent_username | Nombre de usuario para un agente como un agente de vSphere. Se requiere para cada nodo donde se ha instalado un componente de agente. | Dominio\Usuario | iaasDomain\agent_user |
| agent_password | Contraseña para un agente como un agente de vSphere. Se requiere para cada nodo donde se ha instalado un componente de agente. | Contraseña | pa\$\$w0rd! |
| vidm_admin_password | Contraseña del administrador de VIDM. Solo se requiere cuando se actualiza desde vRealize Automation 6.2.5. | vidm_password | pa\$\$w0rd! |

Por motivos de seguridad, el archivo `upgrade.properties` se suprime cuando se ejecuta el script de actualización del shell. Las propiedades en el archivo se definen a partir de la información disponible para cada componente de IaaS que se incluye con los agentes de administración de IaaS. Es importante que todos los agentes de administración de IaaS estén actualizados y en buen estado

antes de ejecutar el script de shell de `./generate_properties` o `./upgrade_from_62x`. Si algún agente de administración de IaaS tiene un problema cuando se ejecuta el script para actualizar el shell, consulte [La actualización no puede actualizar al agente de administración](#). Para volver a crear el archivo `upgrade.properties`, repita los pasos 2 y 3.

5 Ejecute el script de actualización.

a En el símbolo del sistema, introduzca `./upgrade_from_62x`.

b Pulse Entrar.

El script muestra cada nodo de IaaS y todos los componentes que hay instalados. El script valida cada componente antes de instalar la actualización. Si los valores no son correctos en el archivo `upgrade.properties`, el script falla.

El primer componente de servidor de IaaS puede tardar 30 minutos o más en finalizar. Durante la actualización, verá un mensaje parecido a `Upgrading server components for node web1-vra.mycompany.com`.

Si el script para actualizar el shell no se ejecuta correctamente, revise el archivo `upgrade.log`.

Puede volver a ejecutar el script de actualización tras resolver un problema. Antes de volver a ejecutar el script de actualización, vuelva a crear el archivo `upgrade.properties`, ábralo e introduzca todos los valores obligatorios.

6 (Opcional) Habilite la conmutación por error automática de Manager Service. Consulte [Habilitar la conmutación por error automática de Manager Service después de actualizar](#).

Pasos siguientes

[Restaurar el acceso al centro de control integrado de vRealize Orchestrator](#).

Actualizar los componentes de IaaS mediante el instalador de IaaS

Este método alternativo se puede utilizar para actualizar los componentes de IaaS después de actualizar vRealize Automation 6.2.5 a la versión 7.4.

Descargar el instalador de IaaS para actualizar los componentes de IaaS

Después de actualizar de vRealize Automation 6.2.5 a la versión 7.4, descargue el instalador de IaaS en la máquina virtual en la que están instalados los componentes de IaaS que desea actualizar.

Si aparecen advertencias de certificado durante el procedimiento, puede ignorarlos.

Nota Durante el proceso de actualización, el tipo de inicio de todos los servicios debe establecerse en Automático, excepto para las instancias de copia de seguridad pasiva de Manager Service. Si establece los servicios en Manual, se produce un error en el proceso de actualización.

Requisitos previos

- Compruebe que Microsoft .NET Framework 4.5.2 o posterior está instalado en la máquina virtual de instalación de IaaS. El instalador de .NET se puede descargar de la página de instalación de IaaS de VMware vRealize Automation. Si actualiza .NET a 4.5.2 después de desconectar los servicios, es posible que la máquina virtual se reinicie como parte de la instalación. Cuando esto sucede, hay que detener manualmente todos los servicios de IaaS en la máquina virtual, excepto el del agente de administración.
- Si usa Internet Explorer para la descarga, asegúrese de que la configuración de seguridad mejorada no está habilitada. Escriba `res://iesetup.dll/SoftAdmin.htm` en la barra de búsqueda y pulse Entrar.
- Inicie sesión como administrador local en el servidor de Windows en el que están instalados uno o varios de los componentes de IaaS que desea actualizar.

Procedimiento

- 1 Abra un navegador web.
- 2 Escriba la dirección URL de la página de instalación de IaaS de VMware vRealize Automation.
Por ejemplo, `https://vcac-va-hostname.domain.name:5480/installer`, donde `vcac-va-hostname.domain.name` es el nombre del nodo del dispositivo de vRealize Automation principal.
- 3 Haga clic en el **instalador de IaaS**.
- 4 El archivo del instalador, `setup__vcac-va-hostname.domain.name@5480.exe`, se envía a la carpeta de descargas de forma predeterminada.

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

Pasos siguientes

- Si tiene una instancia independiente de vRealize Orchestrator, consulte [Actualizar el dispositivo independiente de vRealize Orchestrator para su uso con vRealize Automation](#).
- Si tiene un clúster del dispositivo de vRealize Orchestrator externo, consulte [Actualizar el clúster de dispositivo externo de vRealize Orchestrator para su uso con vRealize Automation](#).
- Consulte [Actualizar los componentes de IaaS tras actualizar vRealize Automation](#).

Actualizar los componentes de IaaS tras actualizar vRealize Automation

Después de actualizar vRealize Automation 6.2.5 a la versión 7.4, debe actualizar la base de datos de SQL y configurar todos los sistemas en los que se han instalado componentes de IaaS. Puede usar estos pasos para instalaciones mínimas y distribuidas.

Nota El instalador de IaaS debe estar en la máquina que contiene los componentes de IaaS que desea actualizar. El instalador no se puede ejecutar desde una ubicación externa, excepto en el caso de la base de datos de Microsoft SQL, que también se puede actualizar de forma remota desde el nodo web.

Compruebe que los snapshots de los servidores de IaaS de la implementación estén disponibles. Si la actualización no se realiza correctamente, puede volver al snapshot e intentar otra actualización.

Realice la actualización de forma que los servicios se actualicen en el siguiente orden:

1 Sitios web de IaaS

Si está utilizando un equilibrador de carga, deshabilite el tráfico en todos los nodos no principales.

Finalice la actualización en un servidor antes de actualizar el siguiente servidor que esté ejecutando un servicio de sitio web. Empiece con el que tenga instalado el componente de datos de Model Manager.

Si realiza una actualización externa de la base de datos Microsoft SQL, deberá actualizar el SQL externo antes de actualizar el nodo web. Puede actualizar el SQL externo de forma remota desde el nodo web.

2 Manager Service

Actualice el servicio del administrador activo antes de actualizar el servicio del administrador pasivo.

Si no tiene el cifrado SSL habilitado en su instancia de SQL, anule la selección de **cifrado SSL** en el cuadro de diálogo de configuración de la actualización de IaaS.

3 Orquestador de DEM y trabajos

Actualice todas las orquestaciones DEM y los trabajos. Finalice la actualización en un servidor antes de actualizar el siguiente servidor.

4 Agentes

Finalice la actualización en un servidor antes de actualizar el siguiente servidor que esté ejecutando un agente.

5 Agente de administración

Se actualiza como parte del proceso de actualización.

Si está utilizando servicios diferentes en un servidor, la actualización actualiza los servicios en el orden correcto. Por ejemplo, si su sitio tiene un sitio web y servicios del administrador en el mismo servidor, seleccione ambos para la actualización. El instalador de actualización aplica las actualizaciones en el orden correcto. Debe completar la actualización en un servidor antes de iniciar una actualización en otro.

Nota Si su implementación utiliza un equilibrador de carga, el primer dispositivo que tenga previsto actualizar debe estar conectado al equilibrador de carga. Todas las demás instancias de Dispositivo de vRealize Automation deben deshabilitarse para el tráfico del equilibrador de carga antes de aplicar la actualización para evitar errores de almacenamiento en caché.

Requisitos previos

- Haga una copia de seguridad del entorno de vRealize Automation 6.2.5 existente.

- Si reinicia un servidor de IaaS después de actualizar todos los dispositivos de vRealize Automation, tendrá que detener los servicios Windows de IaaS. Antes de actualizar los componentes de IaaS, detenga todos los servicios Windows de IaaS, a excepción del servicio de agente de administración, en el servidor.
- [Descargar el instalador de IaaS para actualizar los componentes de IaaS.](#)
- Compruebe que el nodo principal del sitio web de IaaS donde se han instalado los datos de Model Manager tiene la versión de Java correcta. Debe tener instalado JAVA SE Runtime Environment 8, 64 bits, actualización 161 o posterior. Después de instalar Java, establezca la variable de entorno, JAVA_HOME, en la nueva versión.
- Compruebe que la fecha de creación sea anterior a la fecha de modificación del archivo web.config. Si la fecha de creación del archivo web.config es igual o posterior a la fecha de modificación, realice el procedimiento descrito en [Error en la actualización para el componente de sitio web de IaaS.](#)
- Si está actualizando desde vRealize Automation 6.2.5 y tiene una base de datos de Microsoft SQL externa, debe tener la versión correcta del agente de administración. La versión del agente de administración en la base de datos externa debe ser 7.0 o posterior antes de ejecutar la actualización del sitio web de IaaS. Puede comprobar la versión del agente de administración en el panel de control de la máquina virtual SQL externa. Si el agente de administración no es la versión 7.0 o posterior, siga estos pasos para actualizar al agente de administración.
 - a Abra un navegador y vaya a la página de instalación de IaaS de VMware vRealize Automation en el Dispositivo de vRealize Automation usando el nombre de dominio completo:
`https://virtual_appliance_host:5480/installer.`
 - b Haga clic en **Instalador del agente de administración.**
El instalador se descarga en la carpeta de descargas de forma predeterminada.
 - c Inicie sesión en la base de datos externa, actualice el agente de administración con el archivo del **instalador del agente de administración** y reinicie el servicio de agente de administración de Windows.
- Si hay un componente del Catálogo de componentes comunes instalado, debe desinstalarlo antes de la actualización. Para obtener más información, consulte la *guía de instalación del Catálogo de componentes comunes*, o siga los pasos indicados en la [Lista de comprobación para actualizar vRealize Automation.](#)

Procedimiento

- 1 Si está utilizando un equilibrador de carga, prepare su entorno.
 - a Compruebe que el nodo del sitio web de IaaS que contiene los datos de Model Manager esté habilitado para el tráfico del equilibrador de carga.
Puede identificar este nodo por la presencia de la carpeta `vCAC Folder\Server\ConfigTool.`
 - b Deshabilite los demás sitios web de IaaS y los servicios del administrador no principales para el tráfico del equilibrador de carga.

- 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 Escriba las credenciales del administrador para la implementación actual en la página de inicio de sesión.

El nombre de usuario es **root** y la contraseña es la que introdujo al implementar el dispositivo.

- 6 Seleccione **Aceptar certificado**.
- 7 En la página **Tipo de instalación**, compruebe que se haya seleccionado **Actualizar**.
Si no se ha seleccionado **Actualizar**, los componentes de este sistema ya están actualizados para esta versión.
- 8 Haga clic en **Siguiente**.
- 9 Configure las opciones de actualización.

| Opción | Acción |
|--|---|
| Si está actualizando los datos de Model Manager | Active la casilla Datos de Model Manager en la sección del Servidor vCAC. La casilla de verificación está activada de forma predeterminada. Actualice los datos de Model Manager solo una vez. Cuando se actualiza una instalación distribuida, los servidores web dejan de funcionar si las versiones de los servidores web y los datos de Model Manager no coinciden. Cuando finalice la actualización de los datos de Model Manager, los servidores web funcionarán como de costumbre. |
| Si no está actualizando los datos de Model Manager | Desactive la casilla Datos de Model Manager en la sección del Servidor vCAC. |
| Para preservar los flujos de trabajo personalizados como versión más reciente de los datos de Model Manager | Si está actualizando los datos de Model Manager, active la casilla Preservar mis versiones más recientes del flujo de trabajo en la sección de Flujos de trabajo de extensibilidad. La casilla de verificación está activada de forma predeterminada. Los flujos de trabajo personalizados siempre se preservan. Al seleccionar la casilla de verificación solo se determina el orden de las versiones. Si ha personalizado los flujos de trabajo en Model Manager, seleccione esta opción para que el flujo de trabajo más reciente se mantenga como la versión más reciente después de la actualización. Si no selecciona esta opción, la versión de cada flujo de trabajo proporcionado con vRealize Automation Designer se convierte en la más reciente tras la actualización. La versión más reciente antes de la actualización se convierte en la segunda más reciente. Para obtener información sobre vRealize Automation Designer, consulte <i>Extensibilidad del ciclo de vida</i> . |
| Si está actualizando un Distributed Execution Manager o un agente de proxy | Introduzca las credenciales para la cuenta del administrador en la sección de Cuenta de servicio. Todos los servicios que actualiza se ejecutan en esta cuenta. |

| Opción | Acción |
|--|---|
| Para especificar su base de datos de Microsoft SQL Server | <p>Si actualiza los datos de Model Manager, escriba los nombres del servidor de base de datos y la instancia de base de datos en el cuadro de texto Servidor. Introduzca un nombre de dominio completo (FQDN) para el nombre del servidor de la base de datos en el cuadro de texto Nombre de base de datos.</p> <p>Si la instancia de la base de datos está en un puerto SQL no predeterminado, incluya el número de puerto en la especificación de la instancia del servidor. El número de puerto predeterminado de Microsoft SQL es 1433.</p> <p>Cuando se actualizan los nodos del administrador, la opción SSL de MSSQL está seleccionada de forma predeterminada. Si la base de datos no utiliza SSL, desactive la opción Usar SSL para la conexión de la base de datos.</p> |

10 Haga clic en **Siguiente**.

11 Confirme que todos los servicios que se deben actualizar aparecen en la página Preparado para actualizar y haga clic en **Actualizar**.

Aparecerá la página Actualizando y un indicador de progreso. Cuando finalice el proceso de actualización, se habilitará el botón **Siguiente**.

12 Haga clic en **Siguiente**.

13 Haga clic en **Finalizar**.

14 Compruebe que se hayan reiniciado todos los servicios.

15 Repita estos pasos para cada servidor de IaaS en su implementación en el orden que se indica.

16 Cuando se hayan actualizado todos los componentes, inicie sesión en la consola de administración para el dispositivo y compruebe que todos los servicios, incluido IaaS, estén registrados ahora.

Todos los componentes seleccionados se actualizan a la nueva versión.

Pasos siguientes

- [Restaurar el acceso al centro de control integrado de vRealize Orchestrator](#).
- Si la implementación utiliza un equilibrador de carga, actualice cada nodo del equilibrador de carga para que use las comprobaciones de estado de vRealize Automation. Asimismo, vuelva a habilitar el tráfico del equilibrador de carga para cualquier nodo desconectado. Si en su implementación previa se utilizó una base de datos de PostgreSQL con un equilibrador de carga integrado, deshabilite todos los nodos en el grupo de PostgreSQL porque no son necesarios. Elimine el grupo cuando mejor le convenga.

Para obtener más información, consulte [Equilibrio de carga de vRealize Automation](#).
- (Opcional) Habilite la conmutación por error automática de Manager Service. Consulte [Habilitar la conmutación por error automática de Manager Service después de actualizar](#).

Restaurar el acceso al centro de control integrado de vRealize Orchestrator

Después de actualizar los componentes del servidor de IaaS, debe restaurar el acceso a vRealize Orchestrator.

Cuando se actualiza vRealize Automation 6.2.5 a la versión 7.4, debe realizar este procedimiento para incorporar la nueva característica de control de acceso basado en funciones. Este procedimiento se aplica a un entorno de alta disponibilidad.

Requisitos previos

Cree un snapshot del entorno vRealize Automation.

Procedimiento

- 1 Inicie sesión en la consola de administración de Dispositivo de vRealize Automation como usuario raíz utilizando el nombre de dominio totalmente cualificado de host del dispositivo, `https://va-hostname.domain.name:5480`.
- 2 Seleccione **Configuración de vRA > Base de datos**.
- 3 Identifique los nodos principal y de réplica.
- 4 En cada nodo de réplica, abra una sesión de SSH, inicie sesión como administrador y ejecute el siguiente comando:

```
service vco-server stop && service vco-configurator stop
```
- 5 En el nodo principal, abra una sesión de SSH, inicie sesión como administrador y ejecute el siguiente comando:

```
rm /etc/vco/app-server/vco-registration-id
```
- 6 En el nodo principal, cambie los directorios a `/etc/vco/app-server/`.
- 7 Abra el archivo `sso.properties`.
- 8 Si el nombre de la propiedad `com.vmware.o11n.sso.admin.group.name` contiene espacios o cualquier otro carácter Bash que se pueda aceptar como un carácter especial en un comando Bash, como un apóstrofo (') o un signo de dólar (\$), siga estos pasos.
 - a Copie la línea con la propiedad `com.vmware.o11n.sso.admin.group.name` e introduzca `AdminGroup` para el valor.
 - b Añada `#` al comienzo de la línea original con la propiedad `com.vmware.o11n.sso.admin.group.name` para comentar la línea.
 - c Guarde y cierre el archivo `sso.properties`.
- 9 Ejecute este comando:

```
vcac-vami vco-service-reconfigure
```
- 10 Si ha completado el paso 8, abra el archivo `sso.properties` y siga estos pasos.
 - a Quite el `#` del principio de la línea original con la propiedad `com.vmware.o11n.sso.admin.group.name` para eliminar el comentario de la línea.
 - b Elimine la copia de la línea con la propiedad `com.vmware.o11n.sso.admin.group.name`.
 - c Guarde y cierre el archivo `sso.properties`.

11 Ejecute este comando para reiniciar el servicio vco-server:

```
service vco-server restart
```

12 Ejecute este comando para reiniciar el servicio vco-configurator:

```
service vco-configurator restart
```

13 En la consola de administración de Dispositivo de vRealize Automation, haga clic en **Servicios** y espere hasta que todos los servicios del nodo principal estén REGISTRADOS.

14 Una vez que todos los servicios estén registrados, una los nodos de réplica de vRealize Automation al clúster de vRealize Automation para sincronizar la configuración de vRealize Orchestrator. Para obtener información, consulte [Reconfigurar la instancia integrada de vRealize Orchestrator para admitir la alta disponibilidad](#).

Pasos siguientes

[Actualizar vRealize Orchestrator tras actualizar vRealize Automation.](#)

Actualizar vRealize Orchestrator tras actualizar vRealize Automation

Debe actualizar la instancia de vRealize Orchestrator después de actualizar vRealize Automation 6.2.5 a la versión 7.4.

Con la publicación de vRealize Orchestrator 7.4, tiene dos opciones para actualizar vRealize Orchestrator una vez que se ha actualizado a vRealize Automation 7.4.

- Puede migrar el servidor externo de vRealize Orchestrator existente a la instancia de vRealize Orchestrator integrada que se incluye en vRealize Automation 7.4.
- Puede actualizar el servidor de vRealize Orchestrator independiente o en clúster para que funcione con vRealize Automation 7.4.

Migrar un servidor externo de vRealize Orchestrator a vRealize Automation

Puede migrar el servidor externo de vRealize Orchestrator existente a una instancia de vRealize Orchestrator integrada en vRealize Automation 7.4.

Puede implementar vRealize Orchestrator como instancia externa de servidor y configurar vRealize Automation para que funcione con esa instancia externa; también puede configurar y utilizar el servidor de vRealize Orchestrator que se incluye en Dispositivo de vRealize Automation.

VMware le recomienda que migre su vRealize Orchestrator externo al servidor de Orchestrator que está integrado en vRealize Automation. La migración de una instancia externa al Orchestrator integrado proporciona las siguientes ventajas:

- Reduce el coste total de propiedad.
- Simplifica el modelo de implementación.

- Mejora la eficiencia operativa.

Nota Considere utilizar un vRealize Orchestrator externo en los casos siguientes:

- Varios arrendatarios en el entorno de vRealize Automation
- Entorno geográficamente disperso
- Manejo de la carga de trabajo
- Uso de complementos específicos, como versiones anteriores del complemento de Site Recovery Manager Plug-in

Diferencias del Centro de control entre Orchestrator externo e integrado

Algunos de los elementos de menú que están disponibles en el Centro de control de un vRealize Orchestrator externo no se incluyen en la vista predeterminada del Centro de control correspondiente a una instancia de Orchestrator integrado.

En el Centro de control del servidor de Orchestrator integrado, algunas opciones están ocultas de forma predeterminada.

| Elemento de menú | Detalles |
|---|---|
| Licencias | El Orchestrator integrado está preconfigurado para usar vRealize Automation como proveedor de licencias. |
| Exportar o importar configuración | La configuración de Orchestrator integrado se incluye en los componentes de vRealize Automation exportados. |
| Configurar base de datos | El Orchestrator integrado utiliza la misma base de datos que vRealize Automation. |
| Programa de mejora de la experiencia de cliente | Puede unirse al Programa de mejora de la experiencia de cliente (CEIP) desde la interfaz de administración de dispositivos de vRealize Automation. Consulte <i>el Programa de mejora de la experiencia de cliente en Administración de vRealize Automation</i> . |

Otras opciones que están ocultas en la vista predeterminada del Centro de control son el cuadro de texto de la **dirección del host** y el botón de **cancelación de registro** de la página **Configurar proveedor de autenticación**.

Nota Para conocer todas las opciones del Centro de control de vRealize Orchestrator incorporadas en vRealize Automation, debe acceder a la página de administración avanzada de Orchestrator en la dirección https://vra-va-hostname.dominio.nombre_o_dirección_del_equilibrador_de_carga:8283/vco-controlcenter/#!/?advanced y hacer clic en el botón F5 del teclado para actualizar la página.

Migrar una instancia externa de vRealize Orchestrator en Windows a vRealize Automation

Después de actualizar vRealize Automation de la versión 6.x a la versión 7.4, puede migrar su Orchestrator 6.x externo existente instalado en Windows al servidor de Orchestrator que está integrado en vRealize Automation 7.4.

Nota Si tiene un entorno de vRealize Automation distribuido con varios nodos de vRealize Automation, realice el procedimiento de migración únicamente en el nodo principal de vRealize Automation.

Requisitos previos

- Haber migrado correctamente a vRealize Automation 7.4.
- Detenga el servicio del servidor de Orchestrator en el Orchestrator externo.
- Haga una copia de seguridad de la base de datos, incluido el esquema de base de datos, del servidor externo de Orchestrator.

Procedimiento

- 1 Descargue la herramienta de migración desde el servidor de destino de Orchestrator.
 - a Inicie sesión en el dispositivo de vRealize Automation mediante SSH como **raíz**.
 - b Descargue el archivo `migration-tool.zip` que se encuentra en el directorio `/var/lib/vco/downloads`.
- 2 Exporte la configuración de Orchestrator desde el servidor de Orchestrator de origen.
 - a Configure la variable de entorno `PATH` haciendo que apunte a la carpeta `bin` de la instancia de Java JRE que se instaló con Orchestrator.
 - b Cargue la herramienta de migración al servidor de Windows en el que está instalado el Orchestrator externo.
 - c Extraiga el archivo descargado en la carpeta de instalación de Orchestrator.

La ruta predeterminada de la carpeta de instalación de Orchestrator en una instalación basada en Windows es `C:\Archivos de programa\VMware\Orchestrator`.
 - d Ejecute como administrador el símbolo del sistema de Windows y desplácese hasta la carpeta `bin` en la carpeta de instalación de Orchestrator.

De forma predeterminada, la ruta de la carpeta `bin` es `C:\Archivos de programa\VMware\Orchestrator\migration-cli\bin`.
 - e Ejecute el comando `export` desde la línea de comandos.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Este comando combina los archivos de configuración de vRealize Orchestrator y los complementos en un archivo de exportación.

El archivo se crea en la misma carpeta que la carpeta `migration-cli`.

3 Migre la configuración exportada al servidor de Orchestrator que está integrado en vRealize Automation 7.4.

- a Cargue el archivo de configuración exportado en el directorio `/usr/lib/vco/tools/configuration-cli/bin` de Dispositivo de vRealize Automation.
- b En el directorio `/usr/lib/vco/tools/configuration-cli/bin`, cambie la propiedad del archivo de configuración del Orchestrator exportado.

```
chown vco:vco orchestrator-config-export-dirección_IP_orchestrator-fecha_hora.zip
```

- c Importe el archivo de configuración de Orchestrator en el servidor integrado de vRealize Orchestrator; para ello, ejecute el script `vro-configure` con el comando `import`.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-IP_dispositivo_orchestrator-fecha_hora.zip
```

4 Migre la base de datos a la base de datos interna de PostgreSQL; para ello, ejecute el script `vro-configure` con el comando `db-migrate`.

```
./vro-configure.sh db-migrate --sourceJdbcUrl URL_conexión_JDBC --sourceDbUsername usuario_base_datos --sourceDbPassword contraseña_usuario_base_datos
```

Nota Ponga las contraseñas que contienen caracteres especiales entre comillas simples.

La `URL_conexión_JDBC` depende del tipo de base de datos que utiliza.

PostgreSQL: `jdbc:postgresql://host:puerto/nombre_base_datos`

MSSQL: `jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\;` if using SQL authentication and
MSSQL: `jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\;domain=dominio\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@host:puerto:nombre_base_datos`

La información de inicio de sesión a la base de datos predeterminada es:

| | |
|---|--------|
| <code>nombre_de_base_de_datos</code> | vmware |
| <code>usuario_de_base_de_datos</code> | vmware |
| <code>contraseña_de_usuario_de_base_de_datos</code> | vmware |

- 5 Si migró vRealize Automation en lugar de actualizarlo, elimine los certificados Single Sign-On de la base de datos de la instancia de Orchestrator integrada.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore WHERE id='cakeystore-id';"
```

Ha migrado correctamente un vRealize Orchestrator 6.x externo instalado en Windows a una instancia de vRealize Orchestrator integrada en vRealize Automation 7.4.

Pasos siguientes

Configure el servidor integrado de vRealize Orchestrator. Consulte [Configure el servidor integrado de vRealize Orchestrator](#).

Migrar un dispositivo virtual vRealize Orchestrator 6.x externo a vRealize Automation 7.4

Después de actualizar el vRealize Automation desde la versión 6.x a la versión 7.4, puede migrar el dispositivo virtual Orchestrator 6.x externo al servidor de Orchestrator que está integrado en vRealize Automation 7.4.

Nota Si tiene un entorno de vRealize Automation distribuido con varios nodos de Dispositivo de vRealize Automation, realice el procedimiento de migración únicamente en el nodo principal de vRealize Automation.

Requisitos previos

- Haber migrado correctamente a vRealize Automation 7.4.
- Detenga el servicio del servidor de Orchestrator en el Orchestrator externo.
- Haga una copia de seguridad de la base de datos, incluido el esquema de base de datos, del servidor externo de Orchestrator.

Procedimiento

- 1 Descargue la herramienta de migración desde el servidor de destino de Orchestrator al de origen.
 - a Inicie sesión en el dispositivo virtual vRealize Orchestrator 6.x sobre SSH como **raíz**.
 - b En el directorio `/var/lib/vco`, ejecute el comando `scp` para descargar el archivo `migration-tool.zip`.

```
scp root@VRA-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
```

- c Ejecute el comando `unzip` para extraer el archivo de la herramienta de migración.

```
unzip migration-tool.zipy7
```

2 Exporte la configuración de Orchestrator desde el servidor de Orchestrator de origen.

- a En el directorio `/var/lib/vco/migration-cli/bin`, ejecute el comando `export`.

```
./vro-migrate.sh export
```

Este comando combina los archivos de configuración de VMware vRealize Orchestrator y los complementos en un archivo de exportación.

Se crea un archivo con el nombre de archivo `orchestrator-config-export-orchestrator_ip_address-date_hour.zip` en la carpeta `/var/lib/vco`.

3 Migre la configuración exportada al servidor de Orchestrator que está integrado en vRealize Automation 7.4.

- a Inicie sesión en Dispositivo de vRealize Automation sobre SSH como **raíz**.
- b En el directorio `/usr/lib/vco/tools/configuration-cli/bin`, ejecute el comando `scp` para descargar el archivo de configuración exportado.

```
scp root@nombre_DNS_o_IP_orchestrator:/var/lib/vco/orchestrator-config-export-  
dirección_IP_orchestrator-fecha_hora.zip ./
```

- c Cambie la propiedad del archivo de configuración de Orchestrator exportado.

```
chown vco:vco orchestrator-config-export-dirección_IP_orchestrator-fecha_hora.zip
```

- d Detenga el servicio del servidor de Orchestrator y el servicio del centro de control del servidor integrado de vRealize Orchestrator.

```
service vco-server stop && service vco-configurator stop
```

- e Importe el archivo de configuración de Orchestrator en el servidor integrado de vRealize Orchestrator; para ello, ejecute el script `vro-configure` con el comando `import`.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --  
skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path  
orchestrator-config-export-IP_dispositivo_orchestrator-fecha_hora.zip
```

4 Si el servidor externo de Orchestrator desde el que desea migrar utiliza la base de datos integrada de PostgreSQL, edite los archivos de configuración de la base de datos.

- a En el archivo `/var/vmware/vpostgres/current/pgdata/postgresql.conf`, quite la marca de comentario de la línea `listen_addresses`.
- b Establezca los valores de `listen_addresses` con un carácter comodín (*).

```
listen_addresses = '*'
```

- c Anexe una línea al archivo `/var/vmware/vpostgres/current/pgdata/pg_hba.conf`.

```
host all all vra-va-ip-address/32 md5
```

Nota El archivo `pg_hba.conf` requiere el uso de un formato de prefijo CIDR en lugar de una dirección IP y una máscara de subred.

- d Reinicie el servicio del servidor de PostgreSQL.

```
service vpostgres restart
```

- 5 Migre la base de datos a la base de datos interna de PostgreSQL; para ello, ejecute el script `vro-configure` con el comando `db-migrate`.

```
./vro-configure.sh db-migrate --sourceJdbcUrl URL_conexión_JDBC --sourceDbUsername usuario_base_datos --sourceDbPassword contraseña_usuario_base_datos
```

Nota Ponga las contraseñas que contienen caracteres especiales entre comillas simples.

La `URL_conexión_JDBC` depende del tipo de base de datos que utiliza.

PostgreSQL: `jdbc:postgresql://host:puerto/nombre_base_datos`

MSSQL: `jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\;` if using SQL authentication and
MSSQL: `jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\;domain=dominio\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@host:puerto:nombre_base_datos`

La información de inicio de sesión a la base de datos predeterminada es:

| | |
|---|--------|
| <code>nombre_de_base_de_datos</code> | vmware |
| <code>usuario_de_base_de_datos</code> | vmware |
| <code>contraseña_de_usuario_de_base_de_datos</code> | vmware |

- 6 Si migró vRealize Automation en lugar de actualizarlo, elimine los certificados Single Sign-On de la base de datos de la instancia de Orchestrator integrada.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore WHERE id='cakeystore-id';"
```

- 7 Regrese a la configuración predeterminada de los archivos `postgresql.conf` y `pg_hba.conf`.
 - a Reinicie el servicio del servidor de PostgreSQL.

Ha migrado correctamente una instancia externa del dispositivo virtual vRealize Orchestrator 6.x a una instancia de vRealize Orchestrator integrada en vRealize Automation 7.4.

Pasos siguientes

Configure el servidor integrado de vRealize Orchestrator. Consulte [Configure el servidor integrado de vRealize Orchestrator](#).

Configure el servidor integrado de vRealize Orchestrator

Después de exportar la configuración de un servidor externo de Orchestrator e importarla a vRealize Automation 7.4, debe configurar el servidor de Orchestrator integrado en vRealize Automation.

Requisitos previos

Migre la configuración del vRealize Orchestrator externo al interno.

Procedimiento

- 1 Inicie sesión en Dispositivo de vRealize Automation sobre SSH como **raíz**.
- 2 Inicie el servicio del centro de control y el servicio del servidor de Orchestrator en el servidor de vRealize Orchestrator integrado.

```
service vco-configurator start && service vco-server start
```

- 3 Inicie sesión en el centro del control del servidor integrado de Orchestrator como **administrador**.

Nota Si migra desde una instancia externa de vRealize Orchestrator 7.4, vaya directamente al paso 5.

- 4 Compruebe que Orchestrator esté configurado correctamente en la página **Validar configuración** del centro de control.
- 5 Si el Orchestrator externo se configuró para funcionar en modo de clúster, vuelva a configurar el clúster de Orchestrator en vRealize Automation.
 - a Diríjase a la página avanzada de **Administración de clústeres de Orchestrator** en https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#!/control-app/ha?remove-nodes.

Nota Si no aparecen las casillas de verificación **Quitar** junto a los nodos existentes en el clúster, debe actualizar la página del navegador haciendo clic en el botón F5 del teclado.

- b Seleccione las casillas de verificación junto a los nodos de Orchestrator externos y haga clic en **Quitar** para excluirlos del clúster.
- c Para salir de la página de administración avanzada de clústeres, elimine la cadena de `remove-nodes` de la URL y actualice la página del navegador haciendo clic en el botón F5 del teclado.
- d En la página **Validar configuración** del centro de control, compruebe que Orchestrator está configurado correctamente.

- 6 (opcional) En la pestaña **Certificado de firma del paquete** de la página **Certificados**, genere un nuevo certificado de firma del paquete.
- 7 (opcional) Cambie los valores del **Arrendatario predeterminado** y del **Grupo de administradores** en la página **Configurar proveedor de autenticación**.
- 8 Compruebe que el servicio de vco-server aparece como REGISTRADO en la pestaña **Servicios** de la consola de administración de Dispositivo de vRealize Automation.
- 9 Seleccione los servicios de vco del servidor externo de Orchestrator y haga clic en **Eliminar del registro**.

Pasos siguientes

- Importe todos los certificados de confianza del servidor de Orchestrator externo al almacén de confianza del Orchestrator integrado.
- Una los nodos de réplica de vRealize Automation al clúster de vRealize Automation para sincronizar la configuración de Orchestrator.

Para obtener más información, consulte *Volver a configurar el vRealize Orchestrator integrado de destino para propiciar alta disponibilidad* en la *Instalación o actualización de vRealize Automation*.

Nota Las instancias de vRealize Orchestrator se agrupan en clústeres automáticamente y están disponibles para usarse.

- Reinicie el servicio de vco-configurator en todos los nodos del clúster.
- Actualice el terminal de vRealize Orchestrator para que apunte al servidor de Orchestrator integrado que se migró.
- Agregue el host de vRealize Automation y de IaaS al inventario del complemento vRealize Automation mediante la ejecución de los flujos de trabajo Añadir un host de vRA y Añadir un host de IaaS.

Actualizar el dispositivo independiente de vRealize Orchestrator para su uso con vRealize Automation

Si mantiene un dispositivo de vRealize Orchestrator independiente para usarlo con vRealize Automation, tendrá que actualizar el dispositivo independiente cuando actualice vRealize Automation desde 6.2.5 a 7.4.

Las instancias integradas de vRealize Orchestrator se actualizan como parte de la actualización del dispositivo de vRealize Automation. No hay que realizar ninguna otra acción para una instancia integrada.

Si va a actualizar un clúster de dispositivo de vRealize Orchestrator, consulte [Actualizar el clúster de dispositivo externo de vRealize Orchestrator para su uso con vRealize Automation](#).

Requisitos previos

- [Instalar la actualización en el dispositivo de vRealize Automation](#).

- Actualice los componentes de IaaS tal y como se describe en [Actualizar los componentes del servidor de IaaS tras actualizar vRealize Automation](#).
- Desmonte todos los sistemas de archivos de red. Consulte *Administración de máquinas virtuales de vSphere* en la documentación de vSphere.
- Aumente la memoria del dispositivo de vSphere Orchestrator hasta por lo menos 6 GB. Consulte *Administración de máquinas virtuales de vSphere* en la documentación de vSphere.
- Tome un snapshot de la máquina virtual de vSphere Orchestrator. Consulte *Administración de máquinas virtuales de vSphere* en la documentación de vSphere.
- Si utiliza una base de datos externa, cree una copia de seguridad de la misma.
- Si utiliza la base de datos preconfigurada de PostgreSQL en vSphere Orchestrator, cree una copia de seguridad de la base de datos a través del menú **Exportar base de datos** del centro de control de vSphere.

Procedimiento

- 1 Utilice uno de los métodos que se describen para actualizar su vRealize Orchestrator independiente.
 - [Actualizar Orchestrator Appliance mediante el repositorio predeterminado de VMware](#).
 - [Actualizar Orchestrator Appliance con una imagen ISO](#).
 - [Actualizar Orchestrator Appliance con un repositorio específico](#).
- 2 Desde el centro de control, actualice el complemento NSX de vRealize Automation.

Actualizar Orchestrator Appliance mediante el repositorio predeterminado de VMware

Puede configurar Orchestrator para que descargue el paquete de actualización desde el repositorio predeterminado de VMware.

Requisitos previos

- Desmonte todos los sistemas de archivos de red. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente la memoria de Orchestrator Appliance hasta por lo menos 6 GB. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente el tamaño del disco de la máquina virtual de vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Asegúrese de que la partición raíz de Orchestrator Appliance tenga al menos 3 GB de espacio libre disponible. Para obtener más información sobre cómo aumentar el tamaño de una partición de disco, consulte el artículo de la base de conocimientos 1004071: <http://kb.vmware.com/kb/1004071>.
- Tome una snapshot de la máquina virtual de Orchestrator. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Si utiliza una base de datos externa, cree una copia de seguridad de la misma.

- Si utiliza la base de datos preconfigurada en Orchestrator PostgreSQL, cree una copia de seguridad de la base de datos desde el menú **Exportar base de datos** del centro de control.

Procedimiento

- 1 Acceda a la Interfaz de administración de dispositivos virtuales (VAMI) en https://servidor_orchestrator:5480 e inicie sesión como **raíz**.
- 2 En la pestaña **Actualizar**, haga clic en **Configuración**.
Se selecciona el botón de opción junto a **Usar repositorio predeterminado**.
- 3 En la página **Estado**, haga clic en **Buscar actualizaciones**.
- 4 Si hay actualizaciones disponibles, haga clic en **Instalar actualizaciones**.
- 5 Acepte el contrato de licencia del usuario final de VMware y confirme que desea instalar la actualización.
- 6 Para completar la actualización, reinicie Orchestrator Appliance.
 - a Inicie sesión de nuevo en la Interfaz de administración de dispositivos virtuales (VAMI) como **raíz**.
- 7 (opcional) En la pestaña **Actualizar**, compruebe que se haya instalado correctamente la última versión del Orchestrator Appliance.
- 8 Inicie sesión en el centro de control como **raíz**.
- 9 Si tiene pensado crear un clúster de las instancias de Orchestrator, vuelva a configurar la configuración de los hosts.
 - a En la página **Configuración de hosts** del centro de control, haga clic en **CAMBIAR**.
 - b Introduzca el nombre del host del servidor del equilibrador de carga en lugar del nombre de Orchestrator Appliance de vRealize.
- 10 Vuelva a configurar la autenticación.
 - a Si, antes de la actualización, el servidor de Orchestrator se configuró para que usara **LDAP** o **SSO (heredado)** como método de autenticación, configure **vSphere** o **vRealize Automation** como proveedor de autenticación.
 - b Si la autenticación ya está establecida en **vSphere** o **vRealize Automation**, elimine la configuración del registro y vuelva a registrarla.

Nota Si, antes de la actualización, su instancia de Orchestrator ha utilizado **vSphere** como proveedor de autenticación y se ha configurado para conectarse al nombre de dominio completo o la dirección IP de vCenter Server, en caso de que tenga una instancia externa de Platform Services Controller, después de la actualización debe configurar Orchestrator para que se conecte al nombre de dominio completo o la dirección IP de la instancia de Platform Services Controller que contiene la instancia de vCenter Single Sign-On. También debe importar manualmente a Orchestrator los certificados de todas las instancias de Platform Services Controller que compartan el mismo dominio de vCenter Single Sign-On.

Ha actualizado correctamente Orchestrator Appliance.

Pasos siguientes

Compruebe que Orchestrator esté configurado correctamente en la página **Validar configuración** del centro de control.

Actualizar Orchestrator Appliance con una imagen ISO

Puede configurar Orchestrator para que descargue el paquete de actualización desde un archivo de imagen ISO montado en la unidad de CD-ROM del dispositivo.

Requisitos previos

- Desmonte todos los sistemas de archivos de red. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente la memoria de Orchestrator Appliance hasta por lo menos 6 GB. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente el tamaño del disco de la máquina virtual de vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Asegúrese de que la partición raíz de Orchestrator Appliance tenga al menos 3 GB de espacio libre disponible. Para obtener más información sobre cómo aumentar el tamaño de una partición de disco, consulte el artículo de la base de conocimientos 1004071: <http://kb.vmware.com/kb/1004071>.
- Tome una snapshot de la máquina virtual de Orchestrator. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Si utiliza una base de datos externa, cree una copia de seguridad de la misma.
- Si utiliza la base de datos preconfigurada en Orchestrator PostgreSQL, cree una copia de seguridad de la base de datos desde el menú **Exportar base de datos** del centro de control.

Procedimiento

- 1 Descargue el archivo `VMware-vRO-Appliance-versión-número_compilación-updaterepo.iso` del sitio oficial de descargas de VMware.
- 2 Conecte la unidad de CD-ROM de la máquina virtual de Orchestrator Appliance. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- 3 Monte el archivo de imagen ISO en la unidad de CD-ROM del dispositivo. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- 4 Acceda a la Interfaz de administración de dispositivos virtuales (VAMI) en `https://servidor_orchestrator:5480` e inicie sesión como **raíz**.
- 5 En la pestaña **Actualizar**, haga clic en **Configuración**.

- 6 Seleccione el botón de opción junto a **Usar actualizaciones de CD-ROM**.
- 7 Vuelva a la página **Estado**.

Se mostrará la versión de la actualización disponible.
- 8 Haga clic en **Instalar actualizaciones**.
- 9 Acepte el contrato de licencia del usuario final de VMware y confirme que desea instalar la actualización.
- 10 Para completar la actualización, reinicie Orchestrator Appliance.
 - a Inicie sesión de nuevo en la Interfaz de administración de dispositivos virtuales (VAMI) como **raíz**.
- 11 (opcional) En la pestaña **Actualizar**, compruebe que se haya instalado correctamente la última versión del Orchestrator Appliance.
- 12 Inicie sesión en el centro de control como **raíz**.
- 13 Si tiene pensado crear un clúster de las instancias de Orchestrator, vuelva a configurar la configuración de los hosts.
 - a En la página **Configuración de hosts** del centro de control, haga clic en **CAMBIAR**.
 - b Introduzca el nombre del host del servidor del equilibrador de carga en lugar del nombre de Orchestrator Appliance de vRealize.
- 14 Vuelva a configurar la autenticación.
 - a Si, antes de la actualización, el servidor de Orchestrator se configuró para que usara **LDAP** o **SSO (heredado)** como método de autenticación, configure **vSphere** o **vRealize Automation** como proveedor de autenticación.
 - b Si la autenticación ya está establecida en **vSphere** o **vRealize Automation**, elimine la configuración del registro y vuelva a registrarla.

Nota Si, antes de la actualización, su instancia de Orchestrator ha utilizado **vSphere** como proveedor de autenticación y se ha configurado para conectarse al nombre de dominio completo o la dirección IP de vCenter Server, en caso de que tenga una instancia externa de Platform Services Controller, después de la actualización debe configurar Orchestrator para que se conecte al nombre de dominio completo o la dirección IP de la instancia de Platform Services Controller que contiene la instancia de vCenter Single Sign-On. También debe importar manualmente a Orchestrator los certificados de todas las instancias de Platform Services Controller que compartan el mismo dominio de vCenter Single Sign-On.

Ha actualizado correctamente Orchestrator Appliance.

Pasos siguientes

Compruebe que Orchestrator esté configurado correctamente en la página **Validar configuración** del centro de control.

Actualizar Orchestrator Appliance con un repositorio específico

Puede configurar Orchestrator para que utilice un repositorio local, en el que ha cargado el archivo de actualización.

Requisitos previos

- Desmonte todos los sistemas de archivos de red. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente la memoria de Orchestrator Appliance hasta por lo menos 6 GB. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente el tamaño del disco de la máquina virtual de vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Asegúrese de que la partición raíz de Orchestrator Appliance tenga al menos 3 GB de espacio libre disponible. Para obtener más información sobre cómo aumentar el tamaño de una partición de disco, consulte el artículo de la base de conocimientos 1004071: <http://kb.vmware.com/kb/1004071>.
- Tome una snapshot de la máquina virtual de Orchestrator. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Si utiliza una base de datos externa, cree una copia de seguridad de la misma.
- Si utiliza la base de datos preconfigurada en Orchestrator PostgreSQL, cree una copia de seguridad de la base de datos desde el menú **Exportar base de datos** del centro de control.

Procedimiento

- 1 Prepare el repositorio local para las actualizaciones.
 - a Instale y configure un servidor web local.
 - b Descargue el archivo VMware-vR0-Appliance-versión-número_compilación-updaterepo.zip del sitio oficial de descargas de VMware.
 - c Extraiga el archivo .ZIP en el repositorio local.
- 2 Acceda a la Interfaz de administración de dispositivos virtuales (VAMI) en https://servidor_orchestrator:5480 e inicie sesión como **raíz**.
- 3 En la pestaña **Actualizar**, haga clic en **Configuración**.
- 4 Seleccione el botón de opción junto a **Usar repositorio especificado**.
- 5 Escriba la dirección URL del repositorio local que apunte al directorio Update_Repo.
`http://servidor_web_local:puerto/build/mts/release/bora-número_compilación/publish/exports/Update_Repo`
- 6 Si el repositorio local requiere autenticación, escriba el nombre de usuario y la contraseña.
- 7 Haga clic en **Guardar configuración**.
- 8 En la página **Estado**, haga clic en **Buscar actualizaciones**.

- 9 Si hay actualizaciones disponibles, haga clic en **Instalar actualizaciones**.
- 10 Acepte el contrato de licencia del usuario final de VMware y confirme que desea instalar la actualización.
- 11 Para completar la actualización, reinicie Orchestrator Appliance.
 - a Inicie sesión de nuevo en la Interfaz de administración de dispositivos virtuales (VAMI) como **raíz**.
- 12 (opcional) En la pestaña **Actualizar**, compruebe que se haya instalado correctamente la última versión del Orchestrator Appliance.
- 13 Inicie sesión en el centro de control como **raíz**.
- 14 Si tiene pensado crear un clúster de las instancias de Orchestrator, vuelva a configurar la configuración de los hosts.
 - a En la página **Configuración de hosts** del centro de control, haga clic en **CAMBIAR**.
 - b Introduzca el nombre del host del servidor del equilibrador de carga en lugar del nombre de Orchestrator Appliance de vRealize.
- 15 Vuelva a configurar la autenticación.
 - a Si, antes de la actualización, el servidor de Orchestrator se configuró para que usara **LDAP** o **SSO (heredado)** como método de autenticación, configure **vSphere** o **vRealize Automation** como proveedor de autenticación.
 - b Si la autenticación ya está establecida en **vSphere** o **vRealize Automation**, elimine la configuración del registro y vuelva a registrarla.

Nota Si, antes de la actualización, su instancia de Orchestrator ha utilizado **vSphere** como proveedor de autenticación y se ha configurado para conectarse al nombre de dominio completo o la dirección IP de vCenter Server, en caso de que tenga una instancia externa de Platform Services Controller, después de la actualización debe configurar Orchestrator para que se conecte al nombre de dominio completo o la dirección IP de la instancia de Platform Services Controller que contiene la instancia de vCenter Single Sign-On. También debe importar manualmente a Orchestrator los certificados de todas las instancias de Platform Services Controller que compartan el mismo dominio de vCenter Single Sign-On.

Ha actualizado correctamente Orchestrator Appliance.

Pasos siguientes

Compruebe que Orchestrator esté configurado correctamente en la página **Validar configuración** del centro de control.

Actualizar el clúster de dispositivo externo de vRealize Orchestrator para su uso con vRealize Automation

Si utiliza un clúster de dispositivo de vRealize Orchestrator con vRealize Automation, debe actualizar el clúster de dispositivo de Orchestrator a la versión 7.4. Para ello, debe actualizar una única instancia y unir los nodos de 7.4 que se acaban de instalar con la instancia actualizada.

Requisitos previos

- [Instalar la actualización en el dispositivo de vRealize Automation.](#)
- Actualice los componentes de IaaS. Consulte [Actualizar los componentes del servidor de IaaS tras actualizar vRealize Automation.](#)
- Configure un equilibrador de carga para distribuir el tráfico entre varias instancias de vRealize Orchestrator. Consulte la [guía de configuración del equilibrio de carga de vRealize Orchestrator.](#)
- Tome una snapshot de todos los nodos de servidor de vRealize Orchestrator.
- Realice una copia de seguridad de la base de datos compartida de vRealize Orchestrator.

Procedimiento

- 1 Desde el centro de control, actualice el complemento NSX de vRealize Automation.
- 2 Detenga los servicios de Orchestrator vco-server y vco-configurator en todos los nodos del clúster.
- 3 Actualice únicamente una de las instancias del servidor de Orchestrator en el clúster con uno de los procedimientos que se han descrito.
- 4 Implemente un nuevo Orchestrator Appliance en la versión 7.4.
 - a Configure el nuevo nodo con los ajustes de red de una instancia existente no actualizada que forme parte del clúster.
- 5 Acceda al centro de control del segundo nodo para iniciar el asistente para configuración.
 - a Vaya a `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter`.
 - b Inicie sesión como **raíz** con la contraseña que introdujo durante la implementación de OVA.
- 6 Seleccione el tipo de implementación **Orchestrator en clúster**.

Al seleccionar este tipo, hace que el nodo se una a un clúster de Orchestrator existente.
- 7 En el cuadro de texto **Nombre del host**, escriba el nombre del host o la dirección IP de la primera instancia del servidor de Orchestrator.

Nota Debe ser la IP local o el nombre de host de la instancia de Orchestrator a la que se une el segundo nodo. No debe usar la dirección del equilibrador de carga.

- 8 En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de raíz de la instancia del servidor de Orchestrator.

- 9 Haga clic en **Unir**. La instancia de Orchestrator clona la configuración del nodo, al cual se une.
El servicio del servidor de Orchestrator de ambos nodos se reinicia automáticamente.
- 10 Acceda al Centro de Control del clúster actualizado de Orchestrator a través de la dirección del equilibrador de carga e inicie sesión como **administrador**.
- 11 En la página **Administración de clústeres de Orchestrator**, asegúrese de que las cadenas **Huella digital de configuración activa** y **Huella digital de configuración pendiente** de todos los nodos del clúster coincidan.

Nota Puede que necesite actualizar la página varias veces hasta que coincidan ambas cadenas.

- 12 Compruebe que el clúster de vRealize Orchestrator se haya configurado correctamente en la página **Validar configuración** del centro de control.
- 13 (opcional) Repita los pasos 3 a 8 con cada nodo adicional del clúster.
- 14 Desde el centro de control, actualice el complemento NSX de vRealize Automation.

Ha actualizado correctamente el clúster de Orchestrator.

Pasos siguientes

[Configurar los equilibradores de carga.](#)

Añadir usuarios o grupos a una conexión de Active Directory

Puede añadir usuarios o grupos a una conexión existente de Active Directory.

El sistema de autenticación de usuarios de Administración de directorios importa los datos de Active Directory cuando se añaden grupos y usuarios. La velocidad con la que se realiza el transporte de los datos está limitada por las capacidades de Active Directory. Por lo tanto, las acciones pueden durar mucho tiempo en función del número de grupos y usuarios que se añadan. Para minimizar los problemas, limite los grupos y usuarios a únicamente los grupos y usuarios que hagan falta para una acción de vRealize Automation. Si se producen errores, cierre las aplicaciones que no sean necesarias y compruebe que su implementación tenga asignada una cantidad de memoria adecuada a Active Directory. Si el problema persiste, aumente la asignación de memoria para Active Directory. En el caso de implementaciones con grandes números de usuarios y grupos, quizás tenga que aumentar la asignación de memoria de Active Directory hasta los 24 GB.

Si sincroniza una implementación de vRealize Automation con muchos usuarios y grupos, se pueden producir retrasos antes de que estén disponibles los detalles del registro. La marca de hora del archivo de log y la hora de finalización que se muestra en la consola pueden ser diferentes.

Si los miembros de un grupo no están en la lista de usuarios, se añadirán a esta cuando se añada el grupo desde Active Directory. Cuando sincroniza un grupo, los usuarios que no tengan Usuarios del dominio como su grupo principal en Active Directory no se sincronizan.

Nota No se puede cancelar una acción de sincronización una vez que se inicia.

Requisitos previos

- Conector instalado y con el código de activación activado. Seleccione los atributos predeterminados necesarios y añada atributos adicionales a la página Atributos de usuario.

Consulte [PLUGINS_ROOT/com.vmware.vra.prepare.use.doc/GUID-9B25F502-EC8C-40CF-8ACF-4731B5A6903A.html](https://docs.vmware.com/en/VMware-Realize-Automation/7.0/PLUGINS_ROOT/com.vmware.vra.prepare.use.doc/GUID-9B25F502-EC8C-40CF-8ACF-4731B5A6903A.html).

- Lista de grupos y usuarios de Active Directory para sincronizar desde Active Directory.
- Para Active Directory en LDAP, la información necesaria incluye DN base, DN de enlace y contraseña de DN de enlace.
- Para la Autenticación de Windows integrada de Active Directory, la información necesaria incluye la dirección UPN del usuario de enlace del dominio y la contraseña.
- Si se accede a Active Directory sobre SSL, se necesita una copia del certificado SSL.
- Si tiene un Active Directory de varios bosques integrado con la autenticación de Windows y el grupo local de dominios contiene a miembros de bosques diferentes, haga lo siguiente. Añada al usuario de enlace al grupo Administradores del grupo local de dominios. De lo contrario, estos miembros no estarán en el grupo local de dominios.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Directorios**.
- 2 Haga clic en el nombre de directorio que desee.
- 3 Haga clic en **Configuración de sincronización** para abrir un cuadro de diálogo con opciones de sincronización.
- 4 Haga clic en el icono adecuado, en función de si desea cambiar la configuración del usuario o del grupo.

Para editar la configuración del grupo:

- Para añadir grupos, haga clic en el icono **+** para añadir una línea para definiciones de DN de grupo e introduzca el DN de grupo adecuado.
- Si desea eliminar una definición de DN de grupo, haga clic en el icono **x** para el DN de grupo que desee.

Para editar la configuración del usuario:

- ◆ Para añadir usuarios, haga clic en el icono **+** para añadir una línea para la definición de DN de usuario e introduzca el DN de usuario adecuado.

Si desea eliminar una definición de DN de usuario, haga clic en el icono **x** para el DN de usuario que desee.

- 5 Haga clic en **Guardar** para guardar los cambios sin tener que sincronizar las actualizaciones de forma inmediata. Haga clic en **Guardar y sincronizar** para guardar los cambios y sincronizar las actualizaciones de forma inmediata.

Configurar los equilibradores de carga

Si la implementación usa equilibradores de carga, vuelva a habilitar los nodos secundarios y las comprobaciones de estado, y revierta la configuración de tiempo de espera del equilibrador de carga.

Las comprobaciones de estado de vRealize Automation varían según la versión. Para obtener más información, consulte *Guía de configuración del equilibrio de carga de vRealize Automation* en la documentación de [VMware vRealize Automation](#).

Cambie la configuración de tiempo de espera del equilibrador de carga de 10 minutos al valor predeterminado.

Tareas posteriores a la actualización para actualizar vRealize Automation

Después de actualizar vRealize Automation 6.2.5 o a 7.4, realice las tareas posteriores a la actualización que sean necesarias.

Configurar puertos para implementaciones de alta disponibilidad

Tras finalizar una actualización en una implementación de alta disponibilidad, debe configurar el equilibrador de carga para que transfiera el tráfico del puerto 8444 al dispositivo de vRealize Automation para poder usar la funcionalidad de la consola remota.

Para obtener más información, consulte *Guía de configuración del equilibrio de carga de vRealize Automation* en la documentación de [vRealize Automation](#).

Reconfigurar la instancia integrada de vRealize Orchestrator para admitir la alta disponibilidad

En las implementaciones de alta disponibilidad, debe volver a unir cada dispositivo de vRealize Automation de réplica de destino manualmente al clúster para, de este modo, dar cabida a la alta disponibilidad en la instancia de vRealize Orchestrator integrada.

Requisitos previos

Inicie sesión en la consola de administración del dispositivo de vRealize Automation de réplica de destino.

- 1 Inicie el navegador y abra la consola de administración de vRealize Automation de réplica de destino usando el nombre de dominio completo (FQDN) del dispositivo virtual de réplica de destino:
`https://vra-va-hostname.domain.name:5480`.
- 2 Inicie sesión con el nombre de usuario **root** y la contraseña que especificó al implementar el dispositivo de vRealize Automation de réplica de destino.

Procedimiento

- 1 Seleccione **Configuración de vRA > Clúster**.
- 2 En el cuadro de texto **Nodo de clúster de encabezado**, introduzca el FQDN del dispositivo de vRealize Automation principal de destino.
- 3 Escriba la contraseña raíz en el cuadro de texto **Contraseña**.

4 Haga clic en **Unirse a clúster**.

Continúe aunque aparezcan advertencias de certificado. El sistema reinicia los servicios del clúster.

5 Compruebe que los servicios se están ejecutando.

a En la barra de pestañas superior, haga clic en **Servicios**.

b Haga clic en **Actualizar** para supervisar cómo se van iniciando los servicios.

Habilitar la acción de conexión a la consola remota para consumidores

La acción de consola remota para consumidores es compatible con dispositivos aprovisionados por vSphere en vRealize Automation.

Edite el blueprint después de actualizar la versión y seleccionar la acción **Conectar con la consola remota** en la pestaña **Acción**.

Para obtener más información, consulte el [artículo 2109706 de la Base de conocimientos](#).

Restaurar archivos de tiempo de espera de flujos de trabajo externos

Debe volver a configurar los archivos de tiempo de espera de flujos de trabajo externos de vRealize Automation debido a que el proceso de actualización sobrescribe los archivos xmldb.

Procedimiento

1 Abra los archivos de configuración del flujo de trabajo externo (xmldb) en su sistema desde el siguiente directorio.

```
\\VMware\vcac\Server\ExternalWorkflows\xmldb\.
```

2 Reemplace los archivos xmldb por los archivos a partir de los que ha creado copias de seguridad antes de la migración. Si no tiene archivos de copia de seguridad, vuelva a definir la configuración de tiempo de espera de flujos de trabajo externos.

3 Guarde la configuración.

Comprobar que el servicio de vRealize Orchestrator está disponible

Tras actualizar a la versión más reciente de vRealize Automation, debe comprobar la conexión entre vRealize Automation y vRealize Orchestrator. En ocasiones, después de la actualización es necesario restaurar la conexión.

Requisitos previos

Inicie sesión en la interfaz de configuración de vRealize Orchestrator.

Procedimiento

1 Haga clic en **Validar configuración**.

2 Si se muestra una marca de verificación verde en la sección Autenticación, vaya al paso 5.

- 3 Si no se muestra ninguna marca de verificación verde en la sección Autenticación, realice este proceso para restaurar la conexión a vRealize Orchestrator .
 - a Haga clic en **Inicio**.
 - b Haga clic en **Configurar proveedor de autenticación**.
 - c En el cuadro de texto **Grupo de administración**, seleccione **Cambiar** y elija un nuevo grupo de administración que pueda resolverse correctamente.

El grupo vcoadmins solamente está disponible en el tenant predeterminado vsphere.local. Si utiliza otro tenant para vRealize Orchestrator, entonces deberá seleccionar otro grupo.
 - d Haga clic en **Guardar cambios** y, si se le pide, reinicie el servidor de vRealize Orchestrator.
 - e Haga clic en **Inicio**.
- 4 Repita el paso 1 para confirmar que en la sección Autenticación se muestra una marca de verificación verde.
- 5 Haga clic en **Inicio** y cierre el Centro de control de vRealize Orchestrator.

Reconfigurar un endpoint de infraestructura de vRealize Orchestrator integrado en el entorno de vRealize Automation de destino

Cuando se migra desde un entorno de vRealize Automation 6.2.x, debe actualizar la dirección URL del endpoint de infraestructura que apunta al servidor de vRealize Orchestrator de destino integrado.

Requisitos previos

- La migración a vRealize Automation 7.4 se realiza correctamente.
- Inicie sesión en la consola de vRealize Automation de destino.
 - a Abra la consola de vRealize Automation usando el nombre de dominio completo del dispositivo virtual de destino: `https://vra-va-hostname.domain.name/vcac`.

En un entorno de alta disponibilidad, abra la consola usando el nombre de dominio completo del equilibrador de carga del dispositivo virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Inicie sesión como usuario administrador de laaS.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoints > Endpoints**.
- 2 En la página Endpoints, seleccione el endpoint de vRealize Orchestrator y haga clic en **Editar**.
- 3 En el cuadro de texto Dirección, edite la URL del endpoint de vRealize Orchestrator.
 - Si ha migrado a un entorno mínimo, reemplace la URL del endpoint de vRealize Orchestrator por `https://vra-va-hostname.domain.name:443/vco`.
 - Si ha migrado a un entorno de alta disponibilidad, reemplace la URL del endpoint de vRealize Orchestrator por `https://vra-va-lb-hostname.domain.name:443/vco`.

- 4 Haga clic en **Aceptar**.
- 5 Ejecute manualmente una recopilación de datos en el endpoint de vRealize Orchestrator.
 - a En la página Endpoints, seleccione el endpoint de vRealize Orchestrator.
 - b Seleccione **Acciones > Recopilación de datos**.Compruebe que la recopilación de datos es correcta.

Restaurar cambios para iniciar sesión en el archivo app.config

El proceso de actualización sobrescribe los cambios realizados que se registran en los archivos de configuración. Después de completar una actualización, debe restaurar los cambios realizados en el archivo `app.config` antes de la actualización.

Habilitar la conmutación por error automática de Manager Service después de actualizar

La conmutación por error automática de Manager Service se deshabilita de forma predeterminada cuando vRealize Automation se actualiza.

Siga estos pasos para habilitar la conmutación por error automática de Manager Service después de la actualización.

Procedimiento

- 1 Abra una ventana de símbolo del sistema como usuario raíz en el dispositivo de vRealize Automation.
- 2 Cambie los directorios a `/usr/lib/vcac/tools/vami/commands`.
- 3 Para habilitar la conmutación por error automática de Manager Service, ejecute el siguiente comando.

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

Para deshabilitar la conmutación por error automática en una implementación entera de IaaS, ejecute 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 automáticamente en una copia de seguridad si la instancia principal de Manager Service se detiene.

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 copia de seguridad. La conmutación por error automática de Manager Service se deshabilita de forma predeterminada cuando IaaS se actualiza con el script de actualización de shell o mediante el archivo ejecutable del instalador de IaaS.

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 característica de conmutación por error automática permite que los hosts se supervisen entre sí con transparencia y conmuten por error cuando sea necesario, pero para ello es necesario 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.

Ejecutar la conexión de prueba y comprobar los endpoints actualizados

Al actualizar de vRealize Automation 7.3 o versiones anteriores a la versión 7.4, se modifican los endpoints del entorno de destino.

Después de actualizar a vRealize Automation 7.4, debe utilizar la acción **Probar conexión** para todos los endpoints aplicables. También es posible que tenga que realizar ajustes en algunos de los endpoints actualizados. Para obtener más información, consulte [Consideraciones al trabajar con endpoints actualizados o migrados](#).

La configuración de seguridad predeterminada relativa a endpoints actualizados o migrados consiste en no aceptar certificados que no sean de confianza.

Si usaba certificados que no eran de confianza, después de actualizar o migrar desde una instalación de vRealize Automation anterior, deberá hacer lo siguiente para que todos los endpoints de vSphere y de NSX permitan la validación de certificados. De lo contrario, las operaciones de endpoint generarán errores de certificado. Para obtener más información, consulte los artículos de la base de conocimientos de VMware *La comunicación del endpoint se interrumpe después de actualizar a vRA 7.3 (2150230)* en <http://kb.vmware.com/kb/2150230> y *Cómo descargar e instalar certificados raíz de vCenter Server para evitar advertencias de certificado del navegador web (2108294)* en <http://kb.vmware.com/kb/2108294>.

- 1 Después de la actualización o migración, inicie sesión en la máquina del agente de vSphere de vRealize Automation y reinicie los agentes de vSphere en la pestaña **Servicios**.

Es posible que no todos los agentes se reinicien con la migración, de modo que puede que sea necesario reiniciarlos manualmente.

- 2 Espere a que al menos un informe de ping finalice. Un informe de ping tarda uno o dos minutos en finalizar.
- 3 Cuando los agentes de vSphere hayan empezado a recopilar datos, inicie sesión en vRealize Automation como un administrador de IaaS.
- 4 Haga clic en **Infraestructura > Endpoints > Endpoints**.

- 5 Edite un endpoint de vSphere y haga clic en **Probar conexión**.
- 6 Si aparece un mensaje de certificado, haga clic en **Aceptar** para aceptar el certificado.

Si no aparece un mensaje de certificado, es posible que el certificado esté actualmente almacenado en una entidad raíz de confianza de la máquina de Windows que aloja el servicio del endpoint, por ejemplo, como una máquina de agente de proxy o una máquina de DEM.
- 7 Haga clic en **Aceptar** para confirmar la aceptación de certificado y guardar el endpoint.
- 8 Repita este procedimiento por cada endpoint de vSphere.
- 9 Repita este procedimiento por cada endpoint de NSX.

Si la acción **Probar conexión** finaliza correctamente, pero alguna de las operaciones de aprovisionamiento o de recopilación de datos genera errores, puede instalar el mismo certificado en todas las máquinas de agente que sirvan al endpoint y en todas las máquinas DEM. Si lo prefiere, puede desinstalar el certificado de las máquinas existentes y repetir el procedimiento anterior en el endpoint con el error.

Importar complemento DynamicTypes

Si utiliza el complemento DynamicTypes y ha exportado la configuración como un paquete antes de la actualización, debe importar el siguiente flujo de trabajo:

```
/Library/Dynamic Types/Configuration/Import Configuration From Package
```

El comando `/Library` se ejecuta desde el cliente de Java de vRealize Orchestrator.

Solucionar problemas de actualización de vRealize Automation

En los temas de solución de problemas de actualización se ofrecen soluciones a los problemas que podría encontrar durante la actualización de vRealize Automation 6.2.5 a 7.4.

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.

Error en la actualización para el componente de sitio web de IaaS

Se produce un error en la actualización de IaaS y no es posible continuar.

Problema

Se produce un error en la actualización de IaaS para el componente de sitio web. Los siguientes mensajes de error aparecen en el archivo de log del instalador.

- System.Data.Services.Client.DataServiceQueryException:
An error occurred while processing this request. --->
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- Description: An application error
occurred on the server. The current custom error settings for this application
prevent the details of the application error from being viewed remotely (for
security reasons). It could, however, be viewed by browsers running on the
local server machine.
- Warning: Non-zero return code. Error del comando.
- Done Building Project "C:\Archivos de programa
(x86)\VMware\VMware\Server\Model Manager Data\DeployRepository.xml"
(InstallRepoModel target(s)) -- FAILED.

Los siguientes mensajes de error aparecen en el archivo de log del repositorio.

- [Error]: [sub-thread-Id="20"
context="" token=""] Failed to start repository service. Reason:
System.InvalidOperationException: Configuration section encryptionKey is not
protected
at
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration
config)
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2
decryptFunc)
at
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object
sender, ObjectMaterializedEventArgs e)

```
at
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()
at
System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
at
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(Core
ModelEntities
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String
coreModelConnectionString)
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().
```

Causa

Se produce un error en la actualización de IaaS cuando la fecha de creación del archivo `web.config` es igual o posterior a la fecha modificada.

Solución

- 1 En el host de IaaS, inicie sesión en Windows.
- 2 Abra el símbolo del sistema de Windows.
- 3 Cambie los directorios a la carpeta de instalación de vRealize Automation.
- 4 Inicie su editor de texto preferido con la opción **Ejecutar como administrador**.
- 5 Busque y seleccione el archivo `web.config` y guarde el archivo para cambiar la fecha de modificación del archivo.
- 6 Examine las propiedades del archivo `web.config` para confirmar que la fecha de modificación del archivo es posterior a la fecha de creación.
- 7 Actualice IaaS.

Manager Service no se ejecuta debido a errores de validación de SSL durante el tiempo de ejecución

Manager Service no se ejecuta debido a errores de validación de SSL.

Problema

Manager Service no se ejecuta y muestra el siguiente mensaje en el registro:

```
[Info]: Thread-Id="6" - context="" token="" Error al conectar con la base de datos central; se volverá a intentar en 00:00:05. Detalles del error: La conexión con el servidor se ha establecido correctamente, pero se ha producido un error durante el proceso de inicio de sesión. (Proveedor: proveedor de SSL. Error: 0 - La cadena de certificados la proporciona una entidad que no es de confianza).
```

Causa

Durante el tiempo de ejecución, Manager Service no se ejecuta debido a errores de validación de SSL.

Solución

- 1 Abra el archivo de configuración `ManagerService.config`.
- 2 Actualice `Encrypt=False` en la siguiente línea:

```
<add name="vcac-repository" providerName="System.Data.SqlClient"
connectionString="Data Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated
Security=True;Pooling=True;Max Pool
Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

Error al iniciar sesión tras la actualización

Después de una actualización, debe salir del explorador y volver a iniciar sesión para las sesiones que usan cuentas de usuario sin sincronizar.

Problema

Al iniciar sesión después de actualizar vRealize Automation, el sistema deniega el acceso a las cuentas de usuario no sincronizadas.

Solución

Salga del explorador y vuelva a iniciar vRealize Automation.

Los elementos del catálogo aparecen en el catálogo de servicios después de la actualización, pero no están disponibles para solicitarse

Los elementos del catálogo que utilizan ciertas definiciones de propiedad de versiones anteriores aparecen en el catálogo de servicios, pero no están disponibles para solicitarlos después de actualizar a la última versión de vRealize Automation.

Problema

Si actualizó desde 6.2.x o una versión anterior, y tuvo definiciones de propiedad con los siguientes tipos de control o atributos, los atributos están ausentes en las definiciones de propiedad y cualquier elemento de catálogo que usa las definiciones no funciona del modo en que lo hacía antes de actualizar.

- Tipos de control. Casilla de verificación o vínculo.
- Atributos. Relación, expresiones regulares o diseños de propiedades.

Causa

En vRealize Automation 7.0 y versiones posteriores, las definiciones de propiedad ya no usan los atributos. Debe recrear la definición de propiedades o configurarla para que use una acción de script de vRealize Orchestrator en lugar de los atributos o tipos de control integrados.

Migre el tipo de control o los atributos a vRealize Automation 7.x utilizando una acción de script.

Solución

- 1 En vRealize Orchestrator, cree una acción de script que devuelva los valores de propiedad. La acción debe devolver un tipo simple. (Por ejemplo, devolver cadenas, enteros u otros tipos admitidos). La acción puede tomar las otras propiedades de las que depende como parámetro de entrada.
- 2 En la consola de vRealize Automation, configure la definición de productos.
 - a Seleccione **Administración > Diccionario de propiedades > Definiciones de propiedades**.
 - b Seleccione la definición de propiedades y haga clic en **Editar**.
 - c En el menú desplegable Mostrar recomendación, seleccione **Lista desplegable**.
 - d En el menú desplegable Valores, seleccione **Valores externos**.
 - e Seleccione la acción de script.
 - f Haga clic en **Aceptar**.
 - g Configure los parámetros de entrada que se incluyen en la acción de script. Para preservar la relación existente, enlace el parámetro a la otra propiedad.
 - h Haga clic en **Aceptar**.

Combinación incorrecta de bases de datos externas de PostgreSQL

La combinación de base de datos de PostgreSQL externa con la base de datos de PostgreSQL integrada no se realiza correctamente.

Problema

Si la versión de la base de datos externa de PostgreSQL es posterior a la versión de la base de datos integrada de PostgreSQL, la combinación no podrá realizarse correctamente.

Solución

- 1 Inicie sesión en el host para la base de datos externa de PostgreSQL.
- 2 Ejecute el comando `psql --version`.
Anote la versión de PostgreSQL para la base de datos externa.
- 3 Inicie sesión en el host para la base de datos integrada de PostgreSQL.
- 4 Ejecute el comando `psql --version`.
Anote la versión de PostgreSQL para la base de datos integrada.

Si la versión de PostgreSQL externa es posterior a la versión de PostgreSQL integrada, póngase en contacto con el equipo de soporte técnico y solicite asistencia para combinar su base de datos externa de PostgreSQL.

Parece que el comando Unirse a clúster falla después de actualizar a un entorno de alta disponibilidad

Después de hacer clic en **Unirse a clúster** en la consola de administración en un nodo de clúster secundario, el indicador de progreso desaparece.

Problema

Cuando utiliza la consola de administración del dispositivo de vRealize Automation después de actualizar para unir un nodo de clúster secundario al nodo principal, el indicador de progreso desaparece y no se muestra ningún mensaje de error ni de ejecución correcta. Este comportamiento es un problema intermitente.

Causa

El indicador de progreso desaparece porque algunos navegadores se detienen al esperar una respuesta del servidor. Este comportamiento no detiene el proceso de unión a un clúster. Puede confirmar que el proceso de unión a un clúster se haya realizado correctamente si revisa el archivo de log en `/var/log/vmware/vcac/vcac-config.log`.

La actualización no se realiza correctamente si la partición raíz no proporciona suficiente espacio libre

Si no hay suficiente espacio libre disponible en la partición raíz del host de dispositivo de vRealize Automation, la actualización no se podrá llevar a cabo.

Solución

Con este procedimiento, se aumenta el espacio libre en la partición raíz del disco 1 del host de dispositivo de vRealize Automation. En una implementación distribuida, realice este procedimiento para aumentar el espacio libre en cada nodo de réplica secuencialmente y, después, aumentar el espacio libre en el nodo principal.

Nota Cuando se lleva a cabo este procedimiento, pueden aparecer los siguientes mensajes de advertencia:

- ```
WARNING: Re-reading the partition table failed with error 16:
Device or resource busy. The kernel still uses the old table. The
new table will be used at the next reboot or after you run
partprobe(8) or kpartx(8) Syncing disks.
```
- ```
Error: Partition(s) 1 on /dev/sda have been written, but we have been unable to inform the kernel
of the change, probably because it/they are in use. As a result, the old partition(s) will remain
in use. You should reboot now before making further changes.
```

Ignore el mensaje **Debe reiniciar ahora antes de realizar más cambios**. Si reinicia el sistema antes del paso 10, dañará el proceso de actualización.

Procedimiento

- 1 Encienda la máquina virtual host de dispositivo de vRealize Automation e inicie sesión como si fuera con una conexión de shell segura como usuario raíz.
- 2 Ejecute los siguientes comandos para detener los servicios.
 - a `service vcac-server stop`
 - b `service vco-server stop`
 - c `service vpostgres stop`
- 3 Ejecute el siguiente comando para desmontar la partición swap.


```
swapoff -a
```
- 4 Ejecute el siguiente comando para eliminar las particiones existentes en el disco 1 y crear una partición raíz de 44 GB y una partición swap de 6 GB.


```
(echo d; echo 2; echo d; echo 1; echo n; echo p; echo ; echo ; echo '+44G'; echo n; echo p; echo ; echo ; echo ; echo w; echo p; echo q) | fdisk /dev/sda
```
- 5 Ejecute el siguiente comando para cambiar el tipo de partición swap.


```
(echo t; echo 2; echo 82; echo w; echo p; echo q) | fdisk /dev/sda
```
- 6 Ejecute el siguiente comando para establecer el indicador de arranque del disco 1.


```
(echo a; echo 1; echo w; echo p; echo q) | fdisk /dev/sda
```
- 7 Ejecute el siguiente comando para registrar los cambios realizados en la partición con el kernel de Linux.


```
partprobe
```

Si aparece un mensaje que indica que se debe reiniciar antes de realizar más cambios, ignórelo. Si reinicia el sistema antes del paso 10, dañará el proceso de actualización.
- 8 Ejecute el siguiente comando para dar formato a la nueva partición swap.


```
mkswap /dev/sda2
```
- 9 Ejecute el siguiente comando para montar la partición swap.


```
swapon -a
```
- 10 Reinicie el dispositivo de vRealize Automation.
- 11 Cuando se haya reiniciado el dispositivo, ejecute el siguiente comando para ajustar el tamaño de la tabla de la partición del disco 1.


```
resize2fs /dev/sda1
```
- 12 Para comprobar que la expansión de disco es correcta, ejecute `df -h` y compruebe que el espacio en disco disponible en `/dev/sda1` es superior a 30 GB.

Las copias de seguridad de archivos .xml hacen que el sistema agote el tiempo de espera

vRealize Automation registra todos los archivos con una extensión .xml en el directorio \\VMware\VCAC\Server\ExternalWorkflows\xmlldb\. Si este directorio contiene archivos de copia de seguridad con una extensión .xml, el sistema ejecuta flujos de trabajo duplicados que provocan que el sistema agote el tiempo de espera.

Solución

Solución alternativa: Cuando realice copias de seguridad de archivos en este directorio, traslade las copias de seguridad a otro directorio o cambie la extensión del nombre del archivo de copia de seguridad para que no contenga .xml.

Eliminar nodos huérfanos en vRealize Automation

Un nodo huérfano es un nodo duplicado del que se informa en el host pero que no existe en el host.

Problema

Cuando compruebe que todos los nodos de IaaS y del dispositivo virtual están en buen estado, podría descubrir que algún host tiene uno o varios nodos huérfanos. Debe eliminar todos los nodos huérfanos.

Solución

- 1 En el dispositivo de vRealize Automation principal, inicie sesión en la Administración de dispositivos de vRealize Automation como **raíz** con la contraseña que introdujo al implementar el dispositivo de vRealize Automation.
- 2 Seleccione **Configuración de vRA > Clúster**.
- 3 Haga clic en **Eliminar** en cada uno de los nodos huérfanos de la tabla.

No se puede crear un nuevo directorio en vRealize Automation

Los intentos de agregar un nuevo directorio con el primer conector sincronizado no son correctos.

Problema

El problema se debe a un archivo config-state.json incorrecto ubicado en `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`.

Para obtener más información sobre cómo solucionar el problema, consulte el artículo [2145438 de la Base de conocimientos](#)

En algunas máquinas virtuales, no se crea una implementación durante la actualización

Para las máquinas virtuales con el estado ausente en el momento de la actualización no se crea una implementación correspondiente en el entorno de destino.

Problema

Si una máquina virtual tiene el estado ausente en el entorno de origen durante la actualización, no se creará una implementación correspondiente en el entorno de destino. Si una máquina virtual sale del estado ausente después de la actualización, se podrá importar la máquina a la implementación de destino mediante la importación en bloque.

Error de certificado que no es de confianza

Al consultar la página Visor de logs de la infraestructura en la consola de Dispositivo de vRealize Automation, puede que vea un informe de error de conexión de endpoint que indique: `Certificate is not trusted`.

Problema

En la consola de Dispositivo de vRealize Automation, seleccione **Infraestructura > Supervisión > Log**. En la página Visor de logs, puede que vea un informe similar al siguiente:

Ha fallado la conexión con el endpoint. Para validar que se puede establecer una conexión segura con este endpoint, vaya al endpoint de vSphere en la página Endpoints y haga clic en el botón Probar conexión.

Excepción interna: El certificado no es de confianza (RemoteCertificateChainErrors). Subject: C=US, CN=vc6.mycompany.com Thumbprint: DC5A8816231698F4C9013C42692B0AF93D7E35F1

Causa

Al actualizar vRealize Automation 7.3 o versiones anteriores a la versión 7.4, se modifican los endpoints del entorno original. En los entornos actualizados recientemente a vRealize Automation 7.4, el administrador de IaaS debe revisar cada uno de los endpoints existentes que utilizan una conexión https segura. Si un endpoint presenta un error `Certificate is not trusted`, quiere decir que no funciona correctamente.

Solución

- 1 Inicie sesión en la consola de vRealize Automation como administrador de la infraestructura.
- 2 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 3 Siga estos pasos con cada endpoint que tenga una conexión segura.
 - a Haga clic en **Editar**.
 - b Haga clic en **Probar conexión**.
 - c Revise los detalles del certificado y haga clic en **Aceptar** si confía en él.
 - d Reinicie los servicios de Windows para todos los agentes de proxy de IaaS que usa este endpoint.
- 4 Compruebe que ya no aparecen más errores `Certificate is not trusted` en la página Visor de logs de la infraestructura.

Error al instalar o actualizar vRealize Automation

Al instalar o actualizar vRealize Automation, se produce un error y aparece un mensaje en el archivo de log.

Problema

Al instalar o actualizar vRealize Automation, se produce un error en el procedimiento. Por lo general, esto sucede cuando una corrección que se ha aplicado durante la instalación o la actualización no es correcta. Aparece un mensaje de error en el archivo de log similar al siguiente: Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.

Causa

El entorno de Windows tiene una política de grupo para la ejecución del script de PowerShell establecida en Habilitado.

Solución

- 1 En la máquina host de Windows, ejecute `gpedit.msc` para abrir el Editor de políticas de grupo local.
- 2 En el panel izquierdo, en la **configuración del equipo**, haga clic en el botón para expandir, de manera que se abra **Plantillas administrativas > Componentes de Windows > Windows PowerShell**.
- 3 Para **Activar la ejecución de scripts**, cambie el estado de Enabled a Not Configured.

La actualización no puede actualizar al agente de administración

Aparece un mensaje de error sobre el agente de administración cuando hace clic en **Instalar actualizaciones** en la página Estado de actualización de la consola de administración de Dispositivo de vRealize Automation.

Problema

El proceso de actualización no se realiza correctamente. Aparece el mensaje: No es posible actualizar el agente de administración en el nodo x. A veces, el mensaje muestra más de un nodo.

Causa

Este problema puede deberse a múltiples condiciones. El mensaje de error solo identifica el ID de nodo de la máquina afectada. Encontrará más información en el archivo `ALL.log` del agente de administración en la máquina donde el comando no se ejecuta correctamente.

Realice estas tareas en los nodos afectados según su situación:

Solución

- Si no se está ejecutando el servicio del agente de administración, inicie el servicio y reinicie la actualización en el dispositivo virtual.

- Si se está ejecutando el servicio del agente de administración y se actualiza el agente de administración, reinicie la actualización en el dispositivo virtual.
- Si se está ejecutando el servicio del agente de administración, pero no se actualiza el agente de administración, realice una actualización manual.
 - a Abra un navegador y vaya a la página de instalación de IaaS de vRealize Automation en el dispositivo vRealize Automation en `https:// va-hostname.domain.name:5480/install`.
 - b Descargue y ejecute el instalador del agente de administración.
 - c Reinicie el equipo del agente de administración.
 - d Reinicie la actualización en el dispositivo virtual.

La actualización del agente de administración no se realiza correctamente

La actualización del agente de administración no se realiza correctamente si se hace de vRealize Automation a la versión 7.2. o 7.3.x.

Problema

Si un incidente de conmutación por error ha intercambiado el host del agente de administración principal y secundario, la actualización no se realizará correctamente porque el proceso de actualización automatizado no puede encontrar el host esperado. Realice este procedimiento en cada nodo de IaaS en el que el agente de administración no esté actualizado.

Solución

- 1 Abra All.log en la carpeta de logs del agente de administración, situada en C:\Archivos de programa (x86)\VMware\vCAC\Management Agent\Logos\.

La ubicación de la carpeta de instalación podría ser diferente a la ubicación predeterminada.

- 2 Busque en el archivo de log un mensaje sobre un dispositivo virtual apagado u obsoleto.

Por ejemplo, EXCEPCIÓN INTERNA: System.Net.WebException: No es posible conectar con el servidor remoto ---> System.Net.Sockets.SocketException: Se produjo un error durante el intento de conexión ya que la parte conectada no respondió adecuadamente tras un periodo de tiempo, o bien se produjo un error en la conexión establecida ya que el host conectado no ha podido responder.

Dirección_IP:5480

- 3 Edite el archivo de configuración del agente de administración en C:\Archivos de programa (x86)\VMware\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config para reemplazar el valor `alternativeEndpointaddress` existente con la URL del endpoint del dispositivo virtual principal.

La ubicación de la carpeta de instalación podría ser diferente a la ubicación predeterminada.

Ejemplo de `alternativeEndpointaddress` en `VMware.IaaS.Management.Agent.exe.config`.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="número de miniatura" />
```

- 4 Reinicie el servicio Windows del agente de administración y compruebe el archivo All.log para verificar que esté trabajando.
- 5 Ejecute el procedimiento de actualización en el dispositivo de vRealize Automation principal.

Se produce un error de actualización de vRealize Automation debido a la configuración de tiempo de espera predeterminada

Si la configuración predeterminada de sincronización de bases de datos es demasiado limitada para el entorno, puede aumentar el ajuste de tiempo de actualización.

Problema

La configuración de tiempo de espera para el comando SynchronizeDatabases de Vcac-Config no es suficiente para algunos entornos en los que la sincronización de las bases de datos toma más que el valor predeterminado (3.600 segundos).

Los valores de propiedad cafeTimeoutInSeconds y cafeRequestPageSize del archivo Vcac-Config.exe.config rigen la comunicación entre la API y la herramienta de utilidad Vcac-config.exe. El archivo se encuentra en *Ubicación de instalación de IaaS\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config*.

Puede proporcionar un valor para estos parámetros opcionales para reemplazar el valor de tiempo de espera predeterminado de únicamente el comando SynchronizeDatabases.

| Parámetro | Nombre corto | Descripción |
|------------------------|--------------|--|
| --DatabaseSyncTimeout | -dstm | Establece el valor de tiempo de espera de solicitud HTTP en segundos solo para SynchronizeDatabases. |
| --DatabaseSyncPageSize | -dsps | Establece el tamaño de página de solicitud de sincronización solo para la sincronización de la reserva o de la política de reserva. El valor predeterminado es 10. |

Si no se establecen estos parámetros en el archivo Vcac-Config.exe.config, el sistema utiliza el valor de tiempo de espera predeterminado.

Error al actualizar IaaS en un entorno de alta disponibilidad

Se produce un error al ejecutar el proceso de actualización de IaaS en el nodo del servidor web principal con el equilibrio de carga habilitado. Es posible que aparezcan los siguientes mensajes de error: "System.Net.WebException: se agotó el tiempo de espera de la operación" o "401 - No autorizado: acceso denegado debido a credenciales no válidas".

Problema

Al actualizar IaaS con el equilibrio de carga habilitado, se puede producir un error intermitente. Cuando esto sucede, debe deshabilitar el equilibrio de carga y volver a ejecutar la actualización de vRealize Automation.

Solución

- 1 Revierta el entorno a los snapshots anteriores a la actualización.
- 2 Abra una conexión de escritorio remoto con el nodo del servidor web de IaaS principal.
- 3 Desplácese hasta el archivo de hosts de Windows en C:\windows\system32\drivers\etc.
- 4 Abra el archivo de hosts y añada esta línea para omitir el equilibrador de carga del servidor web.

dirección_IP_de_nodo_de_sitio_web_iaas_principal
FQDN_de_lb_de_sitio_web_iaas_de_vrealizeautomation

Ejemplo:

10.10.10.5 vra-iaas-web-lb.domain.com

- 5 Guarde el archivo de hosts y vuelva a intentar la actualización de vRealize Automation.
- 6 Cuando finalice la actualización de vRealize Automation, abra el archivo de hosts y quite la línea que añadió en el paso 4.

Solucionar problemas de actualización

Puede modificar el proceso de actualización para solucionar problemas de actualización.

Solución

Cuando experimente problemas al actualizar el entorno de vRealize Automation, utilice este procedimiento para modificar el proceso de actualización y seleccione una de las marcas disponibles.

Procedimiento

- 1 Abra una conexión de Secure Shell con el nodo del dispositivo de vRealize Automation principal.
- 2 En el símbolo del sistema, ejecute este comando para crear el archivo de alternancia:

touch available_flag

Por ejemplo: **touch /tmp/disable-iaas-upgrade**

Tabla 1-72. Marcas disponibles

| Marca | Descripción |
|---------------------------|--|
| /tmp/disable-iaas-upgrade | <ul style="list-style-type: none"> ■ Impide el proceso de actualización de IaaS después de que se reinicia el dispositivo virtual. ■ Impide la actualización del agente de administración. ■ Impide las correcciones y comprobaciones de requisitos previos automáticas. ■ Impide la detención de los servicios de IaaS. |
| /tmp/do-not-upgrade-ma | Impide la actualización del agente de administración. Esta marca es adecuada cuando se actualiza el agente de administración de forma manual. |

Tabla 1-72. Marcas disponibles (Continuación)

| Marca | Descripción |
|-----------------------------|---|
| /tmp/skip-prereq-checks | Impide las correcciones y comprobaciones de requisitos previos automáticas. Esta marca es adecuada cuando hay un problema con las correcciones automáticas de requisitos previos y, en su lugar, las correcciones se han aplicado manualmente. |
| /tmp/do-not-stop-services | Impide la detención de los servicios de IaaS. La actualización no detiene los servicios de IaaS de Windows, como Manager Service, DEM y los agentes. |
| /tmp/do-not-upgrade-servers | Impide la actualización automática de todos los componentes de IaaS de servidor, como la base de datos, el sitio web, la WAPI, el repositorio, los datos de Model Mfrontanager y Manager Service. Nota Esta marca también impide la habilitación del modo de conmutación por error automático de Manager Service. |
| /tmp/do-not-upgrade-dems | Impide la actualización de DEM. |
| /tmp/do-not-upgrade-agents | Impide la actualización del agente de proxy de IaaS. |

3 Complete las tareas para la marca elegida.

Tabla 1-73. Tareas adicionales

| Marca | Tareas |
|---------------------------|--|
| /tmp/disable-iaas-upgrade | <ul style="list-style-type: none"> ■ Actualice manualmente el agente de administración. ■ Aplique los requisitos previos de IaaS manualmente. ■ Detenga los servicios de IaaS de forma manual. <ol style="list-style-type: none"> a Inicie sesión en el servidor de Windows de IaaS. b Seleccione Inicio > Herramientas administrativas > Servicios. c Detenga los servicios en el siguiente orden. Nota No desconecte el servidor de Windows de IaaS. <ol style="list-style-type: none"> a Cada agente de proxy de VMware vRealize Automation. b Todos los trabajos de DEM de VMware. c El orquestador de DEM de VMware. d El servicio de VMware vCloud Automation Center. ■ Inicie la actualización de IaaS manualmente una vez completada la actualización del dispositivo virtual. |
| /tmp/do-not-upgrade-ma | Actualice manualmente el agente de administración. |
| /tmp/skip-prereq-checks | Aplique los requisitos previos de IaaS manualmente. |

Tabla 1-73. Tareas adicionales (Continuación)

| Marca | Tareas |
|-----------------------------|--|
| /tmp/do-not-stop-services | <p>Detenga los servicios de IaaS de forma manual.</p> <ol style="list-style-type: none"> 1 Inicie sesión en el servidor de Windows de IaaS. 2 Seleccione Inicio > Herramientas administrativas > Servicios. 3 Detenga los servicios en el siguiente orden. <p>Nota No desconecte el servidor de Windows de IaaS.</p> <ol style="list-style-type: none"> a Cada agente de proxy de VMware vRealize Automation. b Todos los trabajos de DEM de VMware. c El orquestador de DEM de VMware. d El servicio de VMware vCloud Automation Center. |
| /tmp/do-not-upgrade-servers | |
| /tmp/do-not-upgrade-dems | |
| /tmp/do-not-upgrade-agents | |

- 4 Acceda a la consola de administración del dispositivo de vRealize Automation principal y actualice el dispositivo de vRealize Automation principal.

Nota Debido a que cada marca permanece activa hasta que se la quita, ejecute este comando para quitar la marca elegida después de la actualización: `rm /flag_path/flag_name`. Por ejemplo, `rm /tmp/disable-iaas-upgrade`.

Migrar a vRealize Automation 7.4

Puede realizar una actualización en paralelo del entorno actual de vRealize Automation a la última versión mediante la migración.

Esta información es específica para actualizar vRealize Automation a 7.4 mediante una migración. Para obtener información sobre otras rutas de actualización compatibles, consulte [Actualizar vRealize Automation](#).

Migración de vRealize Automation

Puede realizar una actualización en paralelo del entorno actual de vRealize Automation mediante la migración.

La migración mueve todos los datos (excepto los tenants y los almacenes de identidades) desde el entorno de origen de vRealize Automation actual a una implementación de destino de la versión más reciente de vRealize Automation. Además, la migración mueve todos los datos de la instancia integrada de vRealize Orchestrator 7.x a la implementación de destino.

La migración no cambia el entorno de origen, salvo para detener los servicios de vRealize Automation durante el tiempo necesario para recopilar y copiar los datos de forma segura en el entorno de destino. Según cuál sea el tamaño de la base de datos de vRealize Automation de origen, la migración puede tardar unos minutos u horas.

Puede migrar el entorno de origen a una implementación mínima o a una de alta disponibilidad.

Si tiene previsto que el entorno de destino sea de producción después de la migración, no ponga el entorno de origen en funcionamiento. Los cambios que tengan lugar en el entorno de origen después de la migración no se sincronizarán con el entorno de destino.

Si el entorno de origen está integrado con vCloud Air, vCloud Director o tiene endpoints físicos, debe usar la migración para realizar una actualización. La migración elimina estos endpoints y todos los elementos asociados a ellos en el entorno de destino. Con la migración también se elimina una integración de VMware vRealize Application Services 6.x del entorno de destino.

Nota Debe completar las tareas adicionales para preparar las máquinas virtuales de vRealize Automation antes de la migración. Antes de migrar, revise el artículo [51531](#) de la base de conocimientos.

Si migra desde vRealize Automation 6.2.x a la versión más reciente, es posible que experimente estos problemas.

| Problema | Resolución |
|--|---|
| <p>Después de migrar de vRealize Automation 6.2.x a la versión más reciente, los elementos de catálogo que utilizan estas definiciones de propiedad aparecen en el catálogo de servicios pero no están disponibles para solicitarlos.</p> <ul style="list-style-type: none"> ■ Tipos de control: casilla de verificación o vínculo. ■ Atributos: relación, expresiones regulares o diseños de propiedades. <p>En vRealize Automation 7.x, las definiciones de propiedad ya no utilizan estos elementos.</p> | <p>Debe recrear la definición de propiedades o configurarla para que use una acción de script de vRealize Orchestrator en lugar de los atributos o tipos de control integrados. Para obtener más información, consulte Los elementos del catálogo aparecen en el catálogo de servicios después de la migración, pero no están disponibles para solicitarse.</p> |
| <p>En 7.x no se admiten las expresiones regulares que se utilizan para definir las relaciones entre elementos principales y secundarios en un menú desplegable de vRealize Automation 6.2.x. En la versión 6.2.x, puede utilizar expresiones regulares para definir uno o varios elementos de menú secundario que solo están disponibles para un elemento de menú principal determinado. Cuando se selecciona el elemento de menú principal, solo aparecen esos elementos de menú secundario.</p> <p>Tras la migración a la versión 7.x, en el menú desplegable secundario aparecen todos los elementos de menú disponibles, independientemente de la opción seleccionada en el menú desplegable principal. Para mostrar que los valores dinámicos definidos previamente ya no funcionan, en el primer elemento del menú desplegable secundario, se indica "Advertencia: Use flujos de trabajo de vRO para definir valores dinámicos".</p> | <p>Tras la migración, debe recrear la definición de propiedades para restaurar los valores dinámicos anteriores. Para obtener información sobre cómo crear una relación principal-secundaria entre los menús desplegables principales y secundarios, consulte la publicación correspondiente a cómo usar definiciones de propiedades dinámicas en vRA 7.2.</p> |

Interfaces de usuario del entorno de vRealize Automation

El entorno de vRealize Automation se utiliza y administra con varias interfaces.

Interfaces de usuario

En estas tablas se describen las interfaces que se usan para administrar el entorno de vRealize Automation.

Tabla 1-74. Consola de administración de vRealize Automation

| Propósito | Acceso | Credenciales necesarias |
|---|--|---|
| <p>La consola de vRealize Automation se emplea para las siguientes tareas de administrador del sistema.</p> <ul style="list-style-type: none"> ■ Agregar tenants. ■ Personalizar la interfaz de usuario de vRealize Automation. ■ Configurar los servidores de correo electrónico. ■ Ver logs de eventos. ■ Configure vRealize Orchestrator. | <p>1 Inicie un navegador y abra la página de presentación del dispositivo de vRealize Automation con el nombre de dominio completo del dispositivo virtual:</p> <p><code>https://vra-va-hostname.domain.name.</code></p> <p>2 Haga clic en Consola de vRealize Automation.</p> <p>También puede utilizar la siguiente dirección URL para abrir la consola de vRealize Automation: <code>https://vra-va-hostname.domain.name/vcac</code></p> <p>3 Inicie sesión.</p> | <p>Debe ser un usuario con la función de administrador del sistema.</p> |

Tabla 1-75. Consola de tenant de vRealize Automation . Esta es la interfaz de usuario principal que se utiliza para crear y administrar servicios y recursos.

| Propósito | Acceso | Credenciales necesarias |
|---|---|---|
| <p>vRealize Automation se usa para las siguientes tareas.</p> <ul style="list-style-type: none"> ■ Solicitar nuevos blueprints de servicio de TI. ■ Crear y administrar recursos de TI y de nube. ■ Crear y administrar grupos personalizados. ■ Cree y administre grupos empresariales. ■ Asignar funciones a los usuarios. | <p>1 Inicie un navegador e introduzca la dirección URL de los tenants con el nombre de dominio completo del dispositivo virtual y el nombre de la URL de tenant:</p> <p><code>https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name .</code></p> <p>2 Inicie sesión.</p> | <p>Debe ser un usuario con una o varias de las siguientes funciones:</p> <ul style="list-style-type: none"> ■ Arquitecto de aplicaciones ■ Administrador de aprobaciones ■ Administrador del catálogo ■ Administrador de contenedores ■ Arquitecto de contenedores ■ Consumidor de estado ■ Arquitecto de infraestructura ■ Consumidor de exportación segura ■ Arquitecto de software ■ Administrador de tenants ■ Arquitecto XaaS |

Tabla 1-76. Administración de dispositivos de vRealize Automation . Esta interfaz a veces se denomina interfaz de administración de dispositivos virtuales (Virtual Appliance Management Interface, VAMI).

| Propósito | Acceso | Credenciales necesarias |
|---|--|--|
| <p>La administración de dispositivos de vRealize Automation se usa para las siguientes tareas:</p> <ul style="list-style-type: none"> ■ Ver el estado de los servicios registrados. ■ Ver información del sistema y reiniciar o apagar el dispositivo. ■ Administrar la participación en el programa de mejora de la experiencia del cliente. ■ Ver el estado de la red. ■ Ver el estado de actualización e instalar actualizaciones. ■ Administrar la configuración de administración. ■ Administrar la configuración del host de vRealize Automation. ■ Administrar la configuración de SSO. ■ Administrar las licencias del producto. ■ Configurar la base de datos de Postgres de vRealize Automation. ■ Configurar la mensajería de vRealize Automation. ■ Configure el registro de vRealize Automation. ■ Instalar componentes de IaaS. ■ Migrar desde una instalación de vRealize Automation existente. ■ Administrar certificados de componentes de IaaS. ■ Configurar el servicio Xenon. | <ol style="list-style-type: none"> 1 Inicie un navegador y abra la página de presentación del dispositivo de vRealize Automation con el nombre de dominio completo del dispositivo virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Haga clic en Administración de dispositivos de vRealize Automation. También puede utilizar la siguiente dirección URL para abrir la administración de dispositivos de vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Inicie sesión. | <ul style="list-style-type: none"> ■ Nombre de usuario: raíz. ■ Contraseña: la contraseña que ha introducido al implementar el dispositivo de vRealize Automation. |

Tabla 1-77. Cliente de vRealize Orchestrator

| Propósito | Acceso | Credenciales necesarias |
|--|---|---|
| <p>El cliente de vRealize Orchestrator se usa para realizar las siguientes tareas:</p> <ul style="list-style-type: none"> ■ Desarrollar acciones. ■ Desarrollar flujos de trabajo. ■ Administrar políticas. ■ Instalar paquetes. ■ Administrar permisos de usuarios y de grupos de usuarios. ■ Asociar etiquetas a objetos de URI. ■ Ver el inventario. | <ol style="list-style-type: none"> 1 Inicie un navegador y abra la página de presentación de vRealize Automation con el nombre de dominio completo del dispositivo virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Para descargar el archivo <code>client.jnlp</code> en el equipo local, haga clic en Cliente de vRealize Orchestrator. 3 Haga clic con el botón derecho en el archivo <code>client.jnlp</code> y seleccione Iniciar. 4 En el cuadro de diálogo <i>¿Desea continuar?</i>, haga clic en Continuar. 5 Inicie sesión. | <p>Debe ser un usuario con la función de administrador del sistema o miembro del grupo <code>vcoadmins</code> configurado en los ajustes del proveedor de autenticación del centro de control de vRealize Orchestrator.</p> |

Tabla 1-78. Centro de control de vRealize Orchestrator

| Propósito | Acceso | Credenciales necesarias |
|--|---|--|
| <p>El centro de control de vRealize Orchestrator se emplea para editar la configuración de la instancia de vRealize Orchestrator predeterminada que está integrada en vRealize Automation.</p> | <ol style="list-style-type: none"> 1 Inicie un navegador y abra la página de presentación del dispositivo de vRealize Automation con el nombre de dominio completo del dispositivo virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Haga clic en Administración de dispositivos de vRealize Automation. También puede utilizar la siguiente dirección URL para abrir la administración de dispositivos de vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Inicie sesión. 4 Haga clic en Configuración de vRA > Orchestrator. 5 Seleccione la interfaz de usuario de Orchestrator. 6 Haga clic en Iniciar. 7 Haga clic en la URL de interfaz de usuario de Orchestrator. 8 Inicie sesión. | <p>Nombre de usuario</p> <ul style="list-style-type: none"> ■ Introduzca root (raíz) si no se configuró la autenticación basada en funciones. ■ Introduzca su nombre de usuario de vRealize Automation si está configurado para la autenticación basada en funciones. <p>Contraseña</p> <ul style="list-style-type: none"> ■ Escriba la contraseña que introdujo al implementar el dispositivo vRealize Automation si no se configuró la autenticación basada en funciones. ■ Introduzca la contraseña de su nombre de usuario si está configurado para la autenticación basada en funciones. |

Tabla 1-79. Símbolo del sistema de Linux

| Propósito | Acceso | Credenciales necesarias |
|---|--|---|
| <p>El símbolo del sistema de Linux se utiliza en un host, como el host del dispositivo de vRealize Automation, para realizar las siguientes tareas.</p> <ul style="list-style-type: none"> ■ Detener o iniciar servicios. ■ Editar archivos de configuración. ■ Ejecutar comandos. ■ Recuperar datos. | <p>1 En el host del dispositivo de vRealize Automation, abra un símbolo del sistema.</p> <p>Una forma de abrir el símbolo del sistema en el equipo local consiste en iniciar una sesión en el host mediante una aplicación como PuTTY.</p> <p>2 Inicie sesión.</p> | <ul style="list-style-type: none"> ■ Nombre de usuario: raíz. ■ Contraseña: la contraseña que ha creado al implementar el dispositivo de vRealize Automation. |

Tabla 1-80. Símbolo del sistema de Windows

| Propósito | Acceso | Credenciales necesarias |
|---|---|--|
| <p>Se puede utilizar un símbolo del sistema de Windows en un host, como el host de IaaS, para ejecutar scripts.</p> | <p>1 En el host de IaaS, inicie sesión en Windows.</p> <p>Una forma de iniciar sesión desde el equipo local consiste en iniciar una sesión de escritorio remoto.</p> <p>2 Abra el símbolo del sistema de Windows.</p> <p>Una forma de abrir el símbolo del sistema consiste en hacer clic con el botón derecho en el icono Inicio en el host y seleccionar Símbolo del sistema o Símbolo del sistema (administrador).</p> | <ul style="list-style-type: none"> ■ Nombre de usuario: usuario con privilegios administrativos. ■ Contraseña: contraseña del usuario. |

Requisitos previos de la migración

Los requisitos previos de migración varían según el entorno de destino.

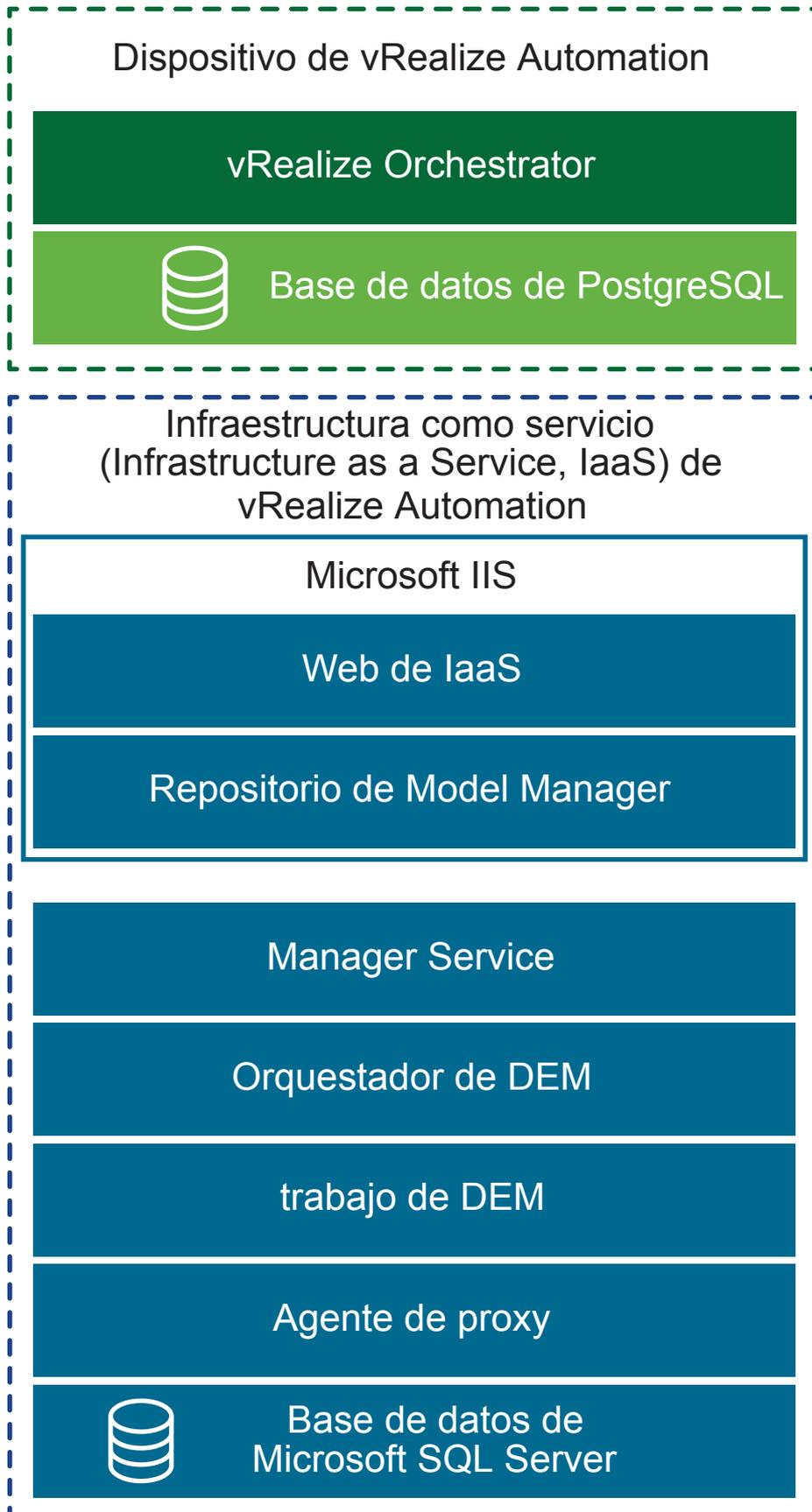
La migración se puede realizar a un entorno mínimo o a un entorno de alta disponibilidad.

Requisitos previos para la migración a un entorno mínimo

Revise estos requisitos previos para asegurarse de que la migración a un entorno mínimo se realiza correctamente.

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 1-17. Implementación mínima de vRealize Automation



Requisitos previos

- Compruebe que dispone de un nuevo entorno de vRealize Automation de destino.
- Instale los agentes de proxy correspondientes en el entorno de destino según estos requisitos.
 - El nombre de agente de proxy de destino debe coincidir con el nombre de agente de proxy de origen de los agentes de proxy de prueba, vSphere, Hyper-V y Citrix XenServer.

Nota Finalice estos pasos para obtener un nombre de agente.

- 1 En el host de IaaS, inicie sesión en Windows como usuario local con privilegios de **administrador**.
- 2 Utilice el Explorador de Windows para ir al directorio de instalación del agente.
- 3 Abra el archivo `VRMAgent.exe.config`.
- 4 Busque el valor del atributo `agentName` en la etiqueta `serviceConfiguration`.

-
- Revise el artículo [51531](#) de la base de conocimientos.
 - El nombre de endpoint de agente de proxy de destino debe coincidir con el nombre de endpoint de agente de proxy de origen de los agentes de proxy de prueba, vSphere, Hyper-V y Citrix XenServer.
 - No cree un endpoint para los agentes de proxy de prueba, vSphere, Hyper-V o Citrix XenServer en el entorno de destino.
 - Revise los números de versión de los componentes de vRealize Automation en el dispositivo de vRealize Automation de destino.
 - a Inicie sesión en la administración de dispositivos de vRealize Automation de destino como **raíz** con la contraseña que ha introducido al implementar el dispositivo de vRealize Automation de destino.
 - b Seleccione **Configuración de vRA > Clúster**.
 - c Expanda los registros Nombre de host/nodo haciendo clic en el triángulo correspondiente.

Compruebe que los números de versión de los componentes de IaaS de vRealize Automation son el mismo.
 - Compruebe que la versión de destino de Microsoft SQL Server de la base de datos de IaaS de vRealize Automation de destino es 2012, 2014 o 2016.
 - Compruebe que el puerto 22 entre los entornos de vRealize Automation de origen y de destino está abierto. Se necesita el puerto 22 para establecer conexiones de Secure Shell (SSH) entre los dispositivos virtuales de origen y de destino.
 - Compruebe que el endpoint de vCenter tenga recursos suficientes para completar la migración.
 - Compruebe que la hora del sistema del entorno de destino de vRealize Automation esté sincronizada entre los componentes de IaaS y Cafe.

- Compruebe que el nodo de servidor de IaaS en el entorno de destino tenga instalado como mínimo Java SE Runtime Environment (JRE) 8, actualización 161 o posterior, de 64 bits. Después de instalar JRE, asegúrese de que la variable de entorno JAVA_HOME apunte a la versión de Java que instaló en cada nodo de IaaS. Revise la ruta de acceso si es necesario.
- Compruebe que cada nodo de IaaS tiene instalado PowerShell 3.0 o una versión posterior.
- Compruebe que los entornos de origen y de destino de vRealize Automation están en ejecución.
- Confirme que no hay ninguna actividad de usuario ni de aprovisionamiento en curso en el entorno de vRealize Automation de origen.
- Compruebe que cualquier software antivirus o de seguridad que se ejecute en nodos de IaaS en el entorno de vRealize Automation de destino que pueda interactuar con el sistema operativo y sus componentes esté correctamente configurado o deshabilitado.
- Verifique que el servicio web de IaaS y Model Manager no deban reiniciarse debido a que hay actualizaciones de instalación de Windows pendientes. Las actualizaciones pendientes podrían impedir que la migración comience o finalice el servicio de publicación World Wide Web.

Pasos siguientes

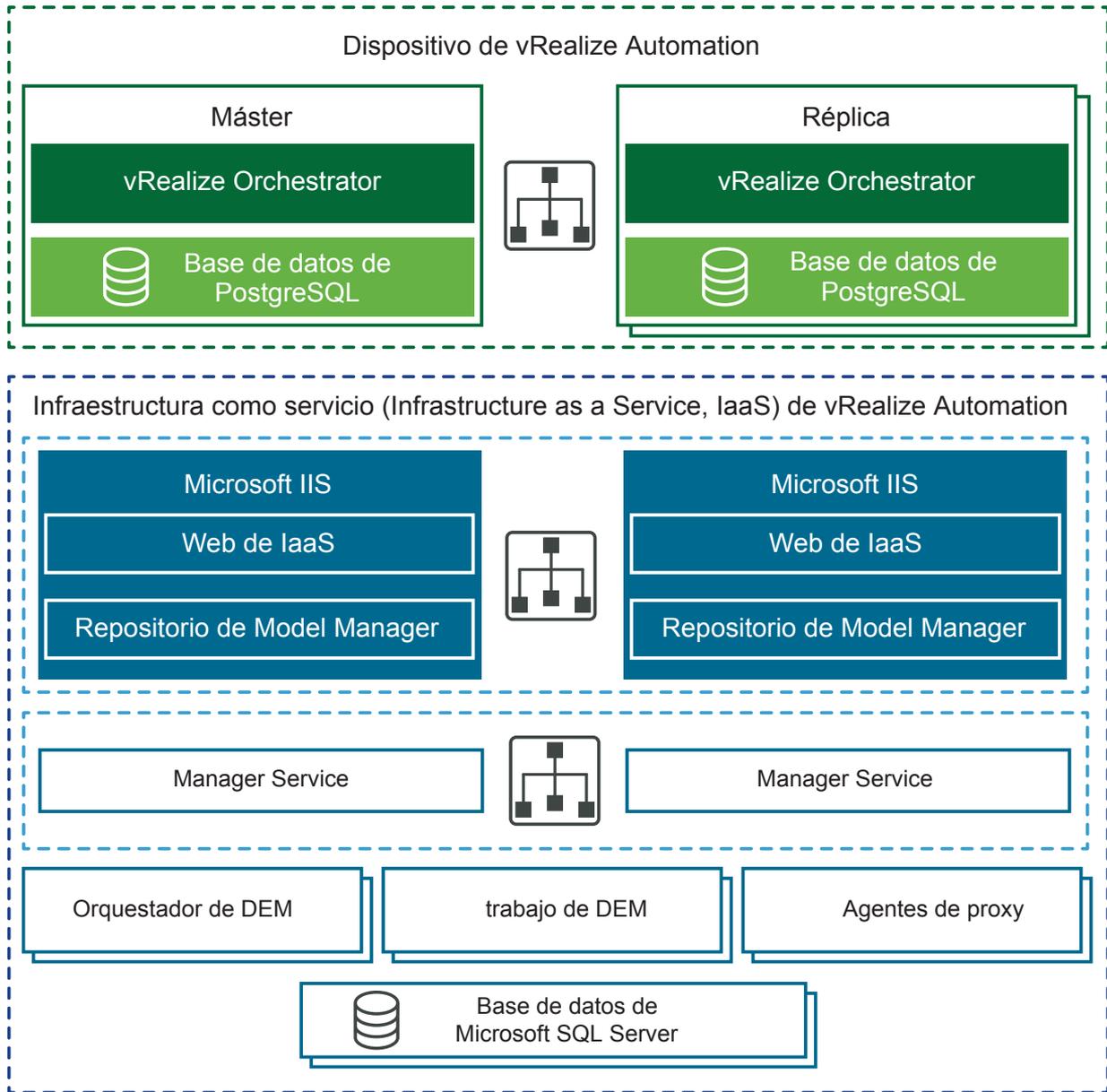
[Tareas previas a la migración.](#)

Requisitos previos para la migración a un entorno de alta disponibilidad

Revise estos requisitos previos para asegurarse de que la migración a un entorno de alta disponibilidad se realiza correctamente.

Los entornos de alta disponibilidad pueden tener distintos tamaños. Una implementación distribuida básica podría mejorar vRealize Automation con solo alojar componentes de IaaS en servidores de Windows independientes. Muchos entornos de alta disponibilidad van incluso más allá y hacen uso de dispositivos redundantes, servidores redundantes y equilibrio de carga para obtener aún más capacidad. Las implementaciones grandes distribuidas proporcionan un mejor escalabilidad, alta disponibilidad y recuperación ante desastres.

Figura 1-18. Entorno de alta disponibilidad de vRealize Automation



Requisitos previos

- Compruebe que hay una nueva instalación de destino de vRealize Automation con un dispositivo virtual principal y uno de réplica configurados para alta disponibilidad. Consulte [Consideraciones sobre la configuración de alta disponibilidad de vRealize Automation](#).
- Compruebe que todos los dispositivos virtuales de vRealize Automation usan la misma contraseña de usuario raíz.
- Instale los agentes de proxy correspondientes en el entorno de destino según estos requisitos.
 - El nombre de agente de proxy de destino debe coincidir con el nombre de agente de proxy de origen de los agentes de proxy de prueba, vSphere, Hyper-V y Citrix XenServer.

Nota Finalice estos pasos para obtener un nombre de agente.

- 1 En el host de IaaS, inicie sesión en Windows como usuario local con privilegios de **administrador**.
 - 2 Utilice el Explorador de Windows para ir al directorio de instalación del agente.
 - 3 Abra el archivo `VRMAgent.exe.config`.
 - 4 Busque el valor del atributo `agentName` en la etiqueta `serviceConfiguration`.
-
- El nombre de endpoint de agente de proxy de destino debe coincidir con el nombre de endpoint de agente de proxy de origen de los agentes de proxy de prueba, vSphere, Hyper-V y Citrix XenServer.
 - No cree un endpoint para los agentes de proxy de prueba, vSphere, Hyper-V o Citrix XenServer en el entorno de destino.
- Compruebe los números de versión de los componentes de vRealize Automation en el dispositivo de vRealize Automation de destino.
 - a En el entorno de destino de vRealize Automation, inicie un navegador y vaya a la consola de administración del dispositivo de vRealize Automation en `https://vra-va-hostname.domain.name:5480`.
 - b Inicie sesión con el nombre de usuario raíz y la contraseña que ha especificado al implementar el dispositivo.
 - c Seleccione **Configuración de vRA > Clúster**.
 - d Para expandir los registros Nombre de host/nodo y que se vean los componentes, haga clic en el botón Expandir.

Compruebe que los números de versión de los componentes de vRealize Automation son el mismo en todos los nodos del dispositivo virtual.

Compruebe que los números de versión de los componentes de IaaS de vRealize Automation son el mismo en todos los nodos de IaaS.
 - Revise el artículo [51531](#) de la base de conocimientos.

- Realice estos pasos para dirigir el tráfico al nodo principal únicamente.
 - a Deshabilite todos los nodos redundantes.
 - b Quite los supervisores de estado de estos elementos según lo que se describe en la documentación del equilibrador de carga:
 - Dispositivo virtual de vRealize Automation
 - Sitio web de IaaS
 - IaaS Manager Service
- Compruebe que la versión de destino de Microsoft SQL Server de la base de datos de IaaS de vRealize Automation de destino es 2012, 2014 o 2016.
- Compruebe que el puerto 22 entre los entornos de vRealize Automation de origen y de destino está abierto. Se necesita el puerto 22 para establecer conexiones de Secure Shell (SSH) entre los dispositivos virtuales de origen y de destino.
- Compruebe que el endpoint de vCenter tenga recursos suficientes para completar la migración.
- Compruebe que haya cambiado la configuración de tiempo de espera del equilibrador de carga de forma predeterminada a 10 minutos como mínimo.
- Compruebe que la hora del sistema del entorno de destino de vRealize Automation esté sincronizada entre los componentes de IaaS y Cafe.
- Compruebe que los nodos del servicio web de IaaS y Model Manager del entorno de destino tengan la instancia correcta de Java Runtime Environment. Debe tener instalada la actualización 161 o posterior de JAVA SE Runtime Environment (JRE) 8, de 64 bits. Asegúrese de que los puntos de variable del sistema JAVA_HOME apuntan a la versión de Java que haya instalado en cada nodo de IaaS. Revise la ruta de acceso si es necesario.
- Compruebe que cada nodo de IaaS tiene instalado como mínimo PowerShell 3.0 o una versión posterior.
- Compruebe que los entornos de origen y de destino de vRealize Automation están en ejecución.
- Confirme que no hay ninguna actividad de usuario ni de aprovisionamiento en curso en el entorno de vRealize Automation de origen.
- Compruebe que cualquier software antivirus o de seguridad que se ejecute en nodos de IaaS en el entorno de vRealize Automation de destino que pueda interactuar con el sistema operativo y sus componentes esté correctamente configurado o deshabilitado.
- Verifique que el servicio web de IaaS y Model Manager no deban reiniciarse debido a que hay actualizaciones de instalación de Windows pendientes. Las actualizaciones pendientes podrían impedir que la migración comience o finalice el servicio de publicación World Wide Web.

Pasos siguientes

[Tareas previas a la migración.](#)

Tareas previas a la migración

Antes de realizar la migración, hay que realizar algunas tareas previas a la migración.

Las tareas previas a la migración que se realizan antes de migrar los datos del entorno de vRealize Automation de origen al entorno de vRealize Automation de destino varían según el entorno de origen.

Revisar los cambios realizados por la migración de vRealize Automation 6.2.x a la versión 7.x

vRealize Automation 7 y las versiones posteriores incorporan una serie de cambios funcionales durante y después del proceso de actualización. Revise estos cambios antes de actualizar la implementación de vRealize Automation 6.2.x a la versión más reciente.

Para obtener información sobre las diferencias entre vRealize Automation 6.2.x y la versión 7.x, consulte las [consideraciones sobre la actualización a una versión determinada de vRealize Automation](#) en *Actualizar de vRealize Automation 6.2.5 a 7.4*.

Nota La herramienta de ayuda para la actualización vRealize Production Test analiza el entorno de vRealize Automation 6.2.x en busca de cualquier configuración de características que pueda causar problemas de actualización y, asimismo, comprueba que el entorno esté listo para la actualización. Para descargar esta herramienta y la documentación relacionada, vaya a la página de descarga del producto [Herramienta VMware vRealize Production Test](#).

Después de migrar de vRealize Automation 6.2.x a la versión más reciente, los elementos de catálogo que utilizan estas definiciones de propiedad aparecen en el catálogo de servicios pero no están disponibles para solicitarlos.

- Tipos de control: casilla de verificación o vínculo.
- Atributos: relación, expresiones regulares o diseños de propiedades.

En vRealize Automation 7.x, las definiciones de propiedad ya no utilizan estos elementos. Debe recrear la definición de propiedad o configurar la definición de propiedad para utilizar una acción de script de vRealize Orchestrator en lugar de los tipos de control incrustado o atributos. Para obtener más información, consulte [Los elementos del catálogo aparecen en el catálogo de servicios después de la migración, pero no están disponibles para solicitarse](#).

Aplicar una revisión de agente de software

Antes de migrar de vRealize Automation 7.1 o 7.3 a la versión 7.4, debe aplicar una revisión al dispositivo de origen de modo que se puedan actualizar los agentes de software a TLS 1.2.

El protocolo de seguridad de capa de transporte (Transport Layer Security, TLS) proporciona integridad de datos entre el navegador y vRealize Automation. Esta revisión permite que los agentes de software del entorno de origen se actualicen a TLS 1.2. Esta actualización garantiza el máximo nivel de seguridad y es necesaria para vRealize Automation 7.1 o 7.3. Cada versión tiene su propia revisión.

Requisitos previos

Un entorno de origen de vRealize Automation 7.1 o 7.3 en ejecución.

Procedimiento

- ◆ Aplique esta revisión en el dispositivo de vRealize Automation 7.1 o 7.3 de origen antes de migrar a la versión 7.4. Consulte [el artículo 52897 de la base de conocimientos](#).

Pasos siguientes

[Cambiar la configuración de DoDeletes en el agente de vSphere a false.](#)

Cambiar la configuración de DoDeletes en el agente de vSphere a false

Si migra desde un entorno de vRealize Automation 6.2.x, debe cambiar el valor de DoDeletes de **true** a **false** en el agente de vSphere de destino antes de la migración.

Requisitos previos

Termine los requisitos previos para la migración.

Procedimiento

- 1 Cambie el valor de DoDeletes a **false**.

Esto impide la eliminación de las máquinas virtuales del entorno de origen. Los entornos de origen y de destino se ejecutan en paralelo. Pueden surgir discrepancias de concesión después de validar la migración de producción.

- 2 Configure el valor de DoDeletes en **true** después de que se valide la migración de producción y se apague el entorno de origen.
- 3 Siga los pasos del procedimiento [Configurar el agente de vSphere](#) para establecer DoDeletes como **false**.

Pasos siguientes

[Preparar máquinas virtuales vRealize Automation para la migración.](#)

Comprobar plantillas en el entorno de origen de vRealize Automation 6.x

Antes de migrar de vRealize Automation 6.x a la versión 7.4, debe comprobar las plantillas de máquina virtual para asegurarse de que cada plantilla tenga una configuración de memoria mínima de al menos 4 MB.

Si hay una plantilla de máquina virtual en el entorno de origen de vRealize Automation 6.x con menos de 4 MB de memoria, se producirá un error en la migración. Complete este procedimiento para determinar si alguno de los blueprints del entorno de origen de la versión 6.x dispone de menos de 4 MB de memoria.

Requisitos previos

Va a migrar de vRealize Automation 6.x a la versión 7.4.

Procedimiento

- 1 Inicie sesión en el dispositivo principal de vRealize Automation mediante SSH como **raíz**.

Si la instancia de vRealize Orchestrator es externa, inicie sesión en la máquina host de Orchestrator.

- 2 Cambie los directorios de la carpeta de datos de PostgreSQL en el host principal en `/var/vmware/vpostgres/current/pgdata/`.
- 3 Ejecute este script para comprobar si hay blueprints con una configuración de memoria inferior a 4 MB.

```
select * from [vCAC].[dbo].[VirtualMachineTemplate] where IsHidden = 0 and MemoryMB < 4;
```

En el ejemplo anterior, vCAC es el nombre de la base de datos.

- 4 Si el script encuentra blueprints con una configuración de memoria inferior a 4 MB, ejecute este script para actualizar la memoria de manera que tenga al menos ese valor.

```
update [vCAC].[dbo].[VirtualMachineTemplate] set MemoryMB = 4 where IsHidden = 0 and MemoryMB < 4;
```

En el ejemplo anterior, vCAC es el nombre de la base de datos.

Pasos siguientes

[Preparar máquinas virtuales vRealize Automation para la migración.](#)

Preparar máquinas virtuales vRealize Automation para la migración

Los problemas conocidos en relación con la migración de las máquinas virtuales vRealize Automation 6.2.x pueden causar problemas tras la migración.

Debe revisar [el artículo 000051531 de la base de conocimientos](#) y realizar las correcciones que correspondan a sus entornos antes de realizar la migración.

Pasos siguientes

[Recopilar información necesaria para la migración.](#)

Recopilar información necesaria para la migración

Utilice estas tablas para registrar la información que necesita para la migración entre sus entornos de origen y de destino.

Requisitos previos

Termine de confirmar los requisitos previos según cuál sea su situación.

- [Requisitos previos para la migración a un entorno mínimo.](#)
- [Requisitos previos para la migración a un entorno de alta disponibilidad.](#)

Tabla 1-81. Dispositivo de vRealize Automation de origen

| Opción | Descripción | Valor |
|------------------------------------|--|-------|
| Nombre del host | Inicie sesión en la Administración de dispositivos de vRealize Automation de origen. Busque el nombre de host en la pestaña Sistema . El nombre de host debe ser un nombre de dominio completo (fully qualified domain name, FQDN). | |
| Nombre de usuario raíz | raíz | |
| Contraseña raíz | La contraseña raíz que ha introducido al implementar el Dispositivo de vRealize Automation de origen. | |
| Ubicación del paquete de migración | Ruta de acceso a un directorio existente en el dispositivo de vRealize Automation 6.2.x o 7.x de origen en el que se crea el paquete de migración. El espacio disponible en el directorio debe ser dos veces más grande que el tamaño de la base de datos de vRealize Automation. La ubicación predeterminada es /storage. | |

Tabla 1-82. Dispositivo de vRealize Automation de destino

| Opción | Descripción | Valor |
|-------------------------------------|---|-------|
| Nombre de usuario raíz | raíz | |
| Contraseña raíz | La contraseña raíz que introdujo al implementar el dispositivo de vRealize Automation de destino. | |
| Tenant predeterminado | vsphere.local | |
| Nombre de usuario del administrador | administrador | |
| Contraseña del administrador | Contraseña del usuario administrator@vsphere.local que ha especificado al implementar el entorno de vRealize Automation de destino. | |

Tabla 1-83. Base de datos de IaaS de destino

| Opción | Descripción | Valor |
|---------------------------------|---|-------|
| Servidor de base de datos | Ubicación de la instancia de Microsoft SQL Server en la que reside la base de datos clonada. Si se utilizan una instancia con nombre y un puerto no predeterminado, especifíquela con el formato SERVIDOR,PUERTO\NOMBRE-DE-INSTANCIA. | |
| Nombre de base de datos clonada | El nombre de la base de datos de Microsoft SQL de IaaS de vRealize Automation 6.2.x/7.x de origen que se ha clonado para la migración. | |
| Modo de autenticación | Seleccione Windows o SQL Server. Si selecciona SQL Server, debe introducir un nombre de inicio de sesión y una contraseña. | |
| Nombre de inicio de sesión | Nombre de inicio de sesión del usuario de SQL Server que tiene la función db_owner para la base de datos clonada de Microsoft SQL de IaaS. | |

Tabla 1-83. Base de datos de IaaS de destino (Continuación)

| Opción | Descripción | Valor |
|---------------------------|--|-------|
| Contraseña | Contraseña del usuario de SQL Server. | |
| Clave de cifrado original | Clave de cifrado original que se recupera del entorno de origen. Consulte Obtener la clave de cifrado del entorno de vRealize Automation de origen . | |
| Nueva frase de contraseña | Una serie de palabras utilizadas para generar una nueva clave de cifrado. Esta frase de contraseña se utiliza cada vez que se instala un nuevo componente de IaaS en el entorno de vRealize Automation de destino. | |

Pasos siguientes

[Obtener la clave de cifrado del entorno de vRealize Automation de origen.](#)

Obtener la clave de cifrado del entorno de vRealize Automation de origen

Durante el proceso de migración hay que introducir la clave de cifrado del entorno de vRealize Automation de origen.

Requisitos previos

Compruebe que tiene privilegios de administrador en la máquina virtual del host de Manager Service activo en el entorno de origen.

Procedimiento

- 1 Abra un símbolo del sistema como administrador en la máquina virtual que aloje el servicio Manager Service activo en el entorno de origen y ejecute el siguiente comando.

```
"C:\Program Files
(x86)\VMware\VCAC\Server\ConfigTool\EncryptionKeyTool\DynamicOps.Tools.Encryption
KeyTool.exe" key-read -c "C:\Program Files
(x86)\VMware\VCAC\Server\ManagerService.exe.config" -v
```

Si su directorio de instalación no se encuentra en la ubicación predeterminada, C:\Archivos de programa (x86)\VMware\VCAC, edite la ruta para que muestre el directorio de instalación real.

- 2 Guarde la clave que aparece después de ejecutar el comando.

La clave es una cadena larga de caracteres con un aspecto parecido al de este ejemplo:

```
NRH+f/BlnCB6yvasLS3sxespgdkcFWAEuyV0g4lfryg=.
```

Pasos siguientes

- Si va a migrar desde un entorno de vRealize Automation 6.2.x: [Añadir cada tenant del entorno de vRealize Automation de origen al entorno de destino](#).
- Si va a migrar desde un entorno de vRealize Automation 7.x: [Enumerar los administradores de tenants e IaaS del entorno de vRealize Automation 6.2.x de origen](#).

Enumerar los administradores de tenants e IaaS del entorno de vRealize Automation 6.2.x de origen

Antes de migrar un entorno de vRealize Automation 6.2.x, conviene elaborar una lista de los administradores de tenants e IaaS en cada tenant.

Realice el siguiente procedimiento por cada tenant que haya en la consola de vRealize Automation de origen.

Nota Este procedimiento no es necesario si va a migrar desde un entorno de vRealize Automation 7.x.

Requisitos previos

Inicie sesión en la consola de vRealize Automation de origen como **Administrador** con la contraseña que ha introducido al implementar el dispositivo de vRealize Automation de origen.

Nota En un entorno de alta disponibilidad, abra la consola usando el nombre de dominio completo del equilibrador de carga del dispositivo virtual de origen: `https://vra-va-lb-hostname.domain.name/vcac`.

Procedimiento

- 1 Seleccione **Administración > Tenants**.
- 2 Haga clic en un nombre de tenant.
- 3 Haga clic en **Administradores**.
- 4 Confeccione una lista de todos los nombres de usuario de administrador de tenants e IaaS.
- 5 Haga clic en **Cancelar**.

Pasos siguientes

[Añadir cada tenant del entorno de vRealize Automation de origen al entorno de destino.](#)

Añadir cada tenant del entorno de vRealize Automation de origen al entorno de destino

Debe añadir tenants en el entorno de destino, para lo cual hay que usar el nombre de cada tenant en el entorno de origen.

Para que la migración se realice correctamente, es imprescindible crear cada uno de los tenants del entorno de origen en el entorno de destino. También se debe utilizar una dirección URL de acceso específica de cada tenant que añada usando el nombre de URL de tenant del entorno de origen. Si hay tenants sin utilizar en el entorno de origen que no quiera migrar, elimínelos de dicho entorno antes de iniciar la migración.

Nota La validación de la migración garantiza que el sistema de destino tenga al menos los mismos tenants configurados en el origen como se indica en los requisitos previos. Se lleva a cabo una comparación de tenants en función de los nombres de las URL de tenants con distinción de mayúsculas y minúsculas, no los nombres de tenants.

Realice este procedimiento por cada tenant del entorno de origen.

- Cuando se realiza la migración desde un entorno de vRealize Automation 6.2.x, se migran los tenants y los almacenes de identidades de SSO2 existentes del entorno de origen al entorno de destino de VMware Identity Manager.
- Cuando se realiza la migración desde un entorno de vRealize Automation 7.x, se migran su los tenants y los almacenes de identidades de VMware Identity Manager existentes del entorno de origen al entorno de destino de VMware Identity Manager.

Requisitos previos

- [Recopilar información necesaria para la migración.](#)
- Inicie sesión en la consola de vRealize Automation de destino como **Administrador** con la contraseña que ha introducido al implementar el dispositivo de vRealize Automation de destino.

Nota En un entorno de alta disponibilidad, abra la consola usando el nombre de dominio completo del equilibrador de carga del dispositivo virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.

Procedimiento

- 1 Seleccione **Administración > Tenants**.
- 2 Haga clic en el icono **Nuevo (+)**.
- 3 En el cuadro de texto **Nombre**, escriba un nombre de tenant que coincida con un nombre de tenant en el entorno de origen.

Por ejemplo, si el nombre de tenant en el entorno de origen es DEVTenant, escriba **DEVTenant**.
- 4 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 5 En el cuadro de texto **Nombre de URL**, escriba un nombre de URL de tenant que coincida con el nombre de URL de tenant en el entorno de origen.

El nombre de URL se usa para anexar un identificador específico del tenant a la URL de la consola de vRealize Automation.

Por ejemplo, si el nombre de URL de DEVTenant en el entorno de origen es dev, escriba **dev** para crear la URL `https://vra-va-hostname.domain.name/vcac/org/dev`.
- 6 (opcional) Escriba una dirección de correo electrónico en el cuadro de texto **Correo electrónico de contacto**.
- 7 Haga clic en **Enviar y siguiente**.

Pasos siguientes

[Crear un administrador para cada tenant añadido.](#)

Crear un administrador para cada tenant añadido

Se debe crear un administrador por cada tenant que se añada al entorno de destino. Para crearlo, hay que crear una cuenta de usuario local y asignarle privilegios de administrador de tenant.

Realice este procedimiento para cada tenant del entorno de destino.

Requisitos previos

- [Añadir cada tenant del entorno de vRealize Automation de origen al entorno de destino.](#)
- Inicie sesión en la consola de vRealize Automation de destino como **Administrador** con la contraseña que ha introducido al implementar el dispositivo de vRealize Automation de destino.

Nota En un entorno de alta disponibilidad, abra la consola usando el nombre de dominio completo del equilibrador de carga del dispositivo virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.

Procedimiento

- 1 Seleccione **Administración > Tenants**.
- 2 Haga clic en un tenant que ha agregado.
Por ejemplo, para DEVTenant, haga clic en **DEVTenant**.
- 3 Haga clic en **Usuarios locales**.
- 4 Haga clic en el icono **Nuevo (+)**.
- 5 En **Detalles de usuarios**, escriba la información solicitada para crear una cuenta de usuario local y asignar la función de administrador de tenant.
El nombre de usuario local debe ser único en el directorio local predeterminado, vsphere.local.
- 6 Haga clic en **Aceptar**.
- 7 Haga clic en **Administradores**.
- 8 Escriba el nombre de usuario local en el cuadro de búsqueda **Administradores de tenants** y pulse Entrar.
- 9 Haga clic en el nombre adecuado en los resultados de búsqueda para añadir el usuario a la lista de administradores de tenant.
- 10 Haga clic en **Finalizar**.
- 11 Cierre sesión en la consola.

Pasos siguientes

- Para una implementación mínima: [Sincronización de usuarios y grupos para un vínculo de Active Directory antes de la migración a un entorno mínimo.](#)
- Para una implementación de alta disponibilidad: [Sincronizar usuarios y grupos para un vínculo de Active Directory antes de la migración a un entorno de alta disponibilidad.](#)

Sincronización de usuarios y grupos para un vínculo de Active Directory antes de la migración a un entorno mínimo

Antes de importar los usuarios y los grupos a una implementación mínima de vRealize Automation, debe conectar la instancia de vRealize Automation de destino al vínculo de Active Directory.

Realice este procedimiento con cada tenant. Si un tenant tiene más de un Active Directory, realícelo por cada Active Directory que el tenant use.

Requisitos previos

- [Crear un administrador para cada tenant añadido.](#)
- Compruebe que tiene privilegios de acceso a Active Directory.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Directorios**.
- 2 Haga clic en el icono **Añadir directorio (+)** y seleccione **Añadir Active Directory en LDAP/IWA**.
- 3 Introduzca la configuración de su cuenta de Active Directory.

◆ Para Active Directory no nativos

| Opción | Entrada de muestra |
|---|--|
| Nombre de directorio | Escriba un nombre de directorio único. Selecione Active Directory en LDAP si utiliza Active Directory no nativo. |
| Este directorio admite la ubicación de servicio de DNS | Anule la selección de esta opción. |
| DN de la base | Escriba el nombre distintivo (distinguished name, DN) del punto de inicio de las búsquedas en el servidor de directorios. Por ejemplo, cn=users,dc=rainpole,dc=local . |
| DN de enlace | Escriba el nombre distintivo (DN) completo, incluido el nombre común (CN), de una cuenta de usuario de Active Directory que tenga privilegios para buscar usuarios. Por ejemplo, cn=config_admin_infra,cn=users,dc=rainpole,dc=local . |
| Contraseña de DN de enlace | Introduzca la contraseña de Active Directory para la cuenta que puede buscar usuarios, y haga clic en Probar conexión para probar la conexión con el directorio configurado. |

◆ Para Active Directory nativos

| Opción | Entrada de muestra |
|--|--|
| Nombre de directorio | Escriba un nombre de directorio único. Selecione Active Directory (Autenticación de Windows integrada) si usa Active Directory nativo. |
| Nombre de dominio | Escriba el nombre del dominio al que desea unirse. |
| Nombre de usuario del administrador del dominio | Escriba el nombre de usuario del administrador del dominio. |

| Opción | Entrada de muestra |
|--|--|
| Contraseña del administrador del dominio | Escriba la contraseña del administrador del dominio. |
| UPN del usuario de enlace | Utilice el formato de dirección de correo electrónico para introducir el nombre del usuario que se puede autenticar en el dominio. |
| Contraseña de DN de enlace | Escriba la contraseña de la cuenta de enlace de Active Directory para la cuenta que puede buscar usuarios. |

4 Haga clic en **Guardar y Siguiente**.

En la página **Seleccione los dominios** verá una lista de dominios.

5 Acepte la configuración de dominio predeterminada y haga clic en **Siguiente**.

6 Compruebe que los nombres de atributo estén asignados a los atributos de Active Directory correctos y haga clic en **Siguiente**.

7 Seleccione los grupos y los usuarios que desea sincronizar.

a Haga clic en el icono **Nuevo (+)**.

b Escriba el dominio de usuario y haga clic en **Buscar grupos**.

Por ejemplo, introduzca **dc=vcac,dc=local**.

c Para seleccionar los grupos que desea sincronizar, haga clic en **Seleccionar** y en **Siguiente**.

d En la página **Seleccionar usuarios**, elija los usuarios que desea sincronizar y haga clic en **Siguiente**.

Añada solo los usuarios y los grupos que deban utilizar vRealize Automation. No seleccione **Sincronizar grupos anidados** a menos que todos los grupos del nido deban utilizar vRealize Automation.

8 Revise los usuarios y los grupos que sincronizará con el directorio, y haga clic en **Sincronizar directorio**.

La sincronización de directorios tarda un poco y se ejecuta en segundo plano.

Pasos siguientes

[Ejecutar la recopilación de datos de inventario de seguridad y de red de NSX en el entorno de vRealize Automation de origen](#)

Sincronizar usuarios y grupos para un vínculo de Active Directory antes de la migración a un entorno de alta disponibilidad

Antes de importar los usuarios y los grupos a en un entorno de vRealize Automation de alta disponibilidad, debe conectarse al vínculo de Active Directory.

- Realice los pasos del 1 al 8 con cada tenant. Si un tenant tiene más de un Active Directory, realícelo por cada Active Directory que el tenant use.
- Repita los pasos 9 y 10 con cada proveedor de identidades asociado con un tenant.

Requisitos previos

- [Crear un administrador para cada tenant añadido.](#)
- Compruebe que tiene privilegios de acceso a Active Directory.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Directorios**.
- 2 Haga clic en el icono **Añadir directorio** (+) y seleccione **Añadir Active Directory en LDAP/IWA**.
- 3 Introduzca la configuración de su cuenta de Active Directory.

◆ Para Active Directory no nativos

| Opción | Entrada de muestra |
|---|--|
| Nombre de directorio | Escriba un nombre de directorio único. Seleccione Active Directory en LDAP si utiliza Active Directory no nativo. |
| Este directorio admite la ubicación de servicio de DNS | Anule la selección de esta opción. |
| DN de la base | Escriba el nombre distintivo (distinguished name, DN) del punto de inicio de las búsquedas en el servidor de directorios. Por ejemplo, cn=users,dc=rainpole,dc=local . |
| DN de enlace | Escriba el nombre distintivo (DN) completo, incluido el nombre común (CN), de una cuenta de usuario de Active Directory que tenga privilegios para buscar usuarios. Por ejemplo, cn=config_admin infra,cn=users,dc=rainpole,dc=local . |
| Contraseña de DN de enlace | Introduzca la contraseña de Active Directory para la cuenta que puede buscar usuarios, y haga clic en Probar conexión para probar la conexión con el directorio configurado. |

◆ Para Active Directory nativos

| Opción | Entrada de muestra |
|--|---|
| Nombre de directorio | Escriba un nombre de directorio único. Seleccione Active Directory (Autenticación de Windows integrada) si usa Active Directory nativo. |
| Nombre de dominio | Escriba el nombre del dominio al que desea unirse. |
| Nombre de usuario del administrador del dominio | Escriba el nombre de usuario del administrador del dominio. |
| Contraseña del administrador del dominio | Escriba la contraseña de usuario del administrador del dominio. |
| UPN del usuario de enlace | Utilice el formato de dirección de correo electrónico para introducir el nombre del usuario que se puede autenticar en el dominio. |
| Contraseña de DN de enlace | Escriba la contraseña de la cuenta de enlace de Active Directory para la cuenta que puede buscar usuarios. |

4 Haga clic en **Guardar y Siguiente**.

En la página **Seleccione los dominios**, se mostrará la lista de dominios.

5 Acepte la configuración de dominio predeterminada y haga clic en **Siguiente**.

6 Compruebe que los nombres de atributo estén asignados a los atributos de Active Directory correctos y haga clic en **Siguiente**.

7 Seleccione los grupos y los usuarios que desea sincronizar.

a Haga clic en el icono **Nuevo** (+).

b Escriba el dominio de usuario y haga clic en **Buscar grupos**.

Por ejemplo, introduzca **dc=vcac,dc=local**.

c Para seleccionar los grupos que desea sincronizar, haga clic en **Seleccionar** y en **Siguiente**.

d En la página **Select Users** (Seleccionar usuarios) elija los usuarios que desea sincronizar y haga clic en **Siguiente**.

Añada solo los usuarios y los grupos que deban utilizar vRealize Automation. No seleccione **Sincronizar grupos anidados** a menos que todos los grupos del nido deban utilizar vRealize Automation.

8 Revise los usuarios y los grupos que sincronizará con el directorio, y haga clic en **Sincronizar directorio**.

La sincronización de directorios tarda un poco y se ejecuta en segundo plano.

9 Seleccione **Administración > Administración de directorios > Proveedores de identidades** y haga clic en el nuevo proveedor de identidades.

Por ejemplo, **WorkspaceIDP__1**.

10 En la página del proveedor de identidades que ha seleccionado, agregue un conector para cada nodo.

a Siga las instrucciones para **Agregar un conector**.

b Actualice el valor de la propiedad **Nombre de host de IDP** para que apunte al nombre de dominio completo (FQDN) del equilibrador de carga de vRealize Automation.

c Haga clic en **Guardar**.

Pasos siguientes

[Ejecutar la recopilación de datos de inventario de seguridad y de red de NSX en el entorno de vRealize Automation de origen.](#)

Ejecutar la recopilación de datos de inventario de seguridad y de red de NSX en el entorno de vRealize Automation de origen

Antes de migrar, debe ejecutar la recopilación de datos de inventario de red y seguridad de NSX en el entorno de vRealize Automation de origen.

Esta recopilación de datos es necesaria para que la acción de reconfiguración del equilibrador de carga funcione en vRealize Automation 7.4 al migrar desde implementaciones de 7.1, 7.2 o 7.3.

Nota No es necesario ejecutar la recopilación de datos en el entorno de origen al migrar desde vRealize Automation 6.2. x. vRealize Automation 6.2. x no es compatible con la acción de reconfiguración del equilibrador de carga.

Procedimiento

- ◆ Ejecute la recopilación de datos de inventario de red y seguridad de NSX en el entorno de vRealize Automation de origen antes de migrar a vRealize Automation 7.4. Consulte [Iniciar recopilación de datos de endpoint manualmente](#) en *Administración de vRealize Automation*.

Pasos siguientes

[Clonar manualmente la base de datos de Microsoft SQL de IaaS del entorno de vRealize Automation de origen.](#)

Clonar manualmente la base de datos de Microsoft SQL de IaaS del entorno de vRealize Automation de origen

Antes de realizar la migración, debe hacer una copia de seguridad de la base de datos de Microsoft SQL de IaaS en el entorno de vRealize Automation de origen y restaurarla en una nueva base de datos en blanco creada en el entorno de vRealize Automation de destino.

Requisitos previos

- [Ejecutar la recopilación de datos de inventario de seguridad y de red de NSX en el entorno de vRealize Automation de origen.](#)
- Obtener información sobre cómo hacer una copia de seguridad de una base de datos de SQL Server y cómo restaurarla. Encuentre artículos en [Microsoft Developer Network](#) sobre cómo crear una copia de seguridad completa de la base de datos de SQL Server y restaurar una base de datos SQL Server en una nueva ubicación.

Procedimiento

- ◆ Cree una copia de seguridad completa de la base de datos de Microsoft SQL de IaaS del entorno de vRealize Automation 6.2.x o 7.x de origen. Esta copia de seguridad sirve para restaurar la base de datos SQL en una nueva base de datos en blanco creada en el entorno de destino.

Pasos siguientes

[Captura de un snapshot del entorno de vRealize Automation de destino.](#)

Captura de un snapshot del entorno de vRealize Automation de destino

Tome un snapshot de cada máquina virtual de destino de vRealize Automation. Si la migración no se realiza correctamente, podrá volver a utilizar los snapshots de máquina virtual.

Para obtener más información, consulte la documentación de vSphere.

Requisitos previos

Clonar manualmente la base de datos de Microsoft SQL de IaaS del entorno de vRealize Automation de origen.

Pasos siguientes

Siga uno de estos procedimientos:

- [Migración de los datos de origen de vRealize Automation a un entorno mínimo de vRealize Automation 7.4.](#)
- [Migrar datos de origen de vRealize Automation a un entorno de alta disponibilidad de vRealize Automation 7.4.](#)

Procedimientos de migración

El procedimiento que hay que realizar para migrar los datos del entorno de vRealize Automation de origen depende de si se van a migrar a un entorno mínimo o a un entorno de alta disponibilidad.

Migración de los datos de origen de vRealize Automation a un entorno mínimo de vRealize Automation 7.4

Puede migrar los datos de su entorno actual de vRealize Automation a una nueva instalación de vRealize Automation 7.4.

Todos los tenants en el sistema de origen deben volver a crearse en el destino y pasar por el procedimiento Migrar almacenes de identidades. Para obtener más información, consulte [Migración de almacenes de identidades a VMware Identity Manager](#).

Requisitos previos

- [Recopilar información necesaria para la migración.](#)
- [Obtener la clave de cifrado del entorno de vRealize Automation de origen.](#)
- [Añadir cada tenant del entorno de vRealize Automation de origen al entorno de destino.](#)
- [Crear un administrador para cada tenant añadido.](#)
- [Sincronización de usuarios y grupos para un vínculo de Active Directory antes de la migración a un entorno mínimo.](#)
- [Clonar manualmente la base de datos de Microsoft SQL de IaaS del entorno de vRealize Automation de origen.](#)
- [Captura de un snapshot del entorno de vRealize Automation de destino.](#)
- Inicie sesión en la administración de dispositivos de vRealize Automation de destino como **raíz** con la contraseña que ha introducido al implementar el dispositivo de vRealize Automation de destino.

Procedimiento

- 1 Seleccione **Configuración de vRA > Migración**.

2 Escriba la información para el dispositivo de origen de vRealize Automation.

| Opción | Descripción |
|------------------------------------|--|
| Nombre del host | Nombre de host del dispositivo de origen de vRealize Automation. |
| Nombre de usuario raíz | root |
| Contraseña raíz | Contraseña raíz que introdujo al implementar el dispositivo de vRealize Automation. |
| Ubicación del paquete de migración | Ruta de acceso a un directorio existente en el dispositivo de vRealize Automation 6.2.x o 7.x de origen en el que se crea el paquete de migración. |

3 Escriba la información para el dispositivo de destino de vRealize Automation.

| Opción | Descripción |
|-------------------------------------|---|
| Nombre de usuario raíz | root |
| Contraseña raíz | La contraseña raíz que introdujo al implementar el dispositivo de vRealize Automation de destino. |
| Tenant predeterminado | vsphere.local No puede modificar este campo. |
| Nombre de usuario del administrador | administrador No puede modificar este campo. |
| Contraseña del administrador | Contraseña del usuario administrator@vsphere.local que ha especificado al implementar el entorno de vRealize Automation de destino. |

4 Escriba la información para el servidor de base de datos de IaaS de destino.

| Opción | Descripción |
|---------------------------------|---|
| Servidor de base de datos | Ubicación de la instancia de Microsoft SQL Server en la que reside la base de datos de Microsoft SQL de IaaS de vRealize Automation restaurada. Si se usa una instancia con nombre y un puerto no predeterminado, especifíquelos con el formato <i>SERVIDOR,PUERTO/NOMBRE-DE-INSTANCIA</i> . Si configura la instancia de Microsoft SQL Server de destino para utilizar la característica de grupo de disponibilidad AlwaysOn (AlwaysOn Availability Group, AAG), debe introducir la instancia de SQL Server de destino como el nombre del agente de escucha de AAG, sin un puerto ni un nombre de instancia. |
| Nombre de base de datos clonada | Nombre de la base de datos de Microsoft SQL de IaaS de vRealize Automation 6.2.x o 7.x de origen a partir de la cual ha creado una copia de seguridad en el origen y que ha restaurado en el entorno de destino. |
| Modo de autenticación | <ul style="list-style-type: none"> ■ Windows Si utiliza el modo de autenticación de Windows, el usuario del servicio de IaaS debe tener la función db_owner de SQL Server. Al utilizar el modo de autenticación de SQL Server, se requieren los mismos permisos. ■ SQL Server SQL Server abre los cuadros de texto Nombre de inicio de sesión y Contraseña. |
| Nombre de inicio de sesión | Nombre de inicio de sesión del usuario de SQL Server con la función db_owner de la base de datos de Microsoft SQL de IaaS clonada. |

| Opción | Descripción |
|---------------------------|--|
| Contraseña | Contraseña del usuario de SQL Server con la función db_owner de la base de datos de Microsoft SQL de IaaS clonada. |
| Clave de cifrado original | Clave de cifrado original que se recupera del entorno de origen. Consulte Obtener la clave de cifrado del entorno de vRealize Automation de origen . |
| Nueva frase de contraseña | Una serie de palabras utilizadas para generar una nueva clave de cifrado. Esta frase de contraseña se utiliza cada vez que se instala un nuevo componente de IaaS en el entorno de vRealize Automation de destino. |

5 Haga clic en **Validar**.

La página muestra el progreso de la validación.

- Si todos los elementos se validan correctamente, vaya al paso 8.
- Si un elemento no se puede validar, examine el mensaje de error y el archivo de log de validación en los nodos de IaaS. Para saber dónde está el archivo de log, consulte [ubicaciones de logs de migración](#). Haga clic en **Editar configuración** y edite el problema. Vaya al paso 7.

6 Haga clic en **Migrar**.

La página muestra el progreso de la migración.

- Si la migración se realiza correctamente, la página muestra todas las tareas de migración como completadas.
- Si la migración no se realiza correctamente, examine los archivos de log de la migración en el dispositivo virtual y los nodos de IaaS. Para saber dónde está el archivo de log, consulte [ubicaciones de logs de migración](#).

Acabe estos pasos antes de reiniciar la migración.

- a Revierta el entorno de vRealize Automation de destino al estado que capturó cuando creó el snapshot antes de la migración.
- b Restablezca la base de datos de Microsoft SQL de IaaS de destino usando la copia de seguridad de la base de datos de IaaS de origen.

Pasos siguientes

[Tareas posteriores a la migración.](#)

Migrar datos de origen de vRealize Automation a un entorno de alta disponibilidad de vRealize Automation 7.4

Puede migrar los datos de su entorno actual de vRealize Automation a una nueva instalación de vRealize Automation 7.4 configurada como un entorno de alta disponibilidad.

Todos los tenants en el sistema de origen deben volver a crearse en el destino y pasar por el procedimiento Migrar almacenes de identidades. Para obtener más información, consulte [Migración de almacenes de identidades a VMware Identity Manager](#).

Requisitos previos

- [Recopilar información necesaria para la migración.](#)
- [Obtener la clave de cifrado del entorno de vRealize Automation de origen.](#)
- [Añadir cada tenant del entorno de vRealize Automation de origen al entorno de destino.](#)
- [Crear un administrador para cada tenant añadido.](#)
- [Sincronizar usuarios y grupos para un vínculo de Active Directory antes de la migración a un entorno de alta disponibilidad.](#)
- [Clonar manualmente la base de datos de Microsoft SQL de IaaS del entorno de vRealize Automation de origen.](#)
- [Captura de un snapshot del entorno de vRealize Automation de destino.](#)
- Inicie sesión en la administración de dispositivos de vRealize Automation de destino como **raíz** con la contraseña que ha introducido al implementar el dispositivo de vRealize Automation de destino.

Procedimiento

- 1 Seleccione **Configuración de vRA > Migración**.
- 2 Escriba la información del dispositivo de origen de Dispositivo de vRealize Automation.

| Opción | Descripción |
|------------------------|---|
| Nombre del host | Nombre de host del dispositivo de origen de vRealize Automation. |
| Nombre de usuario raíz | root |
| Contraseña raíz | Contraseña raíz que introdujo al implementar el dispositivo de vRealize Automation de origen. |

- 3 Introduzca la información de la ubicación del paquete de migración en el dispositivo de vRealize Automation de origen.

| Opción | Descripción |
|------------------------------------|--|
| Ubicación del paquete de migración | Ruta de acceso a un directorio existente en el dispositivo de vRealize Automation 6.2.x o 7.x de origen en el que se crea el paquete de migración. |

- 4 Escriba la información para el dispositivo de destino de vRealize Automation.

| Opción | Descripción |
|-------------------------------------|---|
| Nombre de usuario raíz | root |
| Contraseña raíz | La contraseña raíz que introdujo al implementar el dispositivo de vRealize Automation de destino. |
| Tenant predeterminado | vsphere.local |
| Nombre de usuario del administrador | administrador |
| Contraseña del administrador | Contraseña del usuario administrator@vsphere.local que ha especificado al implementar el entorno de vRealize Automation de destino. |

5 Escriba la información para el servidor de base de datos de IaaS de destino.

| Opción | Descripción |
|--|--|
| Servidor de base de datos | Ubicación de la instancia de Microsoft SQL Server en la que reside la base de datos Microsoft SQL de IaaS de vRealize Automation restaurada. Si se usa una instancia con nombre y un puerto no predeterminado, especifíquelos con el formato <i>SERVIDOR,PUERTO/NOMBRE-DE-INSTANCIA</i> . Si configura la instancia de Microsoft SQL Server de destino para utilizar la característica de grupo de disponibilidad AlwaysOn (AlwaysOn Availability Group, AAG), debe introducir la instancia de SQL Server de destino como el nombre del agente de escucha de AAG, sin un puerto ni un nombre de instancia. |
| Nombre de base de datos clonada | Nombre de la base de datos de Microsoft SQL de IaaS de vRealize Automation 6.2.x o 7.x de origen a partir de la cual ha creado una copia de seguridad en el origen y que ha restaurado en el entorno de destino. |
| Modo de autenticación | <ul style="list-style-type: none"> ■ Windows Si utiliza el modo de autenticación de Windows, el usuario del servicio de IaaS debe tener la función db_owner de SQL Server. Al utilizar el modo de autenticación de SQL Server, se requieren los mismos permisos. ■ SQL Server SQL Server abre los cuadros de texto Nombre de inicio de sesión y Contraseña. |
| Nombre de inicio de sesión | Nombre de inicio de sesión del usuario de SQL Server con la función db_owner de la base de datos de Microsoft SQL de IaaS clonada. |
| Contraseña | Contraseña del usuario de SQL Server con la función db_owner de la base de datos de Microsoft SQL de IaaS clonada. |
| Clave de cifrado original | Clave de cifrado original que se recupera del entorno de origen. Consulte Obtener la clave de cifrado del entorno de vRealize Automation de origen . |
| Nueva frase de contraseña | Una serie de palabras utilizadas para generar una nueva clave de cifrado. Esta frase de contraseña se utiliza cada vez que se instala un nuevo componente de IaaS en el entorno de vRealize Automation de destino. |

6 Haga clic en **Validar**.

La página muestra el progreso de la validación.

- Si todos los elementos se validan correctamente, vaya al paso 8.
- Si un elemento no se puede validar, examine el mensaje de error y el archivo de log de validación en los nodos de IaaS. Para saber dónde está el archivo de log, consulte [ubicaciones de logs de migración](#). Haga clic en **Editar configuración** y edite el problema. Vaya al paso 7.

7 Haga clic en **Migrar**.

La página muestra el progreso de la migración.

- Si la migración se realiza correctamente, la página muestra todas las tareas de migración como completadas.
- Si la migración no se realiza correctamente, examine los archivos de log de la migración en el dispositivo virtual y los nodos de IaaS. Para saber dónde está el archivo de log, consulte [ubicaciones de logs de migración](#).

Acabe estos pasos antes de reiniciar la migración.

- a Revierta el entorno de vRealize Automation de destino al estado que capturó cuando creó el snapshot antes de la migración.
- b Restablezca la base de datos de Microsoft SQL de IaaS de destino usando la copia de seguridad de la base de datos de IaaS de origen.

Pasos siguientes

[Tareas posteriores a la migración.](#)

Tareas posteriores a la migración

Después de migrar vRealize Automation, realice las tareas posteriores a la migración que correspondan a su situación.

Nota Tras migrar los almacenes de identidades, los usuarios de vRealize Code Stream deben reasignar manualmente las funciones de vRealize Code Stream.

Añadir administradores de tenants e IaaS desde el entorno de origen de vRealize Automation 6.2.x

Tras una migración, debe eliminar y restaurar los administradores de tenants de vRealize Automation 6.2.x en cada tenant.

Realice el siguiente procedimiento por cada tenant que haya en la consola de vRealize Automation de destino.

Nota Este procedimiento no es necesario si va a migrar desde un entorno de vRealize Automation 7.x.

Requisitos previos

- Haber migrado correctamente a la versión más reciente de vRealize Automation.
- Inicie sesión en la consola de vRealize Automation de destino como **Administrador** con la contraseña que ha introducido al implementar el dispositivo de vRealize Automation de destino.

Procedimiento

- 1 Seleccione **Administración > Tenants**.
- 2 Haga clic en un nombre de tenant.
- 3 Haga clic en **Administradores**.
- 4 Confeccione una lista de todos los nombres de usuario y nombres de administradores de tenants.
- 5 Seleccione cada administrador y haga clic en el icono de eliminación (Eliminar) hasta eliminar todos los administradores.
- 6 Haga clic en **Finalizar**.
- 7 En la página Tenants, vuelva a hacer clic en el nombre del tenant.

- 8 Haga clic en **Administradores**.
- 9 Escriba en el cuadro de búsqueda correspondiente el nombre de cada usuario eliminado y presione Entrar.
- 10 Haga clic en el nombre del usuario que proceda en los resultados de la búsqueda para volver a añadirlo como administrador.

Cuando termine, la lista de administradores de tenants tendrá el mismo aspecto que la lista de los administradores que ha eliminado.

- 11 Haga clic en **Finalizar**.

Ejecutar la conexión de prueba y comprobar los endpoints migrados

Al realizar la migración a vRealize Automation 7.4, se realizan cambios en los endpoints del entorno de destino.

Después de migrar a vRealize Automation 7.4, debe utilizar la acción **Probar conexión** para todos los endpoints aplicables. También es posible que tenga que realizar ajustes en algunos de los endpoints migrados. Para obtener más información, consulte [Consideraciones al trabajar con endpoints actualizados o migrados](#).

La configuración de seguridad predeterminada relativa a endpoints actualizados o migrados consiste en no aceptar certificados que no sean de confianza.

Si usaba certificados que no eran de confianza, después de actualizar o migrar desde una instalación de vRealize Automation anterior, deberá hacer lo siguiente para que todos los endpoints de vSphere y de NSX permitan la validación de certificados. De lo contrario, las operaciones de endpoint generarán errores de certificado. Para obtener más información, consulte los artículos de la base de conocimientos de VMware *La comunicación del endpoint se interrumpe después de actualizar a vRA 7.3 (2150230)* en <http://kb.vmware.com/kb/2150230> y *Cómo descargar e instalar certificados raíz de vCenter Server para evitar advertencias de certificado del navegador web (2108294)* en <http://kb.vmware.com/kb/2108294>.

- 1 Después de la actualización o migración, inicie sesión en la máquina del agente de vSphere de vRealize Automation y reinicie los agentes de vSphere en la pestaña **Servicios**.

Es posible que no todos los agentes se reinicien con la migración, de modo que puede que sea necesario reiniciarlos manualmente.

- 2 Espere a que al menos un informe de ping finalice. Un informe de ping tarda uno o dos minutos en finalizar.
- 3 Cuando los agentes de vSphere hayan empezado a recopilar datos, inicie sesión en vRealize Automation como un administrador de IaaS.
- 4 Haga clic en **Infraestructura > Endpoints > Endpoints**.
- 5 Edite un endpoint de vSphere y haga clic en **Probar conexión**.
- 6 Si aparece un mensaje de certificado, haga clic en **Aceptar** para aceptar el certificado.

Si no aparece un mensaje de certificado, es posible que el certificado esté actualmente almacenado en una entidad raíz de confianza de la máquina de Windows que aloja el servicio del endpoint, por ejemplo, como una máquina de agente de proxy o una máquina de DEM.

- 7 Haga clic en **Aceptar** para confirmar la aceptación de certificado y guardar el endpoint.
- 8 Repita este procedimiento por cada endpoint de vSphere.
- 9 Repita este procedimiento por cada endpoint de NSX.

Si la acción **Probar conexión** finaliza correctamente, pero alguna de las operaciones de aprovisionamiento o de recopilación de datos genera errores, puede instalar el mismo certificado en todas las máquinas de agente que sirvan al endpoint y en todas las máquinas DEM. Si lo prefiere, puede desinstalar el certificado de las máquinas existentes y repetir el procedimiento anterior en el endpoint con el error.

Ejecutar la recopilación de datos de inventario de red y seguridad de NSX en el entorno de vRealize Automation 7.4 de destino

Después de migrar, debe ejecutar la recopilación de datos de inventario de red y seguridad de NSX en el entorno de vRealize Automation 7.4 de destino.

Esta recopilación de datos es necesaria para que la acción de reconfiguración del equilibrador de carga funcione en vRealize Automation 7.4 para las implementaciones de 7.1, 7.2 y 7.3.

Nota No es necesario realizar esta recopilación de datos si migró de vRealize Automation 6.2.x a 7.4.

Requisitos previos

- [Ejecutar la recopilación de datos de inventario de seguridad y de red de NSX en el entorno de vRealize Automation de origen](#) .
- La migración a vRealize Automation 7.4 se realiza correctamente.

Procedimiento

- ◆ Ejecute la recopilación de datos de inventario de red y seguridad de NSX en el entorno de vRealize Automation de destino antes de migrar a vRealize Automation 7.4. Consulte [Iniciar recopilación de datos de endpoint manualmente](#) en *Administración de vRealize Automation*.

Reconfigurar los equilibradores de carga después de la migración a un entorno de alta disponibilidad

Cuando se migra a un entorno de alta disponibilidad, se deben realizar estas tareas con cada equilibrador de carga después de finalizada la migración.

Requisitos previos

[Migrar datos de origen de vRealize Automation a un entorno de alta disponibilidad de vRealize Automation 7.4.](#)

Procedimiento

- 1 Restaure la configuración de comprobación de estado original de forma que los nodos de réplica puedan aceptar el tráfico entrante. Para ello configure los equilibradores de carga para estos elementos.
 - Dispositivo de vRealize Automation.
 - Servidor web de IaaS que aloja Model Manager.
 - Manager Service.
- 2 Cambie la configuración de tiempo de espera del equilibrador de carga a los valores predeterminados.

Migrar un servidor externo de Orchestrator a vRealize Automation 7.4

Puede migrar un servidor externo de Orchestrator a una instancia de vRealize Orchestrator integrada en vRealize Automation.

Puede implementar vRealize Orchestrator como instancia externa de servidor y configurar vRealize Automation para que funcione con esa instancia externa; también puede configurar y utilizar el servidor de vRealize Orchestrator que se incluye en Dispositivo de vRealize Automation.

VMware le recomienda que migre su vRealize Orchestrator externo al servidor de Orchestrator que está integrado en vRealize Automation. La migración de una instancia externa al Orchestrator integrado proporciona las siguientes ventajas:

- Reduce el coste total de propiedad.
- Simplifica el modelo de implementación.
- Mejora la eficiencia operativa.

Nota Considere utilizar un vRealize Orchestrator externo en los casos siguientes:

- Varios tenants en el entorno de vRealize Automation.
 - Entorno geográficamente disperso.
 - Manejo de la carga de trabajo.
 - Uso de complementos específicos, como versiones anteriores a Site Recovery Manager 6.5.
-

Migration Scenarios

The procedure of migrating an external vRealize Orchestrator instance to a vRealize Orchestrator instance embedded in vRealize Automation varies depending on the setup that you have. Several migration scenarios exist based on whether the external Orchestrator server is Windows-based or a virtual appliance, using the embedded database or an external one, and other conditions. You can combine the migration process with an upgrade of vRealize Orchestrator, vRealize Automation, or both. In this case, the migration procedure depends on the source versions of the products.

Migration Scenario Matrix

You can choose a migration scenario based on the source deployment.

| vRealize Orchestrator Deployment | vRealize Automation Deployment | Migration Scenario |
|--|-----------------------------------|---|
| vRealize Orchestrator 6.0.3 Virtual Appliance | vRealize Automation 6.2.3 | Migrar un dispositivo virtual vRealize Orchestrator 6.x externo a vRealize Automation 7.4 |
| vRealize Orchestrator 6.0.4 on Windows | vRealize Automation 6.2.4 | Migrar un vRealize Orchestrator 6.x externo en Windows a vRealize Automation 7.4 |
| vRealize Orchestrator 6.0.4 Virtual Appliance | vRealize Automation 6.2.4 | Migrar un dispositivo virtual vRealize Orchestrator 6.x externo a vRealize Automation 7.4 |
| vRealize Orchestrator 6.0.5 Virtual Appliance | vRealize Automation 6.2.5 | Migrar un dispositivo virtual vRealize Orchestrator 6.x externo a vRealize Automation 7.4 |
| vRealize Orchestrator 7.0 Virtual Appliance with an external Oracle Database 12 c | vRealize Automation 7.0 or IaaS | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |
| vRealize Orchestrator 7.0.1 Virtual Appliance with an external PostgreSQL 9.3.9 database | vRealize Automation 7.0.1 or IaaS | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |
| vRealize Orchestrator 7.1 Virtual Appliance | vRealize Automation 7.1 | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |
| vRealize Orchestrator 7.2 Virtual Appliance | vRealize Automation 7.2 | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |
| vRealize Orchestrator 7.3 Virtual Appliance | vRealize Automation 7.3 | Migrar un vRealize Orchestrator 7.x externo a vRealize Automation 7.4 |
| vRealize Orchestrator 6.0.3 on Windows | vRealize Automation 6.2.3 | Migrar la configuración de Orchestrator desde Windows al dispositivo virtual |

Migrar la configuración de Orchestrator desde Windows al dispositivo virtual

Migre la configuración independiente de 5.5.x y 6.x Orchestrator Windows a Orchestrator Appliance.

Requisitos previos

- Implemente y configure un nodo de Orchestrator en la versión de destino. Consulte [Configurar un servidor de Orchestrator independiente](#).
- Si la instancia de origen de Orchestrator utiliza un certificado de firma de paquetes SHA1, asegúrese de volver a generar el certificado mediante un algoritmo de firma más seguro. El algoritmo de firma recomendado es SHA2.
- Detenga el servicio del servidor de Orchestrator en las instancias de origen y destino de Orchestrator.

- Cree una copia de seguridad de la base de datos del servidor de origen de Orchestrator, incluido el esquema de la base de datos.

Nota Si tiene pensado utilizar el entorno de Orchestrator de origen hasta el nuevo esté totalmente configurado, cree una copia de la base de datos de origen. De lo contrario, puede configurar la instancia de Orchestrator de destino para que utilice la misma base de datos, pero en ese caso el entorno de Orchestrator de origen ya no funcionará debido a que el esquema de base de datos se actualiza a la versión de la instancia de destino de Orchestrator.

Procedimiento

- 1 Descargue la herramienta de migración desde el servidor de destino de Orchestrator.
 - a Inicie sesión en el centro de control como **raíz**.
 - b Abra la página **Exportar o importar configuración** y haga clic en la pestaña **Importar configuración**.
 - c Descargue la herramienta de migración como se especifica en la descripción de la página o directamente desde https://orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/api/server/migration-tool.
- 2 Exporte la configuración de Orchestrator desde el servidor de Orchestrator de origen.
 - a Extraiga el archivo descargado en la carpeta de instalación de Orchestrator.
La ruta predeterminada de la carpeta de instalación de Orchestrator en una instalación basada en Windows es C:\Archivos de programa\VMware\Orchestrator.
 - b Configure la variable de entorno PATH haciendo que apunte a la carpeta bin de la instancia de Java JRE que se instaló con Orchestrator.
 - c Utilice el símbolo del sistema de Windows para ir hasta la carpeta bin en la carpeta de instalación de Orchestrator.
De forma predeterminada, la ruta de la carpeta bin es C:\Archivos de programa\VMware\Orchestrator\migration-cli\bin.
 - d Ejecute el comando export desde la línea de comandos.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Este comando combina los archivos de configuración de VMware vRealize Orchestrator y los complementos en un archivo de exportación.

Se crea un archivo con el nombre de archivo `orchestrator-config-export-orchestrator_ip_address-date_hour.zip` en la misma carpeta que la carpeta `migration-cli`.

- 3 Importe la configuración en la instancia de Orchestrator de destino.
 - a Inicie sesión en el centro de control como **raíz**.
 - b Abra **Exportar/importar configuración** en el centro de control y haga clic en la pestaña **Importar configuración**.
 - c Busque y seleccione el archivo .ZIP exportado desde la instancia de origen de Orchestrator.
 - d Introduzca la contraseña que utilizó al exportar la configuración.
Deje el campo en blanco si no ha exportado la configuración con una contraseña.
 - e Seleccione el tipo de importación.
 - f Si va a importar la configuración a un servidor externo de Orchestrator, elija si desea importar la configuración de la base de datos.

Nota Si los servidores de origen y de destino de Orchestrator no están configurados para utilizar la misma base de datos externa, deje sin marcar la casilla **Migrar configuración de base de datos**. Así, el esquema de base de datos no se actualiza a la versión más reciente. De lo contrario, el entorno de origen de Orchestrator deja de funcionar.

Debe configurar la base de datos que va a utilizar el Orchestrator de destino antes de la migración.

- g Haga clic en **IMPORTAR** para finalizar la migración.
Un mensaje indica que la configuración se ha importado correctamente. El servicio del servidor de Orchestrator de la instancia de Orchestrator de destino se reinicia automáticamente.
- 4 Si el vRealize Orchestrator de destino utiliza un servidor de proveedores de autenticación que sea distinto del que utiliza el Orchestrator de origen, importe en el almacén de confianza del Orchestrator de destino el certificado SSL del proveedor de autenticación que esté configurado para usarse.
 - a En la página **Certificados** del centro de control, haga clic en **Importar de URL**.
 - b Proporcione la dirección URL de la instancia de vRealize Automation o vSphere.

Un mensaje indica que la migración ha finalizado correctamente. El servicio del servidor de Orchestrator se reinicia automáticamente.

Pasos siguientes

Compruebe que Orchestrator esté configurado correctamente en la página **Validar configuración** del centro de control.

Migrar un vRealize Orchestrator 6.x externo en Windows a vRealize Automation 7.4

Después de actualizar vRealize Automation de la versión 6.x a la versión 7.4, puede migrar su Orchestrator 6.x externo existente instalado en Windows al servidor de Orchestrator que está integrado en vRealize Automation 7.4.

Nota Si tiene un entorno de vRealize Automation distribuido con varios nodos de Dispositivo de vRealize Automation, realice el procedimiento de migración únicamente en el nodo principal de vRealize Automation.

Requisitos previos

- Actualice su vRealize Automation a la versión 7.4. Para obtener más información, consulte *Actualización de vRealize Automation en Instalación o actualización de vRealize Automation*.
- Si la instancia de origen de Orchestrator utiliza un certificado de firma de paquetes SHA1, asegúrese de volver a generar el certificado mediante un algoritmo de firma más seguro. El algoritmo de firma recomendado es SHA2.
- Detenga el servicio del servidor de Orchestrator del Orchestrator externo.
- Haga una copia de seguridad de la base de datos, incluido el esquema de base de datos, del servidor externo de Orchestrator.

Procedimiento

- 1 Descargue la herramienta de migración desde el servidor de destino de Orchestrator.
 - a Inicie sesión en Dispositivo de vRealize Automation sobre SSH como **raíz**.
 - b Descargue el archivo `migration-tool.zip` que se encuentra en el directorio `/var/lib/vco/downloads`.
- 2 Exporte la configuración de Orchestrator desde el servidor de Orchestrator de origen.
 - a Configure la variable de entorno PATH haciendo que apunte a la carpeta `bin` de la instancia de Java JRE que se instaló con Orchestrator.
 - b Cargue la herramienta de migración al servidor de Windows en el que está instalado el Orchestrator externo.
 - c Extraiga el archivo descargado en la carpeta de instalación de Orchestrator.

La ruta predeterminada de la carpeta de instalación de Orchestrator en una instalación basada en Windows es `C:\Archivos de programa\VMware\Orchestrator`.

- d Ejecute como administrador el símbolo del sistema de Windows y desplácese hasta la carpeta bin en la carpeta de instalación de Orchestrator.

De forma predeterminada, la ruta de la carpeta bin es C:\Archivos de programa\VMware\Orchestrator\migration-cli\bin.

- e Ejecute el comando export desde la línea de comandos.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Este comando combina los archivos de configuración de VMware vRealize Orchestrator y los complementos en un archivo de exportación.

El archivo se crea en la misma carpeta que la carpeta migration-cli.

- 3 Migre la configuración exportada al servidor de Orchestrator que está integrado en vRealize Automation 7.4.

- a En el Dispositivo de vRealize Automation, detenga el servicio del servidor de Orchestrator y el servicio del centro de control del servidor integrado de vRealize Orchestrator.

```
service vco-server stop && service vco-configurator stop
```

- b Cargue el archivo de configuración exportado en el directorio /usr/lib/vco/tools/configuration-cli/bin de Dispositivo de vRealize Automation.

- c Cambie la propiedad del archivo de configuración de Orchestrator exportado.

```
chown vco:vco orchestrator-config-export-dirección_IP_orchestrator-fecha_hora.zip
```

- d Importe el archivo de configuración de Orchestrator en el servidor integrado de vRealize Orchestrator; para ello, ejecute el script vro-configure con el comando import.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-IP_dispositivo_orchestrator-fecha_hora.zip
```

- e Elimine todos los certificados del almacén de claves de la base de datos.

```
./vro-configuration.sh untrust --reset-db
```

- 4 Migre la base de datos a la base de datos interna de PostgreSQL; para ello, ejecute el script vro-configure con el comando db-migrate.

```
./vro-configure.sh db-migrate --sourceJdbcUrl URL_conexión_JDBC --sourceDbUsername
usuario_base_datos --sourceDbPassword contraseña_usuario_base_datos
```

Nota Ponga las contraseñas que contienen caracteres especiales entre comillas simples.

La *URL_conexión_JDBC* depende del tipo de base de datos que utiliza.

```
PostgreSQL: jdbc:postgresql://host:puerto/nombre_base_datos
```

```
MSSQL: jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\; if using SQL authentication and
MSSQL: jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\;domain=dominio\;useNTLMv2=TRUE if
using Windows authentication.
```

```
Oracle: jdbc:oracle:thin:@host:puerto:nombre_base_datos
```

La información de inicio de sesión a la base de datos predeterminada es:

| | |
|---|--------|
| <i>nombre_de_base_de_datos</i> | vmware |
| <i>usuario_de_base_de_datos</i> | vmware |
| <i>contraseña_de_usuario_de_base_de_datos</i> | vmware |

Ha migrado correctamente un vRealize Orchestrator 6.x externo instalado en Windows a una instancia de vRealize Orchestrator integrada en vRealize Automation 7.4.

Pasos siguientes

Configure el servidor integrado de vRealize Orchestrator. Consulte [Configure el servidor integrado de vRealize Orchestrator](#).

Migrar un dispositivo virtual vRealize Orchestrator 6.x externo a vRealize Automation 7.4

Después de actualizar el vRealize Automation desde la versión 6.x a la versión 7.4, puede migrar el dispositivo virtual Orchestrator 6.x externo al servidor de Orchestrator que está integrado en vRealize Automation 7.4.

Nota Si tiene un entorno de vRealize Automation distribuido con varios nodos de Dispositivo de vRealize Automation, realice el procedimiento de migración únicamente en el nodo principal de vRealize Automation.

Requisitos previos

- Actualice su vRealize Automation a la versión 7.4. Para obtener más información, consulte *Actualización de vRealize Automation en Instalación o actualización de vRealize Automation*.

- Si la instancia de origen de Orchestrator utiliza un certificado de firma de paquetes SHA1, asegúrese de volver a generar el certificado mediante un algoritmo de firma más seguro. El algoritmo de firma recomendado es SHA2.
- Detenga el servicio del servidor de Orchestrator del Orchestrator externo.
- Haga una copia de seguridad de la base de datos, incluido el esquema de base de datos, del servidor externo de Orchestrator.

Procedimiento

1 Descargue la herramienta de migración desde el servidor de destino de Orchestrator al de origen.

- a Inicie sesión en el dispositivo virtual vRealize Orchestrator 6.x sobre SSH como **raíz**.
- b En el directorio `/var/lib/vco`, ejecute el comando `scp` para descargar el archivo `migration-tool.zip`.

```
scp root@VRA-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
```

- c Ejecute el comando `unzip` para extraer el archivo de la herramienta de migración.

```
unzip migration-tool.zip
```

2 Exporte la configuración de Orchestrator desde el servidor de Orchestrator de origen.

- a En el directorio `/var/lib/vco/migration-cli/bin`, ejecute el comando `export`.

```
./vro-migrate.sh export
```

Este comando combina los archivos de configuración de VMware vRealize Orchestrator y los complementos en un archivo de exportación.

Se crea un archivo con el nombre de archivo `orchestrator-config-export-orchestrator_ip_address-date_hour.zip` en la carpeta `/var/lib/vco`.

3 Migre la configuración exportada al servidor de Orchestrator que está integrado en vRealize Automation 7.4.

- a Inicie sesión en Dispositivo de vRealize Automation sobre SSH como **raíz**.
- b Detenga el servicio del servidor de Orchestrator y el servicio del centro de control del servidor integrado de vRealize Orchestrator.

```
service vco-server stop && service vco-configurator stop
```

- c En el directorio `/usr/lib/vco/tools/configuration-cli/bin`, ejecute el comando `scp` para descargar el archivo de configuración exportado.

```
scp root@nombre_DNS_o_IP_orchestrator:/var/lib/vco/orchestrator-config-export-dirección_IP_orchestrator-fecha_hora.zip ./
```

- d Cambie la propiedad del archivo de configuración de Orchestrator exportado.

```
chown vco:vco orchestrator-config-export-dirección_IP_orchestrator-fecha_hora.zip
```

- e Importe el archivo de configuración de Orchestrator en el servidor integrado de vRealize Orchestrator; para ello, ejecute el script vro-configure con el comando import.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-IP_dispositivo_orchestrator-fecha_hora.zip
```

- 4 Si el servidor externo de Orchestrator desde el que desea migrar utiliza la base de datos integrada de PostgreSQL, edite los archivos de configuración de la base de datos.

- a En el archivo /var/vmware/vpostgres/current/pgdata/postgresql.conf, quite la marca de comentario de la línea listen_addresses.

- b Establezca los valores de listen_addresses con un carácter comodín (*).

```
listen_addresses = '*'
```

- c Anexe una línea al archivo /var/vmware/vpostgres/current/pgdata/pg_hba.conf.

```
host all all vra-va-ip-address/32 md5
```

Nota El archivo pg_hba.conf requiere el uso de un formato de prefijo CIDR en lugar de una dirección IP y una máscara de subred.

- d Reinicie el servicio del servidor de PostgreSQL.

```
service vpostgres restart
```

- 5 Migre la base de datos a la base de datos interna de PostgreSQL; para ello, ejecute el script vro-configure con el comando db-migrate.

```
./vro-configure.sh db-migrate --sourceJdbcUrl URL_conexión_JDBC --sourceDbUsername
usuario_base_datos --sourceDbPassword contraseña_usuario_base_datos
```

Nota Ponga las contraseñas que contienen caracteres especiales entre comillas simples.

La *URL_conexión_JDBC* depende del tipo de base de datos que utiliza.

PostgreSQL: jdbc:postgresql://host:puerto/nombre_base_datos

MSSQL: jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\; if using SQL authentication and
MSSQL: jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\;domain=dominio\;useNTLMv2=TRUE if
using Windows authentication.

Oracle: jdbc:oracle:thin:@host:puerto:nombre_base_datos

La información de inicio de sesión a la base de datos predeterminada es:

| | |
|---|--------|
| <i>nombre_de_base_de_datos</i> | vmware |
| <i>usuario_de_base_de_datos</i> | vmware |
| <i>contraseña_de_usuario_de_base_de_datos</i> | vmware |

- 6 Elimine todos los certificados del almacén de claves de la base de datos.

```
./vro-configure.sh untrust --reset-db
```

- 7 Reinstale los complementos de Orchestrator.
 - a Inicie sesión en el centro de control como **raíz**.
 - b Haga clic en **Solución de problemas**.
 - c Haga clic en **Forzar reinstalación de complementos**.
- 8 Inicie el servicio del servidor de Orchestrator.
- 9 Regrese a la configuración predeterminada de los archivos postgresql.conf y pg_hba.conf.
 - a Reinicie el servicio del servidor de PostgreSQL.

Ha migrado correctamente una instancia externa del dispositivo virtual vRealize Orchestrator 6.x a una instancia de vRealize Orchestrator integrada en vRealize Automation 7.4.

Pasos siguientes

Configure el servidor integrado de vRealize Orchestrator. Consulte [Configure el servidor integrado de vRealize Orchestrator](#).

Migrar un vRealize Orchestrator 7.x externo a vRealize Automation 7.4

Puede exportar la configuración de la instancia externa de Orchestrator e importarla al servidor de Orchestrator que está integrado en vRealize Automation.

Nota Si tiene varios nodos de Dispositivo de vRealize Automation, realice el procedimiento de migración únicamente en el nodo principal de vRealize Automation.

Requisitos previos

- Actualice su vRealize Automation a la versión 7.4. Para obtener más información, consulte *Actualización de vRealize Automation en Instalación o actualización de vRealize Automation*.
- Detenga el servicio del servidor de Orchestrator del Orchestrator externo.
- Haga una copia de seguridad de la base de datos, incluido el esquema de base de datos, del servidor externo de Orchestrator.

Procedimiento

- 1 Exporte la configuración del servidor externo de Orchestrator.
 - a Inicie sesión en el centro de control del servidor externo de Orchestrator como **raíz** o como **administrador**, según la versión de origen.
 - b Detenga el servicio del servidor de Orchestrator desde la página **Opciones de inicio** para prevenir cambios no deseados en la base de datos.
 - c Vaya a la página **Exportar o importar configuración**.
 - d En la página **Exportar configuración**, seleccione **Exportar configuración de servidor**, **Empaquetar complementos** y **Exportar configuraciones de complementos**.
- 2 Migre la configuración exportada a la instancia integrada de Orchestrator.
 - a Cargue el archivo de configuración de Orchestrator exportado en el directorio `/usr/lib/vco/tools/configuration-cli/bin` de Dispositivo de vRealize Automation.
 - b Inicie sesión en Dispositivo de vRealize Automation sobre SSH como **raíz**.
 - c Detenga el servicio del servidor de Orchestrator y el servicio del centro de control del servidor integrado de vRealize Orchestrator.

```
service vco-server stop && service vco-configurator stop
```

- d Importe el archivo de configuración de Orchestrator en el servidor integrado de vRealize Orchestrator; para ello, ejecute el script `vro-configure` con el comando `import`.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-  
IP_dispositivo_orchestrator-fecha_hora.zip
```

- 3 Si el servidor externo de Orchestrator desde el que desea migrar utiliza la base de datos integrada de PostgreSQL, edite los archivos de configuración de la base de datos.
 - a En el archivo `/var/vmware/vpostgres/current/pgdata/postgresql.conf`, quite la marca de comentario de la línea `listen_addresses`.
 - b Establezca los valores de `listen_addresses` con un carácter comodín (*).

```
listen_addresses = '*'
```

- c Anexe una línea al archivo `/var/vmware/vpostgres/current/pgdata/pg_hba.conf`.

```
host all all vra-va-ip-address/32 md5
```

Nota El archivo `pg_hba.conf` requiere el uso de un formato de prefijo CIDR en lugar de una dirección IP y una máscara de subred.

- d Reinicie el servicio del servidor de PostgreSQL.

```
service vpostgres restart
```

- 4 Migre la base de datos a la base de datos interna de PostgreSQL; para ello, ejecute el script `vro-configure` con el comando `db-migrate`.

```
./vro-configure.sh db-migrate --sourceJdbcUrl URL_conexión_JDBC --sourceDbUsername usuario_base_datos --sourceDbPassword contraseña_usuario_base_datos
```

Nota Ponga las contraseñas que contienen caracteres especiales entre comillas simples.

La `URL_conexión_JDBC` depende del tipo de base de datos que utiliza.

```
PostgreSQL: jdbc:postgresql://host:puerto/nombre_base_datos
```

```
MSSQL: jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\; if using SQL authentication and
MSSQL: jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\;domain=dominio\;useNTLMv2=TRUE if
using Windows authentication.
```

```
Oracle: jdbc:oracle:thin:@host:puerto:nombre_base_datos
```

La información de inicio de sesión a la base de datos predeterminada es:

| | |
|---|--------|
| <code>nombre_de_base_de_datos</code> | vmware |
| <code>usuario_de_base_de_datos</code> | vmware |
| <code>contraseña_de_usuario_de_base_de_datos</code> | vmware |

- 5 Elimine todos los certificados del almacén de claves de la base de datos.

```
./vro-configuration.sh untrust --reset-db
```

- 6 Reinstale los complementos de Orchestrator.
 - a Inicie sesión en el centro de control como **raíz**.
 - b Haga clic en **Solución de problemas**.
 - c Haga clic en **Forzar reinstalación de complementos**.
- 7 Inicie el servicio del servidor de Orchestrator.
- 8 Regrese a la configuración predeterminada de los archivos `postgresql.conf` y `pg_hba.conf`.
 - a Reinicie el servicio del servidor de PostgreSQL.

Ha migrado correctamente una instancia externa del servidor de Orchestrator a una instancia de vRealize Orchestrator integrada en vRealize Automation.

Pasos siguientes

Configure el servidor integrado de vRealize Orchestrator. Consulte [Configure el servidor integrado de vRealize Orchestrator](#).

Configure el servidor integrado de vRealize Orchestrator

Tras exportar una configuración externa de vRealize Orchestrator e importarla a vRealize Automation, debe configurar el servidor de vRealize Orchestrator integrado en vRealize Automation.

Requisitos previos

Migre la configuración del vRealize Orchestrator externo al interno.

Procedimiento

- 1 Inicie sesión como raíz en una sesión de símbolo del sistema en el dispositivo de vRealize Automation.
- 2 Inicie los servicios del servidor y el centro de control de vRealize Orchestrator:

```
service vco-configurator start && service vco-server start
```

- 3 Inicie sesión como raíz en el centro de control de vRealize Orchestrator integrado.

<https://vrealize-automation-appliance-FQDN:8283/vco-controlcenter/config>

Nota Puede omitir el siguiente paso cuando las versiones de vRealize Orchestrator internas y externas sean iguales.

- 4 En el centro de control, haga clic en **Validar configuración** y compruebe que vRealize Orchestrator se haya configurado correctamente.

- 5 En el centro de control, haga clic en **Certificados** y en **Certificado de firma de paquetes**, y genere un nuevo certificado de firma de paquetes.
- 6 En el centro de control, haga clic en **Configurar proveedor de autenticación**.
Tenant predeterminado y **Grupo de administradores** se establecen como los valores predeterminados `vsphere.local` y `vsphere.local\vcoadmins`. Cambie los valores predeterminados por los valores del entorno.
- 7 En la interfaz de administración de dispositivos de vRealize Automation, en **Servicios**, compruebe que `vco-server` aparezca como REGISTRADO.
- 8 Seleccione los servicios de vco del servidor externo de vRealize Orchestrator y haga clic en **Eliminar del registro**.

Pasos siguientes

- Importe todos los certificados de confianza del servidor externo de vRealize Orchestrator al almacén de confianza del servidor integrado de vRealize Orchestrator. Para obtener más información, consulte [Administrar certificados de Orchestrator](#).
- Una los nodos de réplica de vRealize Automation al clúster de vRealize Automation para sincronizar la configuración de vRealize Orchestrator.

Para obtener más información, consulte *Volver a configurar el vRealize Orchestrator integrado de destino para propiciar alta disponibilidad* en la *Instalación o actualización de vRealize Automation*.

Nota Las instancias de vRealize Orchestrator se agrupan en clústeres automáticamente y están disponibles para usarse.

- Reinicie el servicio de `vco-configurator` en todos los nodos del clúster.
- Actualice el endpoint de vRealize Orchestrator de manera que apunte al servidor integrado de vRealize Orchestrator que se ha migrado.
- Agregue el host de vRealize Automation y de IaaS al inventario del complemento vRealize Automation mediante la ejecución de los flujos de trabajo **Añadir un host de vRA** y **Añadir un host de IaaS**.

Actualizar una instancia integrada de vRealize Orchestrator para que confíe en certificados de vRealize Automation

Si actualiza o cambia los certificados de Dispositivo de vRealize Automation o IaaS, debe actualizar vRealize Orchestrator para que confíe en los certificados nuevos o actualizados.

Este procedimiento se aplica a todas las implementaciones de vRealize Automation que utilizan una instancia integrada de vRealize Orchestrator. Si utiliza una instancia externa de vRealize Orchestrator, consulte [Actualizar vRealize Orchestrator externo para que confíe en certificados de vRealize Automation](#).

Nota Este procedimiento restablece la configuración predeterminada de la autenticación de tenants y grupos. Si ha personalizado la configuración de autenticación, tenga en cuenta los cambios para poder volver a configurar la autenticación después de completar el procedimiento.

Consulte la documentación de vRealize Orchestrator para obtener información sobre la actualización y el reemplazo de certificados de vRealize Orchestrator.

Si reemplaza o actualiza los certificados de vRealize Automation sin completar este procedimiento, es posible que el centro de control de vRealize Orchestrator no sea accesible y que aparezcan errores en los archivos de log de vco-server y vco-configurator.

También puede haber problemas con la actualización de certificados si vRealize Orchestrator está configurado para autenticarse en un tenant y un grupo de vRealize Automation diferente. Consulte <https://kb.vmware.com/kb/2147612>.

Procedimiento

- 1 Detenga el servidor y los servicios del centro de control de vRealize Orchestrator.

```
service vco-server stop
service vco-configurator stop
```

- 2 Restablezca el proveedor de autenticación de vRealize Orchestrator.
 - a Ejecute el comando `/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication`.
 - b Elimine `/etc/vco/app-server/vco-registration-id`.
 - c Ejecutar `vcac-vami vco-service-reconfigure`
- 3 Inicie el servidor y los servicios del centro de control de vRealize Orchestrator.

```
service vco-server start
service vco-configurator start
```

Diferencias del centro de control entre Orchestrator externo e integrado

Algunos de los elementos de menú que están disponibles en el centro de control de un vRealize Orchestrator externo no se incluyen en la vista predeterminada del centro de control correspondiente a una instancia de Orchestrator integrado.

En el centro de control del servidor de Orchestrator integrado, algunas opciones están ocultas de forma predeterminada.

| Elemento de menú | Detalles |
|--|--|
| Licencias | El Orchestrator integrado está preconfigurado para usar vRealize Automation como proveedor de licencias. |
| Exportar o importar configuración | La configuración de Orchestrator integrado se incluye en los componentes de vRealize Automation exportados. |
| Configurar base de datos | El Orchestrator integrado utiliza la misma base de datos que vRealize Automation. |
| Programa de mejora de la experiencia del cliente | Puede unirse al Programa de mejora de la experiencia del cliente (CEIP) desde la interfaz de administración de dispositivos de vRealize Automation. Consulte el <i>Programa de mejora de la experiencia del cliente</i> en <i>Administración de vRealize Automation</i> . |

Otras opciones que están ocultas en la vista predeterminada del centro de control son el cuadro de texto de la **dirección del host** y el botón de **eliminación de registro** de la página **Configurar proveedor de autenticación**.

Nota Para conocer todas las opciones del centro de control de vRealize Orchestrator incorporadas en vRealize Automation, debe acceder a la página de administración avanzada de Orchestrator en la dirección https://vra-va-hostname.dominio_nombre_o_dirección_del_equilibrador_de_carga:8283/vco-controlcenter/#/?advanced y hacer clic en el botón F5 del teclado para actualizar la página.

Reconfigurar el endpoint de vRealize Automation en la instancia de vRealize Orchestrator de destino

Utilice el siguiente procedimiento para reconfigurar el endpoint de vRealize Automation en la instancia de vRealize Orchestrator de destino integrada.

Requisitos previos

- Haber migrado correctamente a la versión más reciente de vRealize Automation.
- Conéctese a la instancia de vRealize Orchestrator de destino mediante el cliente de vRealize Orchestrator. Para obtener información, consulte *Usar el cliente de VMware vRealize Orchestrator* en la documentación de [vRealize Orchestrator](#).

Procedimiento

- 1 Seleccione **Diseño** en el menú desplegable superior.
- 2 Haga clic en **Inventario**.
- 3 Expanda **vRealize Automation**.

- 4 Si ha realizado la migración desde un entorno mínimo, identifique los endpoints que contengan el nombre de dominio completo (Fully Qualified Domain Name, FQDN) del host del dispositivo de vRealize Automation de origen. Si ha realizado la migración desde un entorno de alta disponibilidad, identifique los endpoints que contengan el FQDN del equilibrador de carga del dispositivo de origen.

| Si encuentra endpoints que contengan el FQDN, siga estos pasos. | Si no encuentra endpoints que contengan el FQDN, siga estos pasos. |
|---|--|
| <ol style="list-style-type: none"> 1 Haga clic en Flujos de trabajo. 2 Haga clic en el botón Expandir para seleccionar Biblioteca > vRealize Automation > Configuración. 3 Siga uno de estos pasos. <ul style="list-style-type: none"> ■ Si ha realizado la migración desde un entorno mínimo, ejecute el flujo de trabajo Quitar un host de vRA para cada endpoint que contenga el FQDN del host de dispositivo de vRealize Automation de origen. ■ Si ha realizado la migración desde un entorno de alta disponibilidad, ejecute el flujo de trabajo Quitar un host de vRA para cada endpoint que contenga el FQDN del equilibrador de carga del dispositivo de origen. | <ol style="list-style-type: none"> 1 Haga clic en Recursos. 2 Haga clic en el icono de actualización en la barra de herramientas superior. 3 Haga clic en el botón Expandir para seleccionar Biblioteca > vCACCAFE > Configuración. 4 Siga uno de estos pasos. <ul style="list-style-type: none"> ■ Si ha realizado la migración desde un entorno mínimo, elimine todos los recursos con una propiedad URL que contenga el FQDN del host de dispositivo de vRealize Automation de origen. ■ Si ha realizado la migración desde un entorno de alta disponibilidad, elimine todos los recursos con una propiedad URL que contenga el FQDN del equilibrador de carga del dispositivo de vRealize Automation de origen. |

- 5 Haga clic en **Flujos de trabajo**.
- 6 Haga clic en el botón Expandir para seleccionar **Biblioteca > vRealize Automation > Configuración**.
- 7 Ejecute el flujo de trabajo **Añadir un host de vRA con un registro de componentes** para añadir el host del dispositivo de vRealize Automation de destino o, si migró desde una implementación de alta disponibilidad, el host con equilibrio de carga.

Reconfigurar un endpoint de infraestructura de vRealize Automation en el entorno de vRealize Orchestrator de destino

Utilice el siguiente procedimiento para reconfigurar el endpoint de infraestructura de vRealize Automation en la instancia de vRealize Orchestrator de destino integrada.

Requisitos previos

- Haber migrado correctamente a la versión más reciente de vRealize Automation.
- Conéctese a la instancia de vRealize Orchestrator de destino mediante el cliente de vRealize Orchestrator. Para obtener información, consulte *Usar el cliente de VMware vRealize Orchestrator* en la documentación de [vRealize Orchestrator](#).

Procedimiento

- 1 Seleccione **Diseño** en el menú desplegable superior.
- 2 Haga clic en **Inventario**.
- 3 Expanda **Infraestructura de vRealize Automation**.

- 4 Si ha realizado la migración desde un entorno mínimo, identifique los endpoints que contengan el nombre de dominio completo (Fully Qualified Domain Name, FQDN) del host de infraestructura de vRealize Automation de origen. Si ha realizado la migración desde un entorno de alta disponibilidad, identifique los endpoints que contengan el FQDN del equilibrador de carga del dispositivo de origen.

| Si encuentra endpoints que contengan el FQDN, siga estos pasos. | Si no encuentra endpoints que contengan el FQDN, siga estos pasos. |
|---|--|
| <ol style="list-style-type: none"> 1 Haga clic en Flujos de trabajo. 2 Haga clic en el botón Expandir para seleccionar Biblioteca > vRealize Automation > Administración de infraestructura > Configuración. 3 Siga uno de estos pasos. <ul style="list-style-type: none"> ■ Si ha realizado la migración desde un entorno mínimo, ejecute el flujo de trabajo Quitar un host de IaaS para cada endpoint que contenga el FQDN del host de infraestructura de vRealize Automation de origen. ■ Si ha realizado la migración desde un entorno de alta disponibilidad, ejecute el flujo de trabajo Quitar un host de IaaS para cada endpoint que contenga el FQDN del equilibrador de carga del host de infraestructura de vRealize Automation de origen. | <ol style="list-style-type: none"> 1 Haga clic en Recursos. 2 Haga clic en el icono de actualización en la barra de herramientas superior. 3 Haga clic en el botón Expandir para seleccionar Biblioteca > vCAC > Configuración. 4 Siga uno de estos pasos. <ul style="list-style-type: none"> ■ Si ha realizado la migración desde un entorno mínimo, elimine todos los recursos con una propiedad host que contenga el FQDN del host de infraestructura de vRealize Automation de origen. ■ Si ha realizado la migración desde un entorno de alta disponibilidad, elimine todos los recursos con una propiedad host que contenga el FQDN del equilibrador de carga del host de infraestructura de vRealize Automation de origen. |

- 5 Haga clic en **Flujos de trabajo**.
- 6 Haga clic en el botón Expandir para seleccionar **Biblioteca > vRealize Automation > Configuración**.
- 7 Ejecute el flujo de trabajo **Añadir el host de IaaS de un host de vRA** para añadir el host de infraestructura de vRealize Automation de destino o si ha realizado la migración desde un host con equilibrio de carga en una implementación de alta disponibilidad.

Instalar personalización de vRealize Orchestrator

Puede ejecutar un flujo de trabajo para instalar los stubs de flujo de trabajo de cambio de estado y los flujos de trabajo de operaciones del menú de vRealize Orchestrator personalizados.

Para obtener más información, consulte el tema de [instalación de personalización de vRealize Orchestrator](#).

Requisitos previos

Haber migrado correctamente a la versión más reciente de vRealize Automation.

Reconfigurar un endpoint de infraestructura de vRealize Orchestrator integrado en el entorno de vRealize Automation de destino

Cuando se migra desde un entorno de vRealize Automation 6.2.x, debe actualizar la dirección URL del endpoint de infraestructura que apunta al servidor de vRealize Orchestrator de destino integrado.

Requisitos previos

- La migración a vRealize Automation 7.4 se realiza correctamente.

- Inicie sesión en la consola de vRealize Automation de destino.
 - a Abra la consola de vRealize Automation usando el nombre de dominio completo del dispositivo virtual de destino: `https://vra-va-hostname.domain.name/vcac`.

En un entorno de alta disponibilidad, abra la consola usando el nombre de dominio completo del equilibrador de carga del dispositivo virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Inicie sesión como usuario administrador de IaaS.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoints > Endpoints**.
- 2 En la página Endpoints, seleccione el endpoint de vRealize Orchestrator y haga clic en **Editar**.
- 3 En el cuadro de texto Dirección, edite la URL del endpoint de vRealize Orchestrator.
 - Si ha migrado a un entorno mínimo, reemplace la URL del endpoint de vRealize Orchestrator por `https://vra-va-hostname.domain.name:443/vco`.
 - Si ha migrado a un entorno de alta disponibilidad, reemplace la URL del endpoint de vRealize Orchestrator por `https://vra-va-lb-hostname.domain.name:443/vco`.
- 4 Haga clic en **Aceptar**.
- 5 Ejecute manualmente una recopilación de datos en el endpoint de vRealize Orchestrator.
 - a En la página Endpoints, seleccione el endpoint de vRealize Orchestrator.
 - b Seleccione **Acciones > Recopilación de datos**.

Compruebe que la recopilación de datos es correcta.

Reconfigurar el endpoint de Azure en el entorno de vRealize Automation de destino

Tras la migración, debe volver a configurar el endpoint de Microsoft Azure.

Realice este procedimiento en cada endpoint de Azure.

Requisitos previos

- La migración a la versión más reciente de vRealize Automation 7.4 se realiza correctamente.
- Inicie sesión en la consola de vRealize Automation de destino.
 - a Abra la consola de vRealize Automation usando el nombre de dominio completo del dispositivo virtual de destino: `https://vra-va-hostname.domain.name/vcac`.

En un entorno de alta disponibilidad, abra la consola usando el nombre de dominio completo del equilibrador de carga del dispositivo virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Inicie sesión como usuario administrador de IaaS.

Procedimiento

- 1 Seleccione **Administración > Configuración de vRO > Endpoints**.
- 2 Seleccione un endpoint de Azure.
- 3 Haga clic en **Editar**.
- 4 Haga clic en **Detalles**.
- 5 En el cuadro de texto de **Secreto de cliente**, introduzca el secreto de cliente original.
- 6 Haga clic en **Finalizar**.
- 7 Repítalo para cada endpoint de Azure.

Migrar vRealize Automation Automation Application Services 6.2.x a 7.4

Puede utilizar la herramienta de migración de VMware vRealize Application Services para migrar los blueprints de servicios de aplicación y los perfiles de implementación existentes de VMware vRealize Application Services 6.2.x a vRealize Automation 7.4.

Requisitos previos

Haber migrado correctamente a la versión más reciente de vRealize Automation.

Procedimiento

- ◆ Haga lo siguiente para descargar la herramienta de migración de VMware vRealize Application Services.
 - a Haga clic en [Descargar VMware vRealize Automation](#).
 - b Seleccione **Controladores y herramientas > Herramienta de migración de VMware vRealize Application Services**.

Eliminar la base de datos de Microsoft SQL de IaaS de vRealize Automation original de destino

Tras completar la migración, puede eliminar la base de datos de IaaS original.

Requisitos previos

Haber migrado correctamente a la versión más reciente de vRealize Automation.

En el entorno migrado no se utiliza la base de datos original de Microsoft SQL de IaaS de vRealize Automation que creó cuando instaló el entorno de vRealize Automation de destino. Por lo tanto, puede eliminar esta base de datos original de IaaS de Microsoft SQL Server después de completar la migración.

Actualizar el contenido del menú de ubicación de centro de datos tras la migración

Después de la migración, debe añadir al menú desplegable **Ubicación** todas las ubicaciones de centro de datos personalizadas que falten.

Después de migrar a la versión más reciente de vRealize Automation, las ubicaciones de centro de datos del menú desplegable **Ubicación** en la página Recursos informáticos se revierten a la lista predeterminada. A pesar de que faltan ubicaciones de centro de datos personalizadas, todas las configuraciones de recursos informáticos se migran bien y la propiedad `Vrm.DataCenter.Location` no se ve afectada. Además, sigue existiendo la posibilidad de añadir esas ubicaciones de centro de datos personalizadas al menú **Ubicación**.

Requisitos previos

Migre a la versión más reciente de vRealize Automation.

Procedimiento

- ◆ Añada las ubicaciones de centro de datos que faltan al menú desplegable **Ubicación**. Consulte [Escenario: Añadir ubicaciones de centro de datos para implementaciones entre regiones](#).

Actualizar agentes de software a TLS 1.2

Después de migrar a vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 a 7.4, debe realizar varias tareas para actualizar los agentes de software del entorno de origen a Transport Layer Security (TLS) 1.2.

A partir de vRealize Automation 7.4, TLS 1.2 es el único protocolo TLS admitido para la comunicación de datos entre vRealize Automation y el navegador. Tras la migración, debe actualizar las plantillas de máquina virtual existentes desde el entorno de vRealize Automation 7.1 o 7.3, así como cualquier máquina virtual existente.

Actualizar las plantillas de máquinas virtuales del entorno de origen

Las plantillas existentes de vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 se deben actualizar después de completar la migración a 7.4 para que los agentes de software usen el protocolo TLS 1.2.

El agente invitado y el código de arranque del agente se deben actualizar en las plantillas del entorno de origen. Si está utilizando una opción de clon vinculado, puede que deba asignar de nuevo las plantillas con las máquinas virtuales recién creadas y sus snapshots.

Para actualizar las plantillas, complete estas tareas.

- 1 Inicie sesión en vSphere.
- 2 Convierta cada plantilla de vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 a una máquina virtual y encienda la máquina.
- 3 Importe el instalador de software adecuado y ejecute el instalador de software en cada máquina virtual.
- 4 Vuelva a convertir cada máquina virtual a una plantilla.

Utilice este procedimiento para ubicar los instaladores de software para Linux o Windows.

Requisitos previos

- [Aplicar una revisión de agente de software](#) si migró desde vRealize Automation 7.1 o 7.3 a 7.4.
- Migración correcta de vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 a la versión 7.4.

Procedimiento

- 1 Inicie un navegador y abra la página de presentación del dispositivo de vRealize Automation 7.4 con el nombre de dominio completo del dispositivo virtual: `https://vra-va-nombredelhost.dominio.nombre`.
- 2 Haga clic en la **página de agentes invitados y de software**.
- 3 Siga las instrucciones para los instaladores de software de Linux o Windows.

Pasos siguientes

[Identificar las máquinas virtuales que necesitan actualización del agente de software.](#)

Identificar las máquinas virtuales que necesitan actualización del agente de software

Puede utilizar el servicio de estado en la consola de vRealize Automation para identificar las máquinas virtuales que necesitan una actualización del agente de software a TLS 1.2.

A veces la revisión aplicada en el entorno de origen de vRealize Automation no actualiza todas las máquinas virtuales. Puede utilizar el servicio de estado para identificar las máquinas virtuales que todavía necesitan una actualización del agente de software a TLS 1.2. Todos los agentes de software en el entorno de destino deben actualizarse para realizar los procedimientos posteriores al aprovisionamiento.

Requisitos previos

- [Aplicar una revisión de agente de software](#) si migró desde vRealize Automation 7.1 o 7.3 a 7.4.
- Ha migrado correctamente vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 a 7.4.
- Ha iniciado sesión en vRealize Automation 7.4 en el dispositivo virtual principal.

Procedimiento

- 1 Haga clic en **Administración > Estado de mantenimiento**.
- 2 Haga clic en **Nueva configuración**.
- 3 En la página Detalles de la configuración, indique la información solicitada.

| Opción | Comentario |
|-------------|---|
| Nombre | Introduzca Verificación de agente de software . |
| Descripción | Añada una descripción opcional, por ejemplo, Buscar los agentes de software para actualización a TLS 1.2 . |
| Producto | Seleccione vRealize Automation 7.4.0. |
| Programar | Seleccione Ninguno. |

- 4 Haga clic en **Siguiente**.
- 5 En la página Seleccionar conjuntos de pruebas, seleccione **Pruebas de sistema de vRealize Automation** y **Pruebas de Tenant de vRealize Automation**.
- 6 Haga clic en **Siguiente**.

7 En la página Configurar parámetros, indique la información solicitada.

Tabla 1-84. Dispositivo virtual de vRealize Automation

| Opción | Descripción |
|--|--|
| Dirección de servidor web pública | <ul style="list-style-type: none"> Es la dirección URL base para el host del dispositivo de vRealize Automation en una implementación mínima. Por ejemplo, <code>https://va-host.domain/</code>. Es la dirección URL base para el equilibrador de carga de vRealize Automation en una implementación de alta disponibilidad. Por ejemplo, <code>https://load-balancer-host.domain/</code>. |
| Dirección de la consola de SSH | Nombre de dominio completo del dispositivo de vRealize Automation. Por ejemplo, <code>va-host.domain</code> . |
| Usuario de la consola de SSH | root |
| Contraseña de la consola de SSH | Contraseña de la raíz. |
| Tiempo máximo de respuesta del servicio (ms) | Acepte el valor predeterminado: 2000 |

Tabla 1-85. Tenant del sistema de vRealize Automation

| Opción | Descripción |
|-------------------------------------|-------------------------------|
| Administrador de tenant del sistema | administrador |
| Contraseña de tenant del sistema | Contraseña del administrador. |

Tabla 1-86. Supervisión de espacio en disco de vRealize Automation

| Opción | Descripción |
|--------------------------------------|------------------------------------|
| Porcentaje del umbral de advertencia | Acepte el valor predeterminado: 75 |
| Porcentaje de umbral crítico | Acepte el valor predeterminado: 90 |

Tabla 1-87. Tenant de vRealize Automation

| Opción | Descripción |
|---|--|
| Tenant en prueba | Tenant seleccionado para las pruebas. |
| Nombre de usuario del administrador de tejido | Nombre de usuario del administrador de tejido. Por ejemplo, <code>admin@va-host.local</code> . Nota Este administrador de tejido también debe tener un administrador de tenant y una función de administrador de IaaS en orden para que se ejecuten todas las pruebas. |
| Contraseña del administrador de tejido | Contraseña del administrador de tejido. |

8 Haga clic en **Siguiente**.

9 En la página Resumen, revise la información y haga clic en **Finalizar**.

Finalizó la configuración de comprobación del agente de software.

10 En la tarjeta de verificación Agente de software, haga clic en **Ejecutar**.

- 11 Una vez completada la prueba, haga clic en el centro de la tarjeta de verificación Agente de software.
- 12 En la página de resultados de verificación del agente de software, explore los resultados de la prueba y busque la prueba Comprobar versión del agente de software, en la columna Nombre. Si se produce un error en el resultado de la prueba, haga clic en el vínculo de la **causa** en la columna Causa para ver las máquinas virtuales que tienen un agente de software desactualizado.

Pasos siguientes

Si tiene máquinas virtuales con un agente de software desactualizado, consulte [Actualizar los agentes de software en vSphere](#).

Actualizar los agentes de software en vSphere

Puede actualizar los agentes de software obsoletos en vSphere a TLS 1.2 después de la migración mediante vRealize Automation Appliance Management.

Este procedimiento actualiza los agentes de software obsoletos en las máquinas virtuales del entorno de origen a TLS 1.2 y es obligatorio para la migración a vRealize Automation 7.4.

Requisitos previos

- [Aplicar una revisión de agente de software](#) si migró desde vRealize Automation 7.1 o 7.3 a 7.4.
- Migración correcta de vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 a la versión 7.4.
- Ha usado el servicio de estado para identificar los dispositivos virtuales con agentes de software obsoletos.

Procedimiento

- 1 En el dispositivo de vRealize Automation principal, inicie sesión en la Administración de dispositivos de vRealize Automation como **raíz** con la contraseña que introdujo al implementar el dispositivo de vRealize Automation.

Para un entorno de alta disponibilidad, abra Appliance Management en el dispositivo principal.

- 2 Haga clic en **Configuración de vRA > Agentes de software**.
- 3 Haga clic en **Activar/desactivar TLS 1.0, 1.1**.

El estado de TLS v1.0, v1.1 es HABILITADO.

- 4 En las credenciales del tenant, escriba la información solicitada para el dispositivo de origen vRealize Automation.

| Opción | Descripción |
|-------------------|---|
| Nombre de tenant | Nombre de tenant en el dispositivo de origen vRealize Automation. Nota El usuario de tenant debe tener la función de arquitecto de software asignada. |
| Nombre de usuario | Nombre de usuario del administrador de tenant en el dispositivo de origen vRealize Automation. |
| Contraseña | Contraseña de administrador de tenant. |

- 5 Haga clic en **Probar conexión**.

Si se establece una conexión, aparece un mensaje de confirmación.

- 6 En el dispositivo de origen, introduzca la dirección IP o el nombre de dominio totalmente cualificado del dispositivo de origen vRealize Automation.

Los dispositivos de origen y de destino deben usar las mismas credenciales de tenant.

- 7 Haga clic en **Enumerar lotes**.

Aparecerá la tabla de lista de opciones de lote.

- 8 Haga clic en **Mostrar**.

Aparece una tabla con una lista de las máquinas virtuales con agentes de software obsoletos.

- 9 Actualice el agente de software de las máquinas virtuales que estén en estado ACTUALIZABLE.

- Para actualizar el agente de software en una máquina virtual individual, haga clic en **Mostrar** para un grupo de máquinas virtuales, identifique la máquina virtual que desea actualizar y haga clic en **Ejecutar** para iniciar el proceso de actualización.
- Para actualizar al agente de software de un lote de máquinas virtuales, identifique el grupo que desea actualizar y haga clic en **Ejecutar** para iniciar el proceso de actualización.

Si tiene más de 200 máquinas virtuales para actualizar, puede controlar la velocidad del proceso de actualización por lotes; para ello, introduzca los valores de estos parámetros.

| Opción | Descripción |
|---------------------|---|
| Tamaño de lote | La cantidad de máquinas virtuales seleccionadas para la actualización por lotes. Puede cambiar este número para ajustar la velocidad de actualización. |
| Profundidad de cola | La cantidad de ejecuciones de actualización en paralelo que tienen lugar a la vez. Por ejemplo, 20. Puede cambiar este número para ajustar la velocidad de actualización. |

| Opción | Descripción |
|-----------------|--|
| Errores de lote | El recuento de errores de REST que hacen que el procesamiento por lotes se ralentice. Por ejemplo, si desea detener la actual actualización por lotes después de 5 errores para mejorar la estabilidad de la actualización, introduzca 5 en el campo de texto. |
| Fallos de lote | El número de actualizaciones fallidas del agente de software que hacen que el procesamiento por lotes se ralentice. Por ejemplo, si desea detener la actual actualización por lotes después de 5 errores para mejorar la estabilidad de la actualización, introduzca 5 en el campo de texto. |
| Sondeo de lote | Con qué frecuencia se sondea el proceso de actualización para comprobarlo. Puede cambiar este número para ajustar la velocidad de actualización. |

Si el proceso de actualización es demasiado lento o genera demasiadas actualizaciones incorrectas, puede ajustar estos parámetros para mejorar el rendimiento de la actualización.

Nota Al hacer clic en **Actualizar**, se borra la lista de lotes. No afecta el proceso de actualización. También se actualiza la información sobre si se ha establecido TLS 1.2 o no. Además, al hacer clic en **Actualizar**, también se realiza una comprobación de estado de los servicios de vRealize Automation. Si los servicios no se están ejecutando, el sistema muestra un mensaje de error y desactiva todos los otros botones de acción.

10 Haga clic en **Activar/desactivar TLS 1.0, 1.1**.

El estado de TLS v1.0, v1.1 es DESHABILITADO.

Actualizar agentes de software en Amazon Web Service o Azure

Puede actualizar manualmente los agentes de software obsoletos en Amazon Web Service (AWS) o Azure.

- Debe actualizar las propiedades de túnel especificadas en la reserva del servidor de vRealize Automation migrado.

Requisitos previos

- [Aplicar una revisión de agente de software](#) si migró desde vRealize Automation 7.1 o 7.3 a 7.4.
- Migración correcta de vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 a la versión 7.4.
- Un túnel de software está presente y se conoce la dirección IP de máquina virtual de túnel.

Procedimiento

- 1 Cree un archivo de nodo para cada nodo que se debe actualizar.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

2 Cree un archivo de plan para actualizar al agente de software en una máquina virtual de Linux o Windows.

- Modifique el archivo de parámetros de migración en `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}` para que contenga el valor de la dirección IP privada correspondiente al endpoint de AWS o Azure.

```
"key": "ipAddress",
  "value": {
    "type": "string",
    "value": "<$PrivateIp:$PrivatePort>"
  }
}
```

- Utilice este comando para actualizar una máquina de Linux.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL Software.LinuxAgentUpdate74 --
source_cloud_provider azure
```

- Utilice este comando para actualizar una máquina de Windows.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW Software.WindowsAgentUpdate74 --
source_cloud_provider azure
```

- Este comando ejecuta el archivo de plan.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

- 3 Utilice este comando para actualizar el agente de software con el archivo de nodo del paso 1 y luego con el archivo de plan del paso 2.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action plan_batch -S <$SourceVRAServer>
```

Como alternativa, puede utilizar este comando para ejecutar un nodo a la vez desde el archivo del nodo proporcionando un índice de nodos.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

Cuando realice este procedimiento, puede seguir los registros del dispositivo virtual de vRealize Automation y la máquina de host para ver el proceso de actualización del agente de servidor.

Tras la actualización, el proceso de actualización importa un script de actualización de software para Windows o Linux en el dispositivo virtual de vRealize Automation 7.4. Puede iniciar sesión en el host de dispositivo virtual de vRealize Automation para asegurarse de que el componente de software se ha importado correctamente. Después de importar el componente, se envía una actualización de software al evento Broker Service (EBS) anterior para retransmitir los scripts de actualización de software a las máquinas virtuales identificadas. Cuando la actualización y los agentes de software nuevos estén operativos, se enlazan al nuevo dispositivo virtual de vRealize Automation mediante el envío de una solicitud de ping.

Nota Archivos de registro útiles

- Salida de Catalina para instancia de origen de vRealize Automation: `/var/log/vcac/catalina.out`. En este archivo, puede ver las solicitudes de actualización que se envían al realizar las migraciones de agente. Esta actividad equivale a ejecutar una solicitud de aprovisionamiento de software.
- Salida de Catalina para instancia de destino de vRealize Automation: `/var/log/vcac/catalina.out`. En este archivo, verá las máquinas virtuales migradas informar aquí de sus solicitudes de ping para que incluyan los números de versión 7.4.0-SNAPSHOT. Puede hacerlas corresponder comparando los nombres de tema de EBS, por ejemplo, `sw-agent-UUID`.
- Carpeta de actualización del agente en el archivo de registro de actualización principal de máquina de destino
vRealize Automation: `/var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`. Puede seguir este archivo para ver qué operación de actualización está en curso.

- Registros individuales disponibles en las carpetas de tenant: `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`. Aquí se enumeran los nodos individuales como archivos de lote con errores y extensiones en curso.
- Máquinas virtuales migradas: `/opt/vmware-appdirector/agent/logs/darwin*.log`. Puede detectar esta ubicación que debería mostrar una lista con las solicitudes de actualización de software que se reciben, así como el posterior reinicio del agente `agent_bootstrap + software`.

Cambiar la configuración del diccionario de propiedades después de la migración

Después de la migración de vRealize Automation 6.2.x, establezca que las propiedades de tipo de control `Label` del diccionario de propiedades no sean reemplazables en los blueprints.

El control `Label` en el diccionario de propiedades de vRealize Automation 6.2.x no existe en vRealize Automation 7.x. Durante la migración, el control `Label` se traduce en un control de tipo `TextBox` en el diccionario de propiedades migrado.

Después de la migración, establezca las propiedades afectadas como no reemplazables, ya sea manualmente en el diccionario de propiedades de vRealize Automation o mediante las capacidades de importación y exportación.

Validación del entorno de destino de vRealize Automation 7.4

Puede comprobar que todos los datos se migraron correctamente al entorno de vRealize Automation de destino.

Requisitos previos

- Migre a la versión más reciente de vRealize Automation.
- Inicie sesión en la consola de vRealize Automation de destino.
 - a Abra la consola de vRealize Automation usando el nombre de dominio completo del dispositivo virtual de destino: `https://vra-va-hostname.domain.name/vcac`.

En un entorno de alta disponibilidad, abra la consola usando el nombre de dominio completo del equilibrador de carga del dispositivo virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Inicie sesión con el nombre de usuario y la contraseña del administrador de tenants.

Procedimiento

- 1 Seleccione **Infraestructura > Máquinas administradas** y compruebe que todas las máquinas virtuales administradas estén presentes.
- 2 Haga clic en **Recursos informáticos**, seleccione los endpoints, y haga clic en **Recopilación de datos**, **Solicitar ahora** y **Actualizar** para comprobar que los endpoints funcionan.
- 3 Haga clic en **Diseño** y, en la página **Blueprints**, compruebe los elementos de cada blueprint.
- 4 Haga clic en **XaaS** y compruebe el contenido de **Recursos personalizados**, **Asignaciones de recursos**, **Blueprints XaaS** y **Acciones personalizadas**.

- 5 Seleccione **Administración > Administración de catálogos** y compruebe el contenido de **Servicios, Elementos del catálogo, Acciones y Autorizaciones**.
- 6 Seleccione **Elementos > Implementaciones** y compruebe los detalles de las máquinas virtuales aprovisionadas.
- 7 En la página Implementaciones, seleccione una máquina virtual aprovisionada y apagada, seleccione **Acciones > Encender**, haga clic en **Enviar** y después en **Aceptar**. Compruebe que la máquina virtual se enciende correctamente.
- 8 Haga clic en **Catálogo** y solicite un nuevo elemento del catálogo.
- 9 En la pestaña **General**, escriba la información de la solicitud.
- 10 Haga clic en el icono de máquina, acepte la configuración predeterminada, haga clic en **Enviar** y luego en **Aceptar**.
- 11 Compruebe que la solicitud finaliza correctamente.

Solución de problemas de migración

Los temas que explican cómo resolver problemas de migración ofrecen soluciones a aquellos problemas que podría experimentar al migrar vRealize Automation.

Versión de PostgreSQL causa un error

Un entorno de vRealize Automation 6.2.x de origen que contiene una base de datos de PostgreSQL actualizada bloquea el acceso del administrador.

Problema

Si vRealize Automation 6.2.x usa una base de datos de PostgreSQL actualizada, un administrador debe añadir una entrada en el archivo `pg_hba.conf` que proporcione acceso a esta base de datos desde vRealize Automation.

Solución

- 1 Abra el archivo `pg_hba.conf`.
- 2 Para otorgar acceso a esta base de datos, añada la siguiente entrada.

```
host all vcac-database-user vra-va-ip trust-method
```

En algunas máquinas virtuales no se crea una implementación durante la migración

Para las máquinas virtuales con el estado ausente en el momento de la migración no se crea una implementación correspondiente en el entorno de destino.

Problema

Si una máquina virtual tiene el estado ausente en el entorno de origen durante la migración, no se creará una implementación correspondiente en el entorno de destino.

Solución

- ◆ Si una máquina virtual sale del estado ausente después de la migración, se podrá importar en bloque a la implementación de destino.

ubicaciones de logs de migración

Puede solucionar problemas de validación o migración consultando los logs que registran el proceso de migración.

Tabla 1-88. Dispositivo de vRealize Automation de origen

| Log | Ubicación |
|-----------------------------|--|
| Log de creación del paquete | /var/log/vmware/vcac/migration-package.log |

Tabla 1-89. Dispositivo de vRealize Automation de destino

| Log | Ubicación |
|--|--|
| Log de migración | /var/log/vmware/vcac/migrate.log |
| Log de ejecución de la migración | /var/log/vmware/vcac/mseq.migration.log |
| Log de salida de ejecución de la migración | /var/log/vmware/vcac/mseq.migration.out.log |
| Log de ejecución de validación | /var/log/vmware/vcac/mseq.validation.log |
| Log de salida de ejecución de validación | /var/log/vmware/vcac/mseq.validation.out.log |

Tabla 1-90. Nodos de la infraestructura de vRealize Automation de destino

| Log | Ubicación |
|-------------------|--|
| Log de migración | C:\Archivos de programa (x86)\VMware\VCAC\InstallLogs- YYYYMMDDHHMMXX\Migrate.log |
| Log de validación | C:\Archivos de programa (x86)\VMware\VCAC\InstallLogs- YYYYMMDDHHMMXX\Validate.log |

Los elementos del catálogo aparecen en el catálogo de servicios después de la migración, pero no están disponibles para solicitarse

Los elementos del catálogo que utilizan ciertas definiciones de propiedad de versiones anteriores aparecen en el catálogo de servicios, pero no están disponibles para solicitarlos después de migrar a la última versión de vRealize Automation.

Problema

Si migró desde 6.2.x o una versión anterior, y tenía definiciones de propiedad con estos tipos de control o atributos, estos elementos están ausentes en las definiciones de propiedad y cualquier elemento de catálogo que usa las definiciones no funciona del modo en que lo hacía antes de la migración.

- Tipos de control. Casilla de verificación o vínculo.
- Atributos. Relación, expresiones regulares o diseños de propiedades.

Causa

En vRealize Automation 7.0 y versiones posteriores, las definiciones de propiedad ya no usan estos elementos. Debe recrear la definición de propiedades o configurarla para que use una acción de script de vRealize Orchestrator en lugar de los atributos o tipos de control integrados.

Migre el tipo de control o los atributos a vRealize Automation 7.x utilizando una acción de script.

Solución

- 1 En vRealize Orchestrator, cree una acción de script que devuelva los valores de propiedad. La acción debe devolver un tipo simple. (Por ejemplo, devolver cadenas, enteros u otros tipos admitidos). La acción puede tomar las otras propiedades de las que depende como parámetro de entrada.
- 2 En la consola de vRealize Automation, configure la definición de productos.
 - a Seleccione **Administración > Diccionario de propiedades > Definiciones de propiedades**.
 - b Seleccione la definición de propiedades y haga clic en **Editar**.
 - c En el menú desplegable Mostrar recomendación, seleccione **Lista desplegable**.
 - d En el menú desplegable Valores, seleccione **Valores externos**.
 - e Seleccione la acción de script.
 - f Haga clic en **Aceptar**.
 - g Configure los parámetros de entrada que se incluyen en la acción de script. Para preservar la relación existente, enlace el parámetro a la otra propiedad.
 - h Haga clic en **Aceptar**.

Botones de opción de Recopilación de datos deshabilitados en vRealize Automation

Después de migrar de vRealize Automation 6.2.x a la versión 7.x, la página Recursos informáticos en la instancia de vRealize Automation de destino contiene botones de opción deshabilitados en Recopilación de datos.

Causa

Si instala un agente en el entorno de origen que apunta a un endpoint, e instala un agente en el entorno de destino que apunta al mismo endpoint, pero el agente tiene un nombre diferente, puede ejecutar una conexión de prueba al endpoint como administrador en el entorno de destino. Sin embargo, si inicia sesión en vRealize Automation en el entorno de destino como un administrador de tejido, se deshabilitan los botones de opción de la página Recursos informáticos en Recopilación de datos.

Solución

Puede evitar esta situación dando al agente instalado en el entorno de destino el mismo nombre que el del agente instalado en el entorno de origen.

Solucionar problemas de actualización del agente de software

Cuando se utiliza la administración de dispositivos de vRealize Automation para actualizar los agentes de software, es posible revisar los archivos de log para identificar la causa de cualquier problema que se produzca.

Problema

Podría experimentar algunos problemas al actualizar los agentes de software. Si observa los archivos de log durante el proceso de actualización del agente de software, podrá identificar dónde existe un problema.

Nota

Logs del servidor

- Vaya al archivo `updateSoftwareAgents.log` en el servidor para observar el proceso: `/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`.
- Vaya al archivo `catlaina.out` en el dispositivo de destino para ver qué agentes de software se están completando correctamente: `/var/log/vcac/catalina.out`.

Busque una cadena como "ping" que se notifica para 7.4.0-SNAPSHOT.

Puede encontrar información adicional en estas ubicaciones.

- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.plan`
- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.log`
- `/var/cache/vcac/agentupdate/sqa/UUID/UUID.log` (por sistema operativo)

Antes de iniciar una actualización principal por lotes, siempre debe realizar una actualización de prueba del agente de software del dispositivo virtual. Para obtener una descripción general del proceso:

- Observe la primera solicitud realizada al dispositivo virtual de destino para identificar las versiones del agente.
- Fíjese en la solicitud realizada al dispositivo virtual de origen para la actualización.
- Observe los agentes que informan sobre la nueva versión 7.4 en el dispositivo virtual de destino.
- Entre estos eventos, observe el archivo `updateSoftwareAgents.log` situado en `/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`

Nota

Logs de cliente

Los logs del agente de Linux se encuentran en la carpeta de logs del agente `appdirector`: `/opt/vmware-appdirector/agent/logs/*.log`

Podrían aparecer errores de log como estos, los cuales son temporales debido a que las colas de EBS se desactivan y se activan durante el proceso de actualización.

```
Feb 15 2018 16:54:10.105 ERROR [EventPoller-sw-agent-0ad2418d-5b42-4231-a839-a05dd618e43e] []
com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler - Error while polling
events for subscription '{}'
```

org.springframework.web.client.HttpClientErrorException: 404 Not Found

at

org.springframework.web.client.DefaultResponseErrorHandler.handleError(DefaultResponseErrorHandler.java:91) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.handleResponse(RestTemplate.java:641) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.execute(RestTemplate.java:557) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.exchange(RestTemplate.java:503) ~[nobel-agent.jar:na]

at

com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler.pollEvents(RestEventSubscribeHandler.java:297) ~[nobel-agent.jar:na]

at com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler\$EventPoller.run(RestEventSubscribeHandler.java:329) ~[nobel-agent.jar:na]