

Instalación y configuración de VMware vRealize Orchestrator

12 de agosto de 2021
vRealize Orchestrator 8.5

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

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

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

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

Copyright © 2008-2021 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Instalación y configuración de VMware vRealize Orchestrator 6

- 1 Introducción a VMware vRealize Orchestrator 7**
 - Funciones clave de la plataforma de Orchestrator 7
 - Funciones de usuario de vRealize Orchestrator 10
 - Arquitectura de vRealize Orchestrator 11
 - vRealize Orchestrator Plug-ins 12
- 2 Requisitos del sistema de vRealize Orchestrator 13**
 - Componentes predeterminados de Appliance 13
 - Requisitos de hardware 14
 - Valores máximos de escalabilidad 14
 - Requisitos de red 14
 - Puertos y endpoints 15
 - Compatibilidad con navegadores 15
 - Compatibilidad con la internacionalización 16
- 3 Configurar componentes de vRealize Orchestrator 17**
 - Configuración de vCenter Server 17
 - Métodos de autenticación 18
- 4 Instalar vRealize Orchestrator 19**
 - Descargar e implementar vRealize Orchestrator Appliance 19
 - Encender vRealize Orchestrator Appliance y abrir la página de inicio 21
 - Habilitar o deshabilitar el acceso SSH a vRealize Orchestrator Appliance 22
- 5 Configuración inicial 23**
 - Configurar un servidor de vRealize Orchestrator independiente 23
 - Configurar un servidor de vRealize Orchestrator independiente con la autenticación de vRealize Automation 23
 - Configurar un servidor de vRealize Orchestrator independiente con la autenticación de vSphere 25
 - Habilitar funciones de vRealize Orchestrator con licencias 27
 - Conexión con una base de datos de vRealize Orchestrator 28
 - Administrar certificados 28
 - Administrar certificados de vRealize Orchestrator 29
 - Generar un certificado TLS personalizado para vRealize Orchestrator 29
 - Establecer un certificado TLS personalizado para vRealize Orchestrator 30

Importar un certificado de confianza con el centro de control	33
Configurar los complementos de vRealize Orchestrator	33
Administrar complementos de vRealize Orchestrator	34
Instalar o actualizar un complemento de vRealize Orchestrator	34
Eliminar un complemento	35
Alta disponibilidad de vRealize Orchestrator	35
Valores máximos de escalabilidad	36
Configurar un clúster de vRealize Orchestrator	36
Eliminar un nodo de clúster de vRealize Orchestrator	38
Escalar horizontalmente una implementación de vRealize Orchestrator independiente	39
Supervisar un clúster de vRealize Orchestrator	40
Configurar el programa de mejora de la experiencia de cliente	41
Categorías de información que recibe VMware	41
Unirse al programa de mejora de la experiencia de cliente o abandonarlo	41
6 Usar los servicios de API de vRealize Orchestrator	43
Administrar certificados SSL a través de API de REST	43
Eliminar un certificado TLS mediante la API de REST	44
Importar certificados TLS mediante la API de REST	44
Creación de un almacén de claves mediante la API de REST	46
Eliminación de un almacén de claves mediante la API de REST	46
Adición de una clave mediante la API de REST	47
7 Opciones de configuración adicionales	48
Volver a configurar la autenticación	48
Cambiar el proveedor de autenticación	48
Cambiar los parámetros de autenticación	49
Configurar las propiedades de ejecución de los flujos de trabajo	49
Archivos de registro de vRealize Orchestrator	50
Persistencia del registro	50
Configuración de registros de vRealize Orchestrator	51
Configurar la integración de registro con vRealize Log Insight	52
Crear o sobrescribir una integración de syslog en vRealize Orchestrator	52
Eliminar una integración de syslog en vRealize Orchestrator	54
Habilitar el registro de depuración de Kerberos	54
Habilitar las extensiones de Opentracing y Wavefront	55
Configurar la extensión de Opentracing	56
Configurar la extensión de Wavefront	57
Habilitar la sincronización de hora de vRealize Orchestrator	58
Desactivar la sincronización de hora vRealize Orchestrator	59
Configurar CIDR de Kubernetes de vRealize Orchestrator	60

Actualizar la configuración de DNS para vRealize Orchestrator 61

8 Casos prácticos de configuración y solución de problemas 63

Comprobar el número de compilación del servidor de vRealize Orchestrator 63

Configurar el complemento de vRealize Orchestrator para vSphere Web Client 64

Cancelar flujos de trabajo en ejecución 65

Habilitar la depuración del servidor de vRealize Orchestrator 65

Cambiar el tamaño de los discos de vRealize Orchestrator Appliance 67

Cómo ampliar el tamaño de la memoria de pila del servidor de vRealize Orchestrator 68

Recuperación ante desastres de vRealize Orchestrator mediante Site Recovery Manager 69

Configurar máquinas virtuales para vSphere Replication 70

Crear grupos de protección 70

Crear un plan de recuperación 73

Organizar planes de recuperación en carpetas 74

Editar un plan de recuperación 74

9 Establecimiento de las propiedades del sistema 76

Establecer el acceso al sistema de archivos del servidor para flujos de trabajo y acciones 76

Reglas del archivo js-io-rights.conf que permiten el acceso de escritura al sistema de vRealize Orchestrator 76

Establecer el acceso al sistema de archivos del servidor para flujos de trabajo y acciones 77

Establecer el acceso a los comandos del sistema operativo para los flujos de trabajo y las acciones 78

Establecer acceso de JavaScript a clases de Java 79

Establecer la propiedad de tiempo de espera personalizado 80

Agregar un conector JDBC para el complemento SQL de vRealize Orchestrator 81

10 Pasos a seguir 83

Instalación y configuración de VMware vRealize Orchestrator

Instalación y configuración de VMware vRealize Orchestrator proporciona información e instrucciones sobre cómo instalar y configurar VMware® vRealize Orchestrator.

Público objetivo

Esta información está destinada a administradores de vSphere con conocimientos avanzados, así como a administradores del sistema con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Introducción a VMware vRealize Orchestrator

1

VMware vRealize Orchestrator es una plataforma de desarrollo y automatización que proporciona una biblioteca de flujos de trabajo extensibles para crear y ejecutar procesos automatizados configurables que permitan administrar los productos de VMware y tecnologías de terceros.

vRealize Orchestrator automatiza las tareas operativas y de administración de las aplicaciones de VMware y de terceros, como los procedimientos de los departamentos de servicios, los sistemas de administración de cambios y los sistemas de administración de activos de TI.

Este capítulo incluye los siguientes temas:

- [Funciones clave de la plataforma de Orchestrator](#)
- [Funciones de usuario de vRealize Orchestrator](#)
- [Arquitectura de vRealize Orchestrator](#)
- [vRealize Orchestrator Plug-ins](#)

Funciones clave de la plataforma de Orchestrator

vRealize Orchestrator se compone de tres capas: una plataforma de orquestación que proporciona las características comunes necesarias para una herramienta de orquestación; una arquitectura de complemento para integrar el control de los subsistemas y una biblioteca de flujos de trabajo. vRealize Orchestrator es una plataforma abierta que se puede ampliar con nuevos complementos y contenido, y que se puede integrar en arquitecturas más grandes a través de una API de REST.

vRealize Orchestrator incluye varias características clave que ayudan a ejecutar y administrar flujos de trabajo.

Persistencia

La base de datos PostgreSQL de nivel de producción se utiliza para almacenar información relevante, como procesos, estados de flujo de trabajo y la configuración de vRealize Orchestrator.

Administración central

vRealize Orchestrator proporciona una herramienta centralizada para administrar los procesos. La plataforma basada en servidor de aplicaciones, con un historial de versiones completo, puede almacenar scripts y primitivos relacionados con los procesos en la misma ubicación. De esta forma, se evitan los scripts sin versiones y se controlan los cambios en los servidores.

Puntos de comprobación

Todos los pasos de un flujo de trabajo se guardan en la base de datos, lo que evita la pérdida de datos en caso de tener que reiniciar el servidor. Esta función resulta especialmente útil para procesos de larga ejecución.

Centro de control

El centro de control es un portal basado en la web que aumenta la eficiencia administrativa de las instancias de vRealize Orchestrator al proporcionar una interfaz administrativa centralizada para operaciones de tiempo de ejecución, supervisión de flujos de trabajo y correlación entre las ejecuciones de flujo de trabajo y los recursos del sistema.

Control de versiones

Un historial de versiones está asociado a todos los objetos de la plataforma de vRealize Orchestrator. El historial de versiones resulta útil para la administración de cambios básicos cuando se distribuyen procesos a las ubicaciones o las fases del proyecto.

Integración de Git

Con vRealize Orchestrator Client, puede integrar un repositorio Git para mejorar aún más la versión y el control de origen del contenido de vRealize Orchestrator. Con Git, puede administrar el desarrollo de flujos de trabajo en varias instancias de vRealize Orchestrator. Consulte *Usar Git con el cliente de vRealize Orchestrator* en la guía *Uso del cliente de VMware vRealize Orchestrator*.

Motor de creación de scripts

El motor de JavaScript Rhino de Mozilla permite generar bloques de creación para la plataforma de vRealize Orchestrator Client. El motor de creación de scripts se mejora mediante un control básico de versiones, la comprobación de tipos de variables, la administración de espacio de nombres y el control de excepciones. El motor se puede utilizar en los siguientes bloques de creación:

- Acciones
- Flujos de trabajo
- Políticas

Motor de flujo de trabajo

El motor de flujo de trabajo permite automatizar los procesos empresariales. Utiliza los objetos siguientes para crear una automatización de procesos detallada en los flujos de trabajo:

- Flujos de trabajo y acciones que proporciona vRealize Orchestrator Client.
- Bloques de creación personalizados creados por el cliente.
- Objetos que los complementos agregan a vRealize Orchestrator Client.

Los usuarios, otros flujos de trabajo, los programas o las políticas pueden iniciar flujos de trabajo.

Motor de políticas

Puede utilizar el motor de directivas para supervisar y generar eventos con el fin de reaccionar ante los cambios de condiciones en el servidor de vRealize Orchestrator Client o una tecnología conectada. Las políticas pueden agregar eventos desde la plataforma o los complementos, lo que permite administrar los cambios de condiciones en cualquiera de las tecnologías integradas.

vRealize Orchestrator Client

Cree, ejecute, edite y supervise flujos de trabajo con el vRealize Orchestrator Client. También puede usar el vRealize Orchestrator Client para administrar elementos de acción, configuración, política y recursos. Consulte *Usar el cliente de vRealize Orchestrator*.

Desarrollo y recursos

La página de destino de vRealize Orchestrator proporciona acceso rápido a los recursos para ayudarlo a desarrollar sus propios complementos, para su uso en vRealize Orchestrator. También encontrará información sobre el uso de la API de REST de vRealize Orchestrator para enviar solicitudes al servidor de vRealize Orchestrator.

Seguridad

vRealize Orchestrator proporciona las siguientes funciones avanzadas de seguridad:

- Infraestructura de clave pública (PKI) para firmar y cifrar contenido importado y exportado entre servidores.
- Administración de derechos digitales (DRM) para controlar cómo se puede visualizar, editar y redistribuir el contenido.
- Capa de seguridad de confianza (Transport Layer Security, TLS) para proporcionar comunicaciones cifradas entre el vRealize Orchestrator Client y el servidor de vRealize Orchestrator, así como acceso HTTPS al front-end web.
- Administración de derechos de acceso avanzados para proporcionar control sobre el acceso a los procesos y los objetos que manipulan.

Cifrado

vRealize Orchestrator utiliza un estándar de cifrado avanzado compatible con FIPS (AES) con una clave de cifrado de 256 bits para el cifrado de cadenas. La clave de cifrado se genera aleatoriamente y es única en los dispositivos que no forman parte de un clúster. Todos los nodos de un clúster comparten una clave de cifrado.

Funciones de usuario de vRealize Orchestrator

vRealize Orchestrator proporciona diferentes herramientas e interfaces basadas en las responsabilidades específicas de las funciones de usuarios globales. En vRealize Orchestrator, puede tener usuarios que tengan todos los derechos, que sean parte del grupo de administradores (**administradores**), desarrolladores (**diseñadores de flujos de trabajo**), usuarios de solución de problemas (**visualizadores**) y usuarios con acceso limitado.

Las funciones de usuario de vRealize Orchestrator se administran en el menú **Administración de funciones** de vRealize Orchestrator Client. Para obtener más información sobre cómo configurar funciones de usuario en vRealize Orchestrator Client, consulte *Asignar funciones en el cliente de vRealize Orchestrator* en la guía *Uso del cliente de VMware vRealize Orchestrator*.

Nota En el caso de las implementaciones de vRealize Orchestrator autenticadas con vRealize Automation o que usan una licencia de vRealize Automation, las funciones de usuario se asignan con el servicio de administración de acceso e identidades de la plataforma de vRealize Automation. Consulte *Configurar funciones del cliente de vRealize Orchestrator en vRealize Automation* en *Uso del cliente de VMware vRealize Orchestrator*.

Función de usuario	Descripción
Administrador	<p>Este usuario tiene acceso completo a todas las capacidades y el contenido de la plataforma de vRealize Orchestrator, incluido el contenido creado por grupos específicos. Las responsabilidades del usuario administrador principal incluyen:</p> <ul style="list-style-type: none"> ■ Instalar y configurar vRealize Orchestrator. ■ Agregar usuarios al vRealize Orchestrator Client, asignar funciones, y crear y eliminar grupos. Consulte <i>Crear grupos en el cliente de vRealize Orchestrator</i> en <i>Uso del cliente de VMware vRealize Orchestrator</i>. ■ Crear una integración con un repositorio de Git para los desarrolladores en su entorno de vRealize Orchestrator. Consulte <i>Configurar una conexión con un repositorio de Git</i> en <i>Uso del cliente de VMware vRealize Orchestrator</i>. ■ Solucionar problemas de su entorno de vRealize Orchestrator mediante funciones como la validación de flujos de trabajo y la depuración de scripts de flujos de trabajo.
Visualizador	<p>Este usuario tiene acceso de solo lectura a todas las instancias de vRealize Orchestrator Client, incluidos todos los grupos y el contenido del grupo. Este usuario puede ver, pero no puede crear, editar o ejecutar contenido ni exportar ejecuciones de flujos de trabajo, registros de ejecución de flujos de trabajo o paquetes. Los visualizadores no están limitados por permisos de grupo.</p> <p>Nota La función de visualizador solo se admite para instancias de vRealize Orchestrator autenticadas con vRealize Automation. Esta función no está asignada a una función de vRealize Automation de forma predeterminada, por lo que se debe asignar de forma explícita a los usuarios.</p>

Función de usuario	Descripción
Diseñador de flujos de trabajo	<p>Este usuario puede ampliar la funcionalidad de la plataforma de vRealize Orchestrator mediante la creación y la edición de objetos. Los diseñadores de flujos de trabajo no tienen acceso a las funciones de administración y solución de problemas del vRealize Orchestrator Client. Entre las responsabilidades principales del diseñador de flujos de trabajo se incluyen:</p> <ul style="list-style-type: none"> ■ Crear, editar, ejecutar y eliminar objetos de vRealize Orchestrator, como flujos de trabajo, acciones, políticas y elementos de configuración. ■ Programar ejecuciones de flujos de trabajo. Consulte <i>Programar flujos de trabajo en el cliente de vRealize Orchestrator</i> en <i>Uso del cliente de VMware vRealize Orchestrator</i>. ■ Agregar el contenido que creó el desarrollador de flujos de trabajo a los grupos a los que están asignados. ■ Insertar cambios locales en el inventario de contenido de vRealize Orchestrator en el repositorio de Git conectado. Consulte <i>Insertar cambios en un repositorio de Git en Uso del cliente de VMware vRealize Orchestrator</i>.
Usuarios con derechos limitados	<p>Los usuarios que no tienen ninguna función asignada pueden seguir iniciando sesión en el vRealize Orchestrator Client, pero tendrán acceso limitado al contenido y las funciones del cliente. Si están asignados a un grupo, podrán ver y ejecutar el contenido que se incluye en ese grupo.</p>

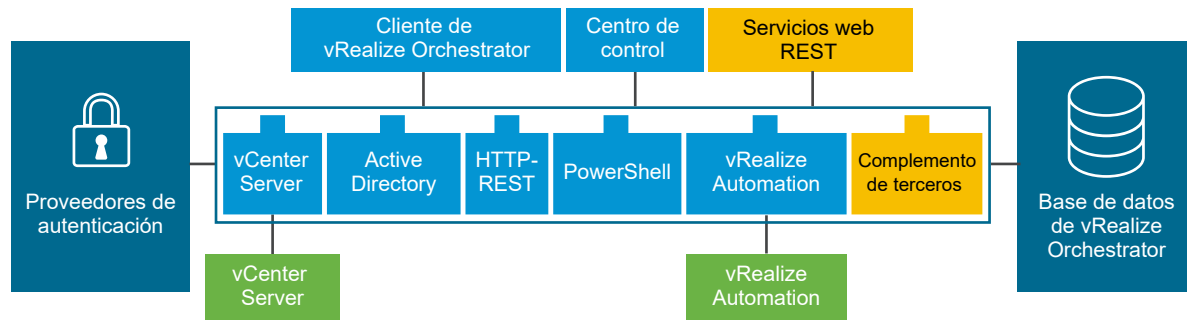
Arquitectura de vRealize Orchestrator

vRealize Orchestrator contiene una biblioteca de flujos de trabajo y un motor de flujos de trabajo para crear y ejecutar flujos de trabajo que automaticen los procesos de orquestación. Se ejecutan flujos de trabajo en los objetos de diferentes tecnologías a las que vRealize Orchestrator accede mediante una serie de complementos.

vRealize Orchestrator proporciona una serie de complementos estándar, incluidos algunos para vCenter Server y vRealize Automation, que permiten orquestar tareas en los distintos entornos que los complementos exponen.

vRealize Orchestrator también presenta una arquitectura abierta para conectar aplicaciones externas de terceros a la plataforma de orquestación. Se pueden ejecutar flujos de trabajo en los objetos de las tecnologías conectadas que defina usted mismo. vRealize Orchestrator se conecta a un proveedor de autenticación para administrar cuentas de usuario y a una base de datos PostgreSQL preconfigurada para almacenar información de los flujos de trabajo que ejecuta. Puede acceder a vRealize Orchestrator, a los objetos que expone y a los flujos de trabajo de vRealize Orchestrator a través de vRealize Orchestrator Client o a través de servicios web. La supervisión y configuración de los flujos de trabajo y servicios de vRealize Orchestrator se realiza a través del vRealize Orchestrator Client y el centro de control.

Figura 1-1. Arquitectura de VMware vRealize Orchestrator



vRealize Orchestrator Plug-ins

Los complementos permiten usar vRealize Orchestrator para acceder y controlar tecnologías y aplicaciones externas. Al utilizar una tecnología externa en un complemento de vRealize Orchestrator, puede incorporar objetos y funciones en flujos de trabajo que tienen acceso a los objetos y las funciones de esa tecnología externa.

Las tecnologías externas a las que puede acceder a través de los complementos abarcan herramientas de administración de virtualización, sistemas de correo electrónico, bases de datos, servicios de directorio e interfaces de control remoto.

vRealize Orchestrator proporciona una serie de complementos de serie que puede usar para incorporar en los flujos de trabajo dichas tecnologías, como la API devCenter Server de VMware y funciones de correo electrónico. Mediante los complementos, puede automatizar la prestación de nuevos servicios de TI, o bien adaptar las capacidades de la infraestructura y los servicios de aplicaciones existentes. Además, puede utilizar la arquitectura de código abierto de complementos de vRealize Orchestrator para desarrollar complementos que le permitan acceder a otras aplicaciones.

Los complementos de vRealize Orchestrator que desarrolla VMware se distribuyen como archivos `.vmoapp`.

Para obtener más información sobre los complementos de vRealize Orchestrator, consulte [Uso de los complementos de VMware vRealize Orchestrator](#).

Para obtener más información sobre complementos de terceros de vRealize Orchestrator, consulte [VMware Marketplace](#).

Requisitos del sistema de vRealize Orchestrator

2

El sistema debe cumplir los requisitos técnicos necesarios para que vRealize Orchestrator funcione correctamente.

Para obtener una lista de las versiones compatibles de vCenter Server, vSphere Web Client, vRealize Automation y otras soluciones de VMware, consulte [Matriz de interoperabilidad de productos de VMware](#).

Este capítulo incluye los siguientes temas:

- [Componentes de vRealize Orchestrator Appliance](#)
- [Requisitos de hardware de vRealize Orchestrator Appliance](#)
- [Valores máximos de escalabilidad de vRealize Orchestrator](#)
- [Requisitos de red para vRealize Orchestrator](#)
- [Endpoints y puertos de vRealize Orchestrator](#)
- [Navegadores compatibles con vRealize Orchestrator](#)
- [Nivel de internacionalización y compatibilidad con la localización](#)

Componentes de vRealize Orchestrator Appliance

vRealize Orchestrator Appliance es un dispositivo virtual basado en Photon que se ejecuta en contenedores.

vRealize Orchestrator Appliance incluye los siguientes componentes:

- Una capa de Kubernetes de nivel de infraestructura.
- Una base de datos PostgreSQL preconfigurada.
- Los servicios principales de vRealize Orchestrator: el servicio del servidor, el servicio del centro de control y el servicio de la interfaz de usuario de orquestación.

La configuración de la base de datos predeterminada de vRealize Orchestrator Appliance está lista para la producción.

Nota Para usar vRealize Orchestrator Appliance en un entorno de producción, debe configurar el servidor de vRealize Orchestrator para que se autentique a través de vRealize Automation o de vSphere. Consulte [Configurar un servidor de vRealize Orchestrator independiente](#).

Requisitos de hardware de vRealize Orchestrator Appliance

vRealize Orchestrator Appliance es una máquina virtual preconfigurada basada en Photon que se ejecuta en contenedores. Antes de implementar el dispositivo, compruebe que el sistema cumpla los requisitos mínimos de hardware.

El vRealize Orchestrator Appliance presenta los siguientes requisitos de hardware:

- 4 CPU
- 12 GB de memoria
- Disco duro de 200 GB

No reduzca el tamaño predeterminado de la memoria, ya que el servidor de vRealize Orchestrator requiere al menos 8 GB de memoria libre.

Valores máximos de escalabilidad de vRealize Orchestrator

En la tabla de límites de escalabilidad se describen los valores máximos recomendados en implementaciones de vRealize Orchestrator 8.x.

Componente	Destinos de escala	Más información
Máquinas virtuales	35.000	
Conexiones de vCenter Server	10	Consulte Configuración de vCenter Server
Nodos activos en un clúster	3	Consulte Configurar un clúster de vRealize Orchestrator
Flujos de trabajo en ejecución simultánea	300 por nodo	Consulte Configurar las propiedades de ejecución de los flujos de trabajo
Flujos de trabajo en ejecución en cola	10.000 por nodo	
Ejecuciones de flujos de trabajo conservadas	100 por nodo	
Días para caducidad de evento de registro	15	

Requisitos de red para vRealize Orchestrator

Cada nodo de vRealize Orchestrator requiere una configuración de red.

Los requisitos de red para vRealize Orchestrator son:

- Dirección de red e IPv4 única y estática
- Servidor DNS accesible configurado manualmente

- Nombre de dominio completo (Fully-Qualified Domain Name, FQDN) válido configurado manualmente que se puede resolver tanto hacia adelante como hacia atrás a través del servidor DNS

Nota No se admite el cambio de dirección IP o el cambio de nombre de host después de la instalación y se produce un error en la configuración del que no es posible recuperarse.

Endpoints y puertos de vRealize Orchestrator

El servicio Kubernetes de vRealize Orchestrator incluye dos endpoints y varios puertos de red principales.

Puertos de red de vRealize Orchestrator

Puede acceder a vRealize Orchestrator a través del puerto 443. El puerto 443 está protegido con un certificado autofirmado que se genera durante la instalación y el usuario no puede reemplazarlo. Cuando se utiliza un equilibrador de carga externo, se debe configurar para lograr el equilibrio en el puerto 443.

Para ver todos los puertos de vRealize Orchestrator, consulte la herramienta [Puertos y protocolos](#).

Endpoints de vRealize Orchestrator

Puede acceder al cliente de vRealize Orchestrator y a los servicios del centro de control en los siguientes endpoints.

Servicio	Endpoint
Cliente de vRealize Orchestrator	<code>https://your_orchestrator_FQDN/orchestration-ui</code>
Centro de control	<code>https://your_orchestrator_FQDN/vco-controlcenter</code>

Navegadores compatibles con vRealize Orchestrator

Confirme que los navegadores sean compatibles con vRealize Orchestrator.

Para acceder a vRealize Orchestrator Client y al centro de control, debe utilizar uno de los siguientes navegadores:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Nivel de internacionalización y compatibilidad con la localización

El centro de control de vRealize Orchestrator y vRealize Orchestrator Client son compatibles con sistemas operativos que no están en inglés, formatos de datos distintos al inglés y poseen compatibilidad con varios idiomas para el centro de control y la interfaz de usuario del cliente.

El centro de control de vRealize Orchestrator y vRealize Orchestrator Client admiten el uso de sistemas operativos que no están en inglés, la entrada y la salida en un idioma distinto del inglés, y la compatibilidad con formatos de datos distintos al inglés (por ejemplo, en las fechas, la hora y los números).

Las interfaces de usuario de vRealize Orchestrator y vRealize Orchestrator Client están localizadas en los siguientes idiomas:

- Español
- Francés
- Alemán
- Chino tradicional
- Chino simplificado
- Coreano
- Japonés
- Italiano
- Neerlandés
- Portugués de Brasil
- Ruso

Configurar componentes de vRealize Orchestrator

3

Cuando vRealize Orchestrator Appliance se descarga e implementa, el servidor de vRealize Orchestrator está preconfigurado. Después de la implementación, los servicios se inician de manera automática.

Tenga en cuenta estas directrices para mejorar la disponibilidad y la escalabilidad de la configuración de vRealize Orchestrator:

- Instale y configure un proveedor de autenticación, y configure vRealize Orchestrator para que funcione con él. Consulte [Configurar un servidor de vRealize Orchestrator independiente](#).
- En el caso de entornos de vRealize Orchestrator agrupados en clúster, instale y configure un servidor de equilibrio de carga y configúrelo para distribuir la carga de trabajo entre los servidores de vRealize Orchestrator.

Este capítulo incluye los siguientes temas:

- [Configuración de vCenter Server](#)
- [Métodos de autenticación](#)

Configuración de vCenter Server

Aumentar el número de instancias de vCenter Server en la configuración de vRealize Orchestrator hace que vRealize Orchestrator tenga que administrar más sesiones. Cuando hay demasiadas sesiones activas, vRealize Orchestrator puede experimentar tiempos de espera si se producen más de 10 conexiones de vCenter Server.

Para obtener una lista de las versiones compatibles de vCenter Server, consulte [Matriz de interoperabilidad de productos de VMware](#).

Nota Si la red tiene un ancho de banda y una latencia suficientes, puede ejecutar varias instancias de vCenter Server en diferentes máquinas virtuales en la configuración de vRealize Orchestrator. Si utiliza una LAN para mejorar las comunicaciones entre vRealize Orchestrator y vCenter Server, es indispensable contar con una línea de 100 Mb.

Métodos de autenticación

Para autenticar y administrar permisos de usuario, vRealize Orchestrator requiere una conexión a vRealize Automation o a una instancia de servidor de vSphere.

Cuando descargue e implemente vRealize Orchestrator Appliance, debe configurar el servidor con una autenticación de vRealize Automation o vSphere. Consulte [Configurar un servidor de vRealize Orchestrator independiente](#).

Nota La autenticación de vRealize Orchestrator 8.x con vRealize Automation solo se admite con vRealize Automation 8.x.

Instalar vRealize Orchestrator

4

vRealize Orchestrator consta de un componente servidor y un componente cliente.

Para usar vRealize Orchestrator, debe implementar vRealize Orchestrator Appliance y configurar el servidor de vRealize Orchestrator.

Puede cambiar los ajustes de configuración predeterminados de vRealize Orchestrator mediante el centro de control de vRealize Orchestrator.

Este capítulo incluye los siguientes temas:

- [Descargar e implementar vRealize Orchestrator Appliance](#)

Descargar e implementar vRealize Orchestrator Appliance

Antes de poder acceder al contenido y los servicios de vRealize Orchestrator, debe descargar e implementar vRealize Orchestrator Appliance.

Requisitos previos

- Compruebe que está ejecutando una instancia de vCenter Server. La versión de vCenter Server debe ser la 6.0 o una posterior.
- Compruebe que el host donde se implementa vRealize Orchestrator Appliance cumpla los requisitos de hardware mínimos. Consulte [Requisitos de hardware de vRealize Orchestrator Appliance](#).
- Si el sistema está aislado y no tiene acceso a Internet, debe descargar el archivo `.ova` para el dispositivo desde el sitio web de VMware.

Procedimiento

- 1 Inicie sesión en el vSphere Web Client como **administrador**.
- 2 Seleccione un objeto de inventario que sea un objeto principal válido de una máquina virtual, por ejemplo, un centro de datos, una carpeta, un clúster, un grupo de recursos o un host.
- 3 Seleccione **Acciones > Implementar plantilla OVF**.
- 4 Introduzca la ruta o la URL al archivo `.ova` y haga clic en **Siguiente**.
- 5 Introduzca un nombre y una ubicación para la instancia de vRealize Orchestrator Appliance, y haga clic en **Siguiente**.

- 6 Seleccione un host, un clúster, un grupo de recursos o una vApp como destino en el que ejecutar el dispositivo, y haga clic en **Siguiente**.
- 7 Revise los detalles de la implementación y haga clic en **Siguiente**.
- 8 Acepte los términos del contrato de licencia y haga clic en **Siguiente**.
- 9 Seleccione el formato de almacenamiento que desea usar para la instancia de vRealize Orchestrator Appliance.

Formato	Descripción
Aprovisionamiento grueso diferido reducido a cero	Crea un disco virtual en un formato grueso predeterminado. El espacio necesario para el disco virtual se asigna en el momento de la creación del disco virtual. Si quedan datos en el dispositivo físico, no se borran durante la creación, pero reducen a cero a petición posteriormente a la escritura desde la máquina virtual.
Aprovisionamiento grueso diligente reducido a cero	Admite las funciones de clúster como la tolerancia a errores. El espacio necesario para el disco virtual se asigna en el momento de la creación del disco virtual. Si quedan datos en el dispositivo físico, se reducen a cero cuando se crea el disco virtual. La creación de discos en este formato podría tardar mucho más que la creación de discos en otros formatos.
Formato de aprovisionamiento fino	Ahorra espacio en el disco duro. En el disco fino, se aprovisiona tanto espacio de almacén de datos como requiera el disco en función del valor seleccionado para el tamaño de disco. El disco fino inicialmente es pequeño y, al principio, solo utiliza el espacio de almacén de datos que necesita el disco para sus operaciones iniciales.

- 10 Haga clic en **Siguiente**.
- 11 Configure las opciones de red e introduzca la contraseña **raíz**.

Al configurar las opciones de red de los archivos vRealize Orchestrator Appliance, debe utilizar el protocolo IPv4. Para las configuraciones de red DHCP y estática, debe agregar un nombre de dominio completo (Fully Qualified Domain Name, FQDN) para vRealize Orchestrator Appliance.

Si el nombre de host que se muestra en el shell de la instancia de vRealize Orchestrator Appliance implementada es *photon-machine*, no se cumplen los requisitos anteriores de configuración de red.

- 12 (opcional) Configure opciones de red adicionales para vRealize Orchestrator Appliance, como la habilitación del acceso SSH.

Nota Al configurar una red de Kubernetes, los valores del CIDR de clúster interno y el CIDR de servicio interno deben permitir al menos 1024 hosts. Debido a este requisito, el valor de máscara de red debe ser 22 o menos. Los valores de máscara de red superiores a 22 no son válidos. Las propiedades de red de Kubernetes tienen que seguir los valores predeterminados:

Kubernetes network property	Default value	Property description
CIDR de clúster interno de Kubernetes	10.244.0.0/22	El CIDR utilizado para pods que se ejecutan dentro del clúster de Kubernetes.
CIDR de servicio interno de Kubernetes	10.244.4.0/22	El CIDR utilizado para servicios de Kubernetes dentro del clúster de Kubernetes.

Nota También puede cambiar las propiedades de red CIDR de Kubernetes después de la implementación. Consulte [Configurar CIDR de Kubernetes de vRealize Orchestrator](#).

- 13** (opcional) Para habilitar el modo FIPS para vRealize Orchestrator Appliance, establezca el **Modo FIPS** en **estricto**.

Nota La habilitación de FIPS 140-2 solo se admite en entornos nuevos de vRealize Orchestrator. Si desea habilitar el modo FIPS en su entorno, debe hacerlo durante la instalación.

- 14** Haga clic en **Siguiente**.

- 15** Revise la página **Listo para finalizar** y haga clic en **Finalizar**.

Resultados

vRealize Orchestrator Appliance se habrá implementado correctamente.

Pasos siguientes

Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz** y confirme que puede realizar una búsqueda de DNS directa o inversa.

- Para realizar una búsqueda de DNS directa, ejecute el comando `nslookup your_orchestrator_FQDN`. El comando debe devolver la dirección IP de vRealize Orchestrator Appliance.
- Para realizar una búsqueda de DNS inversa, ejecute el comando `nslookup your_orchestrator_IP`. El comando debe devolver el FQDN de vRealize Orchestrator Appliance.

Nota Si no ha habilitado SSH durante la implementación, también puede realizar búsquedas de DNS desde la consola de la máquina virtual en vSphere Web Client.

Encender vRealize Orchestrator Appliance y abrir la página de inicio

Para usar la instancia de vRealize Orchestrator Appliance independiente, primero debe encenderla.

Procedimiento

- 1** Inicie sesión en vSphere Web Client como **administrador**.

- 2 Haga clic con el botón secundario en vRealize Orchestrator Appliance y seleccione **Alimentación > Encender**.
- 3 En un navegador web, desplácese hasta la dirección del host de la máquina virtual de vRealize Orchestrator Appliance que configuró durante la implementación del OVA.

https://your_orchestrator_FQDN/vco.

Habilitar o deshabilitar el acceso SSH a vRealize Orchestrator Appliance

Puede habilitar o deshabilitar el acceso SSH a vRealize Orchestrator Appliance.

Requisitos previos

- Descargue e implemente el vRealize Orchestrator Appliance.
- Compruebe que vRealize Orchestrator Appliance esté listo y en ejecución.

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz**.
- 2 Para habilitar el acceso SSH, ejecute el comando `/usr/bin/toggle-ssh enable`.
- 3 Para deshabilitar el acceso SSH, ejecute el comando `/usr/bin/toggle-ssh disable`.

Configuración inicial

5

Antes de empezar a automatizar tareas y administrar sistemas y aplicaciones con vRealize Orchestrator, debe utilizar el centro de control de vRealize Orchestrator para configurar un proveedor de autenticación externo. También puede utilizar el centro de control de vRealize Orchestrator para realizar otras tareas de configuración, como la administración de la información de licencias y certificados, la instalación de complementos y la supervisión del estado del clúster de vRealize Orchestrator.

Este capítulo incluye los siguientes temas:

- [Configurar un servidor de vRealize Orchestrator independiente](#)
- [Habilitar funciones de vRealize Orchestrator con licencias](#)
- [Conexión con una base de datos de vRealize Orchestrator](#)
- [Administrar certificados](#)
- [Configurar los complementos de vRealize Orchestrator](#)
- [Alta disponibilidad de vRealize Orchestrator](#)
- [Configurar el programa de mejora de la experiencia de cliente](#)

Configurar un servidor de vRealize Orchestrator independiente

A pesar de que vRealize Orchestrator Appliance es una máquina virtual preconfigurada basada en Photon, debe configurar un proveedor de autenticación antes de acceder a la funcionalidad completa del centro de control de vRealize Orchestrator y vRealize Orchestrator Client.

Configurar un servidor de vRealize Orchestrator independiente con la autenticación de vRealize Automation

Para preparar vRealize Orchestrator Appliance para su uso, debe configurar los ajustes del host y el proveedor de autenticación. Puede configurar vRealize Orchestrator para que se autentique con vRealize Automation. Use la autenticación de vRealize Automation con vRealize Automation 8.x.

Requisitos previos

- Descargue e implemente la versión más reciente de vRealize Orchestrator Appliance. Consulte [Descargar e implementar vRealize Orchestrator Appliance](#).
- Instale y configure vRealize Automation 8.x, y compruebe que el servidor de vRealize Automation se esté ejecutando. Consulte la documentación de vRealize Automation.

Importante La versión del producto del proveedor de autenticación de vRealize Automation debe coincidir con la versión del producto de su implementación de vRealize Orchestrator. Por ejemplo, para autenticar una implementación de vRealize Orchestrator 8.5, debe utilizar una implementación de vRealize Automation 8.5.

Si tiene previsto crear un clúster:

- Configure un equilibrador de carga para distribuir el tráfico entre varias instancias de vRealize Orchestrator. Consulte la [Guía de equilibrio de carga de VMware vRealize Orchestrator 8.x](#).

Procedimiento

- 1 Acceda al centro de control para iniciar el asistente para configuración.
 - a Vaya a `https://your_orchestrator_FQDN/vco-controlcenter`.
 - b Inicie sesión como **raíz** con la contraseña que introdujo durante la implementación de OVA.
- 2 Configure el proveedor de autenticación.
 - a En la página **Configurar proveedor de autenticación**, seleccione **vRealize Automation** en el menú desplegable **Modo de autenticación**.
 - b En el cuadro de texto **Dirección del host**, indique la dirección de host de vRealize Automation y haga clic en **CONECTAR**.

El formato de la dirección de host de vRealize Automation debe ser `https://your_vra_hostname`.
 - c Haga clic en **Aceptar certificado**.
 - d Introduzca las credenciales del propietario de la organización de vRealize Automation en la que se configurará vRealize Orchestrator. Haga clic en **REGISTRAR**.
 - e Haga clic en **GUARDAR CAMBIOS**.

Aparecerá un mensaje que indica que la configuración se ha guardado correctamente.

Resultados

La configuración del servidor de vRealize Orchestrator se ha llevado a cabo correctamente.

Pasos siguientes

- Compruebe que **CSP** sea el proveedor de licencias configurado en la página **Licencias**.

- Compruebe que el nodo esté configurado correctamente en la página **Validar configuración**.

Nota Tras configurar el proveedor de autenticación, el servidor de vRealize Orchestrator se reinicia automáticamente pasados dos minutos. La verificación de la configuración que se realiza inmediatamente después de la autenticación puede devolver un estado de configuración no válido.

Configurar un servidor de vRealize Orchestrator independiente con la autenticación de vSphere

Para registrar el servidor de vRealize Orchestrator con un servidor de vCenter Single Sign-On, debe utilizar el modo de autenticación de vSphere. Utilice la autenticación de vCenter Single Sign-On con vCenter Server 6.0 y versiones posteriores.

Requisitos previos

- Descargue e implemente la versión más reciente de vRealize Orchestrator Appliance. Consulte [Descargar e implementar vRealize Orchestrator Appliance](#).
- Instale y configure una instancia de vCenter Server con vCenter Single Sign-On en ejecución. Consulte la documentación de vSphere.

Si tiene previsto crear un clúster:

- Configure un equilibrador de carga para distribuir el tráfico entre varias instancias de vRealize Orchestrator. Consulte la [Guía de equilibrio de carga de VMware vRealize Orchestrator 8.x](#).

Procedimiento

- 1 Acceda al centro de control para iniciar el asistente para configuración.
 - a Vaya a `https://your_orchestrator_FQDN/vco-controlcenter`.
 - b Inicie sesión como **raíz** con la contraseña que introdujo durante la implementación de OVA.

2 Configure el proveedor de autenticación.

- a En la página **Configurar proveedor de autenticación**, seleccione **vSphere** en el menú desplegable **Modo de autenticación**.
- b En el cuadro de texto **Dirección del host**, introduzca el nombre de dominio completo o la dirección IP de la instancia de Platform Services Controller que contiene el vCenter Single Sign-On, y haga clic en **Conectar**.

Nota Si utiliza un Platform Services Controller externo o varias instancias de Platform Services Controller detrás de un equilibrador de carga, debe importar manualmente los certificados de todas las instancias de Platform Services Controller que compartan un dominio de vCenter Single Sign-On.

Nota Para integrar un vSphere Client diferente con el entorno de vRealize Orchestrator configurado, debe configurar vSphere para que use la misma instancia de Platform Services Controller registrada en vRealize Orchestrator. En los entornos de alta disponibilidad de vRealize Orchestrator, debe replicar las instancias de PCS detrás del servidor del equilibrador de carga de vRealize Orchestrator.

- c Revise la información del certificado del proveedor de autenticación y haga clic en **Aceptar certificado**.
- d Introduzca las credenciales de la cuenta de administrador local para el dominio de vCenter Single Sign-On. Haga clic en **REGISTRAR**.

De forma predeterminada, la cuenta es **administrator@vsphere.local** y el nombre del tenant predeterminado es **vsphere.local**.
- e En el cuadro de texto **Grupo de administradores**, escriba el nombre de un grupo de administradores y haga clic en **BUSCAR**.

Por ejemplo, **vsphere.local\vcoadmins**.
- f Seleccione el grupo de administración que desee usar.
- g Haga clic en **GUARDAR CAMBIOS**.

Aparecerá un mensaje que indica que la configuración se ha guardado correctamente.

Resultados

La configuración del servidor de vRealize Orchestrator se ha llevado a cabo correctamente.

Pasos siguientes

- Compruebe que **CIS** sea el proveedor de licencias configurado en la página **Licencias**.

- Compruebe que el nodo esté configurado correctamente en la página **Validar configuración**.

Nota Tras configurar el proveedor de autenticación, el servidor de vRealize Orchestrator se reinicia automáticamente pasados dos minutos. La verificación de la configuración que se realiza inmediatamente después de la autenticación puede devolver un estado de configuración no válido.

Habilitar funciones de vRealize Orchestrator con licencias

El acceso a determinadas funciones de vRealize Orchestrator se basa en la licencia que se aplica a la implementación de vRealize Orchestrator.

Tras la autenticación, se asigna una licencia a la instancia de vRealize Orchestrator en base al proveedor de autenticación. Las licencias controlan el acceso a las siguientes funciones de vRealize Orchestrator:

- Integración de Git
- Administración de funciones
- Compatibilidad con varios lenguajes (Python, Node.js y PowerShell)

La licencia del servidor de vRealize Orchestrator se puede cambiar manualmente en la página **Licencias** del centro de control.

Nota No hay ningún límite para el número de implementaciones de vRealize Orchestrator a las que se puede aplicar la misma licencia, independientemente del tipo de licencia. Para las licencias de vRealize Automation, no se requiere un entorno de vRealize Automation implementado y configurado.

Autenticación	Licencia	Integración de Git	Administración de funciones	Compatibilidad con varios lenguajes
vSphere	vSphere vCloud Suite Standard	No	No	No
vSphere	vRealize Automation vRealize Suite Advanced o Enterprise vCloud Suite Advanced o Enterprise	Sí	Sí	Sí
vRealize Automation	vRealize Automation vRealize Suite Advanced o Enterprise vCloud Suite Advanced o Enterprise	Sí	Las funciones se administran desde la instancia de vRealize Automation utilizada para autenticar vRealize Orchestrator.	Sí

Nota Las licencias de vRealize Suite Standard no incluyen vRealize Automation, por lo que no admiten el acceso a las funciones de vRealize Orchestrator.

Conexión con una base de datos de vRealize Orchestrator

El servidor de vRealize Orchestrator requiere una base de datos para almacenar los datos.

La instancia de vRealize Orchestrator Appliance implementada incluye una base de datos de PostgreSQL preconfigurada que utiliza el servidor de vRealize Orchestrator para almacenar los datos.

Los usuarios no pueden acceder a la base de datos de postgresQL.

Administrar certificados

Emitido para un determinado servidor y con información sobre la clave pública del servidor, el certificado permite firmar todos los elementos creados en vRealize Orchestrator y garantizar la autenticidad. Cuando el cliente recibe un elemento del servidor de un usuario, habitualmente un paquete, el cliente verifica la identidad del usuario y decide si su firma será o no de confianza.

■ Administrar certificados de vRealize Orchestrator

Los certificados de vRealize Orchestrator se pueden administrar desde la página

Certificados en el centro de control de vRealize Orchestrator o con el vRealize Orchestrator Client mediante los flujos de trabajo etiquetados *ssl_trust_manager*.

Administrar certificados de vRealize Orchestrator

Los certificados de vRealize Orchestrator se pueden administrar desde la página **Certificados** en el centro de control de vRealize Orchestrator o con el vRealize Orchestrator Client mediante los flujos de trabajo etiquetados *ssl_trust_manager*.

Importar un certificado al almacén de confianza de Orchestrator

El centro de control de vRealize Orchestrator utiliza una conexión segura para comunicarse con vCenter Server, el sistema de administración de bases de datos relacionales (RDBMS), LDAP, Single Sign-On y otros servidores. Puede importar el certificado TLS requerido desde una URL o desde un archivo con codificación PEM. Cada vez que desee utilizar una conexión TLS a una instancia de servidor, debe importar el certificado correspondiente de la pestaña **Certificados de confianza** en la página **Certificados** e importar el certificado TLS pertinente.

Puede cargar el certificado TLS en vRealize Orchestrator desde una dirección URL o desde un archivo con codificación PEM.

Opción	Descripción
Importar de URL o URL de proxy	URL del servidor remoto: <code>https://dirección_IP_servidor o dirección_IP_servidor:puerto</code>
Importar de archivo	Ruta del archivo de certificado con codificación PEM. Nota También puede importar un certificado de confianza si ejecuta el flujo de trabajo Importar un certificado de confianza desde un archivo en el vRealize Orchestrator Client. El archivo importado a través de este flujo de trabajo debe estar codificado con DER.

Para obtener más información sobre cómo importar un certificado, consulte [Importar un certificado de confianza con el centro de control](#).

Certificado de firma del paquete

Los paquetes que se exportan desde un servidor de vRealize Orchestrator están firmados digitalmente. Importe, exporte o genere un certificado nuevo para utilizar en la firma de paquetes. Los certificados de firma de paquetes son una forma de identificación digital que se emplea para garantizar la comunicación cifrada y como firma de paquetes de Orchestrator.

vRealize Orchestrator Appliance incluye un certificado de firma de paquetes que se genera automáticamente según la configuración de red del dispositivo. Si la configuración de red del dispositivo cambia, se debe generar manualmente otro certificado de firma de paquetes. Después de generar un certificado de firma de paquetes nuevo, todos los paquetes que se exporten posteriormente se firmarán con el nuevo certificado.

Generar un certificado TLS personalizado para vRealize Orchestrator

Puede usar vRealize Orchestrator Appliance para generar un nuevo certificado TLS para su entorno o para establecer un certificado personalizado existente.

vRealize Orchestrator Appliance incluye un certificado Capa de seguridad de confianza (Trusted Layer Security, TLS) que se genera automáticamente con base en la configuración de red del dispositivo. Si la configuración de red del dispositivo cambia, se debe generar manualmente un nuevo certificado. Puede crear una cadena de certificados para garantizar la comunicación cifrada y proporcionar una firma para los paquetes. Ahora bien, el destinatario no puede estar seguro de que el paquete autofirmado sea, de hecho, un paquete de su servidor y no de un tercero que afirme ser usted. Para probar la identidad del servidor, utilice un certificado firmado por una entidad de certificación (Certificate Authority, CA).

vRealize Orchestrator genera un certificado de servidor exclusivo para su entorno. La clave privada se almacena en la tabla `vmo_keystore` de la base de datos de vRealize Orchestrator.

Nota Para configurar vRealize Orchestrator Appliance para usar un certificado TLS personalizado existente, consulte [Establecer un certificado TLS personalizado para vRealize Orchestrator](#).

Requisitos previos

Compruebe que el acceso SSH a vRealize Orchestrator Appliance esté habilitado. Consulte [Habilitar o deshabilitar el acceso SSH a vRealize Orchestrator Appliance](#).

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance mediante SSH como **raíz**.
- 2 Ejecute el comando `vracli certificate ingress --generate auto --set stdin`.
- 3 Para aplicar el certificado personalizado a vRealize Orchestrator Appliance, ejecute el script de implementación.

- a Desplácese hasta el directorio `/opt/scripts/`.

```
cd /opt/scripts/
```

- b Ejecute el script `./deploy.sh`.

Importante No interrumpa el script de implementación. Recibirá el siguiente mensaje cuando el script termine de ejecutarse:

```
El preludio se implementó correctamente. Para acceder, vaya a your_orchestrator_address
```

Pasos siguientes

Para confirmar que se ha aplicado la nueva cadena de certificados, ejecute el comando `vracli certificate ingress --list`.

Establecer un certificado TLS personalizado para vRealize Orchestrator

Establezca un certificado TLS personalizado para su vRealize Orchestrator Appliance.

vRealize Orchestrator Appliance incluye un certificado Capa de seguridad de confianza (Trusted Layer Security, TLS) que se genera automáticamente con base en la configuración de red del dispositivo.

Puede configurar vRealize Orchestrator Appliance para que use un certificado TLS personalizado existente. Puede establecer el certificado mediante la importación del archivo PEM correspondiente desde la máquina local en vRealize Orchestrator Appliance. También puede configurar el certificado TLS personalizado copiando la cadena de certificados directamente en vRealize Orchestrator Appliance. Ambos procedimientos requieren que se ejecute el script `./deploy.sh` para poder usar el nuevo certificado TLS en la implementación de vRealize Orchestrator.

Para obtener información sobre cómo generar un nuevo certificado TLS personalizado, consulte [Generar un certificado TLS personalizado para vRealize Orchestrator](#).

Requisitos previos

- Compruebe que el acceso SSH a vRealize Orchestrator Appliance esté habilitado. Consulte [Habilitar o deshabilitar el acceso SSH a vRealize Orchestrator Appliance](#).
- Compruebe que el archivo PEM con el certificado TLS contenga los siguientes componentes en el orden establecido:
 - a La clave privada del certificado.
 - b El certificado principal.
 - c Si corresponde, los certificados o el certificado intermedio de la entidad de certificación (CA).
 - d El certificado de CA raíz.

Por ejemplo, el certificado de TLS puede tener la siguiente estructura:

```
-----BEGIN RSA PRIVATE KEY-----
<Private Key>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Primary TLS certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA certificate>
-----END CERTIFICATE-----
```

Procedimiento

- 1 Configure el certificado mediante la importación del archivo PEM en vRealize Orchestrator Appliance.

- a Importe el archivo PEM del certificado desde su máquina local mediante la ejecución de un comando de copia segura (SCP) desde un shell SSH.

Para Linux, puede utilizar un comando SCP de terminal:

```
scp ~/PEM_local_filepath/your_cert_file.PEM root@orchestrator_FQDN_or_IP:/
PEM_orchestrator_filepath/your_cert_file.PEM
```

Para Windows, puede usar un comando PSCP de cliente PuTTY:

```
pscp C:\PEM_local_filepath\your_cert_file.PEM root@<orchestrator_FQDN_or_IP>:/
PEM_orchestrator_filepath/your_cert_file.PEM
```

- b Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance mediante SSH como **raíz**.
 - c Ejecute el comando `vracli certificate ingress --set archivo_cert.PEM`.
- 2 (opcional) Configure el certificado copiando la cadena de certificados directamente en el dispositivo.

- a Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance mediante SSH como **raíz**.
 - b Ejecute el comando `vracli certificate ingress --set stdin`.
 - c Copie y pegue la cadena de certificados y presione Ctrl + D.

- 3 Para aplicar el nuevo certificado TLS, ejecute el script de implementación.

- a Desplácese hasta el directorio `/opt/scripts/`.

```
cd /opt/scripts/
```

- b Ejecute el script `./deploy.sh`.

Importante No interrumpa el script de implementación. Recibirá el siguiente mensaje cuando el script termine de ejecutarse:

```
El preludio se implementó correctamente. Para acceder, vaya a https://
your_orchestrator_FQDN
```

Resultados

Ha establecido un certificado TLS personalizado para vRealize Orchestrator Appliance.

Pasos siguientes

Para confirmar que se ha aplicado la nueva cadena de certificados, ejecute el comando `vracli certificate ingress --list`.

Importar un certificado de confianza con el centro de control

Para comunicarse con otros servidores de forma segura, el servidor de vRealize Orchestrator debe poder comprobar su identidad. Para ello, puede que tenga que importar el certificado TLS de la entidad remota al almacén de confianza de vRealize Orchestrator. Para confiar en un certificado, puede importarlo al almacén de confianza, ya sea mediante el establecimiento de una conexión a una dirección URL específica, o bien directamente como archivo con codificación PEM.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Vaya a la página **Certificados**.
- 3 Seleccione **Certificados de confianza** y haga clic en **Importar**.
- 4 Para importar el certificado de un archivo, seleccione **Importar de un archivo con codificación PEM**.
- 5 Desplácese hasta el archivo del certificado y haga clic en **Importar**.
- 6 Para importar el certificado desde una dirección URL, seleccione **Importar desde URL**.
- 7 Introduzca la dirección URL en la que se almacena el certificado y haga clic en **Importar**.

Resultados

Ha importado correctamente el certificado de servidor remoto al almacén de confianza de vRealize Orchestrator.

Configurar los complementos de vRealize Orchestrator

vRealize Orchestrator Appliance proporciona acceso a una biblioteca preinstalada de complementos predeterminados. Los complementos de vRealize Orchestrator predeterminados se configuran con flujos de trabajo específicos del complemento que se ejecutan en el cliente de vRealize Orchestrator.

Los complementos de vRealize Orchestrator predeterminados incluyen flujos de trabajo de configuración. Puede ejecutar estos flujos de trabajo desde el cliente de vRealize Orchestrator para registrar endpoints para administrar.

Los flujos de trabajo de configuración tienen la etiqueta *configuration*. Por ejemplo, para acceder a flujos de trabajo que se utilizan para administrar suscripciones y agentes de AMQP, introduzca las etiquetas *AMQP* y *Configuration* en el cuadro de texto de búsqueda de la biblioteca de flujos de trabajo.

Administrar complementos de vRealize Orchestrator

En la página **Administrar complementos** del centro de control de vRealize Orchestrator, puede ver una lista de todos los complementos instalados en vRealize Orchestrator y realizar acciones de administración básicas.

Instalar o actualizar un complemento

Con los complementos de vRealize Orchestrator, el servidor de vRealize Orchestrator puede integrarse con otros productos de software. vRealize Orchestrator se entrega con un conjunto de complementos predeterminados preinstalados. Puede ampliar las capacidades de la plataforma de vRealize Orchestrator si instala complementos personalizados.

Puede instalar o actualizar los complementos desde la página **Administrar complementos** de vRealize Orchestrator. La extensión de archivo que se puede utilizar es `.vmoapp`.

Para obtener más información sobre cómo instalar o actualizar complementos de vRealize Orchestrator, consulte [Instalar o actualizar un complemento de vRealize Orchestrator](#).

Cambiar el nivel de registro de complementos

En vez de cambiar el nivel de registro para vRealize Orchestrator, puede cambiarlo solo para complementos concretos.

Deshabilitar un complemento

Si desea deshabilitar un complemento, anule la selección de la opción **Habilitar complemento** junto al nombre del complemento.

Esta acción no quita el archivo del complemento. Para obtener más información sobre cómo desinstalar un complemento en vRealize Orchestrator, consulte [Eliminar un complemento](#).

Instalar o actualizar un complemento de vRealize Orchestrator

Puede instalar o actualizar complementos de terceros en el centro de control de vRealize Orchestrator.

Requisitos previos

Descargue el archivo `.dar` o `.vmoapp` del complemento.

Nota El formato de archivo preferido para los complementos de vRealize Orchestrator es `.vmoapp`.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Seleccione la página **Administrar complementos**.
- 3 Haga clic en **Examinar** y seleccione el archivo `.dar` o `.vmoapp` del complemento que desea instalar o actualizar.

- 4 Haga clic en **Cargar**.
- 5 Revise la información del complemento, si corresponde, acepte el acuerdo de licencia para el usuario final y haga clic en **Instalar**.

El complemento se instala o se actualiza entonces, y el servicio del servidor de vRealize Orchestrator se reinicia.

Pasos siguientes


Compruebe que la información del complemento que aparece en la página **Administrar complementos** es correcta.

Eliminar un complemento

Puede eliminar complementos de terceros de vRealize Orchestrator Appliance a través del Centro de control.

Nota A partir de vRealize Orchestrator 8.0, el paquete del complemento ya no se elimina manualmente del vRealize Orchestrator Client.

Procedimiento

- 1 Inicie sesión en el centro de control como usuario **raíz**.
- 2 Seleccione **Administrar complementos**.
- 3 Busque el complemento que desea eliminar y haga clic en el icono de eliminación ().
- 4 Confirme que desea eliminar el complemento y, a continuación, haga clic en **Eliminar**.

Resultados

Ha eliminado el complemento de vRealize Orchestrator Appliance.

Alta disponibilidad de vRealize Orchestrator

Para incrementar la disponibilidad de los servicios de vRealize Orchestrator, inicie varias instancias del servidor de vRealize Orchestrator en un clúster con una base de datos compartida. vRealize Orchestrator funciona como una sola instancia hasta que se configura para que funcione como parte de un clúster.

Varias instancias del servidor de vRealize Orchestrator con configuraciones idénticas de servidor y de complemento funcionan conjuntamente en un clúster y comparten una base de datos.

Todas las instancias del servidor de vRealize Orchestrator se comunican entre sí mediante el intercambio de latidos. Cada latido es una marca de hora que el nodo escribe en la base de datos compartida del clúster cada cierto intervalo de tiempo. Los problemas de red, un servidor de base de datos bloqueado o una sobrecarga podrían hacer que un nodo de clúster de vRealize Orchestrator dejase de responder. Si una instancia activa del servidor de vRealize Orchestrator no consigue enviar latidos dentro del tiempo de espera de conmutación por error, se considera

bloqueado. El tiempo de espera de conmutación por error equivale al valor del intervalo de latidos multiplicado por el número de latidos de conmutación por error. Sirve como definición para un nodo no fiable; asimismo, se puede personalizar conforme a los recursos disponibles y a la carga de producción.

Un nodo de vRealize Orchestrator pasa al modo de espera cuando pierde la conexión con la base de datos y permanece así hasta que se restaura la conexión de la base de datos. Los otros nodos del clúster se encargan del trabajo activo; para ello, reanudan todos los flujos de trabajo interrumpidos a partir de los últimos elementos inacabados, por ejemplo tareas de scripts o invocaciones de flujos de trabajo.

Puede supervisar el estado del clúster de vRealize Orchestrator desde la página **Administración de clústeres de Orchestrator** del centro de control de vRealize Orchestrator. También puede usar esta página para configurar los latidos de clúster, el número de latidos de conmutación por error y el número de nodos de vRealize Orchestrator activos.

Valores máximos de escalabilidad de vRealize Orchestrator

En la tabla de límites de escalabilidad se describen los valores máximos recomendados en implementaciones de vRealize Orchestrator 8.x.

Componente	Destinos de escala	Más información
Máquinas virtuales	35.000	
Conexiones de vCenter Server	10	Consulte Configuración de vCenter Server
Nodos activos en un clúster	3	Consulte Configurar un clúster de vRealize Orchestrator
Flujos de trabajo en ejecución simultánea	300 por nodo	Consulte Configurar las propiedades de ejecución de los flujos de trabajo
Flujos de trabajo en ejecución en cola	10.000 por nodo	
Ejecuciones de flujos de trabajo conservadas	100 por nodo	
Días para caducidad de evento de registro	15	

Configurar un clúster de vRealize Orchestrator

Puede configurar la nueva implementación de vRealize Orchestrator para que se ejecute en alta disponibilidad. Para ello, debe implementar tres nodos y conectarlos como un clúster.

Un clúster de vRealize Orchestrator consta de tres instancias de vRealize Orchestrator que comparten una base de datos de PostgreSQL común. La base de datos del clúster de vRealize Orchestrator configurado solo puede ejecutarse en modo asincrónico.

Para crear un clúster de vRealize Orchestrator, debe seleccionar una instancia de vRealize Orchestrator para que sea el nodo principal del clúster. Después de configurar el nodo principal, debe unir los nodos secundarios a él.

El clúster de vRealize Orchestrator creado se configura previamente con conmutación por error automática.

Nota Un error en la conmutación por error automática puede provocar la pérdida de datos de la base de datos.

Requisitos previos

- Descargue e implemente tres instancias independientes de vRealize Orchestrator. Consulte [Descargar e implementar vRealize Orchestrator Appliance](#).

Nota El número recomendado de nodos que se pueden utilizar para crear un entorno de vRealize Orchestrator agrupado en clúster es tres.

- Compruebe que el acceso SSH esté habilitado para todos los nodos de vRealize Orchestrator. Consulte [Habilitar o deshabilitar el acceso SSH a vRealize Orchestrator Appliance](#).
- Configure un servidor del equilibrador de carga. Consulte la [Guía de equilibrio de carga de VMware vRealize Orchestrator 8.x](#).

Procedimiento

1 Configure el nodo principal.

- a Inicie sesión en el vRealize Orchestrator Appliance del nodo principal a través de SSH como **raíz**.
- b Para configurar el servidor del equilibrador de carga del clúster, ejecute el comando `vracli load-balancer set load_balancer_FQDN`.
- c Inicie sesión en el centro de control del nodo principal y seleccione **Ajustes del host**.
- d Haga clic en **Cambiar** y establezca la dirección del host del servidor del equilibrador de carga conectado.
- e Configure el proveedor de autenticación. Consulte [Configurar un servidor de vRealize Orchestrator independiente](#).

2 Una los nodos secundarios al nodo principal.

- a Inicie sesión en el vRealize Orchestrator Appliance del nodo secundario a través de SSH como **raíz**.
- b Para unir el nodo secundario al nodo principal, ejecute el comando `vracli cluster join primary_node_hostname_or_IP`.
- c Introduzca la contraseña raíz del nodo principal.
- d Repita el procedimiento para otro nodo secundario.

- 3 (opcional) Si el nodo principal utiliza un certificado personalizado, debe establecer el certificado en el dispositivo o generar un nuevo certificado. Consulte [Generar un certificado TLS personalizado para vRealize Orchestrator](#).

Nota El archivo que contiene la cadena de certificados debe tener codificación PEM.

- 4 Finalice la implementación del clúster.
 - a Inicie sesión en el vRealize Orchestrator Appliance del nodo principal a través de SSH como **raíz**.
 - b Para confirmar que todos los nodos se encuentran en estado listo, ejecute el comando `kubect1 -n prelude get nodes`.
 - c Ejecute el script `/opt/scripts/deploy.sh` y espere a que finalice la implementación.

Resultados

Se creó un clúster de vRealize Orchestrator. Después de crear el clúster, puede acceder al entorno de vRealize Orchestrator solo desde la dirección FQDN del servidor del equilibrador de carga.

Nota Debido a que solo puede acceder al centro de control del clúster con la contraseña raíz del equilibrador de carga, no puede editar la configuración de un nodo del clúster si tiene una contraseña raíz diferente. Para editar la configuración de este nodo, elimínelo del equilibrador de carga, edite la configuración en el centro de control y vuelva a agregar el nodo al equilibrador de carga.

Pasos siguientes

Para supervisar el estado del clúster de vRealize Orchestrator, inicie sesión en el centro de control y seleccione la página **Administración de clústeres de Orchestrator**. Consulte [Supervisar un clúster de vRealize Orchestrator](#).

Eliminar un nodo de clúster de vRealize Orchestrator

Puede eliminar una instancia de vRealize Orchestrator para poder reducir la capacidad del clúster.

Después de eliminar un nodo del clúster de vRealize Orchestrator, ese nodo dejará de funcionar. Si desea volver a utilizar este nodo, debe eliminar su vRealize Orchestrator Appliance de vCenter Server y volver a implementarlo. Consulte [Descargar e implementar vRealize Orchestrator Appliance](#).

Requisitos previos

Crear un clúster de vRealize Orchestrator. Consulte [Configurar un clúster de vRealize Orchestrator](#).

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance del nodo que desea eliminar como **raíz**.
- 2 Para eliminar el nodo de su vRealize Orchestrator, ejecute el comando `vracli cluster leave`.
- 3 Inicie sesión como **raíz** en la línea de comandos de vRealize Orchestrator Appliance de uno de los nodos restantes.
- 4 Ejecute el comando `kubectl -n prelude get nodes` y confirme que el nodo eliminado ya no forma parte del clúster.

Escalar horizontalmente una implementación de vRealize Orchestrator independiente

La disponibilidad y la escalabilidad de su implementación de vRealize Orchestrator configurada se pueden aumentar mediante el escalado horizontal.

Requisitos previos

- Descargue, implemente y configure una instancia de vRealize Orchestrator. Consulte [Descargar e implementar vRealize Orchestrator Appliance](#) y [Configurar un servidor de vRealize Orchestrator independiente](#).
- Descargue e implemente dos instancias más de vRealize Orchestrator. Consulte [Descargar e implementar vRealize Orchestrator Appliance](#).
- Configure un servidor del equilibrador de carga. Consulte la [Guía de equilibrio de carga de VMware vRealize Orchestrator 8.x](#).

Procedimiento

- 1 Configure el nodo principal.
 - a Inicie sesión en el centro de control de la implementación de vRealize Orchestrator configurada como usuario **raíz**.
 - b Seleccione **Configurar proveedor de autenticación** y elimine del registro su proveedor de autenticación.
 - c Seleccione **Configuración de host** y escriba el nombre de host del servidor del equilibrador de carga.
 - d Seleccione **Configurar proveedor de autenticación** y vuelva a registrar el proveedor de autenticación.
 - e Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance de la instancia configurada como **raíz**.
 - f Para detener todos los servicios de la instancia de vRealize Orchestrator, ejecute el comando `/opt/scripts/deploy.sh --onlyClean`.

- g Para establecer el equilibrador de carga, ejecute `vracli load-balancer set load_balancer_FQDN`.
- h (opcional) Si la instancia de vRealize Orchestrator usa un certificado personalizado, ejecute el comando `vracli certificate ingress --set su_archivo_de_certificado.pem`.

Nota El archivo que contiene la cadena de certificados debe tener codificación PEM.

- 2 Una los nodos secundarios a la instancia configurada.
 - a Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance del nodo secundario como **raíz**.
 - b Para unir el nodo secundario a la instancia configurada, ejecute el comando `vracli cluster join nombre_de_host_o_IP_del_nodo_principal`.
 - c Repita el procedimiento en el otro nodo secundario.
- 3 Finalice el proceso de escalado horizontal.
 - a Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance de la instancia configurada como **raíz**.
 - b Ejecute `/opt/scripts/deploy.sh` y espere a que el script finalice.

Resultados

Ha escalado horizontalmente la implementación de vRealize Orchestrator.

Supervisar un clúster de vRealize Orchestrator

Puede supervisar el clúster de vRealize Orchestrator existente a través del centro de control de vRealize Orchestrator.

En la página **Administración de clústeres de Orchestrator** del centro de control puede supervisar los estados de sincronización de la configuración de las instancias de vRealize Orchestrator que se han unido en un clúster.

Estado de sincronización de la configuración	Descripción
EN EJECUCIÓN	El servicio de vRealize Orchestrator está disponible y puede aceptar solicitudes.
EN ESPERA	<p>El servicio de vRealize Orchestrator no puede procesar solicitudes porque:</p> <ul style="list-style-type: none"> ■ El nodo forma parte de un clúster de Alta disponibilidad (HA) y permanece en modo de espera hasta que falla el nodo principal. ■ El servicio no puede verificar los requisitos previos de configuración, como una conexión válida a la base de datos, el proveedor de autenticación y la licencia de instancia de vRealize Orchestrator.

Estado de sincronización de la configuración	Descripción
Error al recuperar el estado de la integridad del servicio	No se puede establecer contacto con el servicio del servidor de vRealize Orchestrator porque está detenido o se ha producido un error de red.
Reinicio pendiente	El centro de control detecta un cambio en la configuración y el servidor de vRealize Orchestrator se reinicia automáticamente.

Configurar el programa de mejora de la experiencia de cliente

Si opta por participar en el programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP), VMware recibe información anónima que ayuda a mejorar la calidad, la confiabilidad y la funcionalidad de los productos y servicios de VMware.

Categorías de información que recibe VMware

El programa de mejora de la experiencia del cliente (CEIP) proporciona a VMware información que le permite mejorar sus productos y servicios, además de solucionar problemas.

Los detalles relacionados con los datos recopilados mediante el CEIP, así como los fines para los que VMware los utiliza, se pueden encontrar en el Centro de seguridad y confianza en <http://www.vmware.com/trustvmware/ceip.html>. Para unirse al CEIP de este producto o abandonarlo, consulte [Unirse al programa de mejora de la experiencia de cliente o abandonarlo](#).

Unirse al programa de mejora de la experiencia de cliente o abandonarlo

Únase al programa de mejora de la experiencia de cliente desde la línea de comandos de vRealize Orchestrator Appliance.

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz**.
- 2 Para unirse al programa de mejora de la experiencia de cliente, ejecute el comando `vracli ceip on`.
- 3 Revise la información del programa de mejora de la experiencia de cliente y ejecute el comando `vracli ceip on --acknowledge-ceip`.
- 4 Reinicie los servicios de vRealize Orchestrator.
 - a Para reiniciar el servicio del servidor, ejecute el comando `kubect1 -n prelude exec -it your_vro_pod -c vco-server-app /bin/bash`.
 - b Para detener el servicio, ejecute el comando `kill 1`.

- c Para reiniciar el servicio del centro de control, ejecute el comando `kubect1 -n prelude exec -it your_vro_pod -c vco-controlcenter-app /bin/bash`.
 - d Para detener el servicio, ejecute el comando `kill 1`.
- 5 Para abandonar del programa de mejora de la experiencia de cliente, ejecute el comando `vracli ceip off`.
 - 6 Repita los pasos para reiniciar los servicios.

Usar los servicios de API de vRealize Orchestrator

6

Además de configurar vRealize Orchestrator mediante el centro de control, puede modificar la configuración del servidor de vRealize Orchestrator mediante la API de REST de vRealize Orchestrator, la API de REST del centro de control o la utilidad de la línea de comandos que se almacenan en el dispositivo.

El complemento Configuración se incluye de forma predeterminada en el paquete de vRealize Orchestrator. Puede acceder a los flujos de trabajo del complemento Configuración desde la biblioteca de flujos de trabajo de vRealize Orchestrator o la API de REST de vRealize Orchestrator. Con estos flujos de trabajo, puede cambiar la configuración del certificado de confianza y el almacén de claves del servidor de vRealize Orchestrator. Para obtener información sobre todas las llamadas de servicio de API de REST de vRealize Orchestrator disponibles, consulte la documentación de la *API del servidor de vRealize Orchestrator* en https://your_orchestrator_FQDN/vco/api/docs.

■ Administrar certificados TLS y almacenes de claves con la API de REST

Aparte de administrar certificados TLS mediante el centro de control, también puede administrar los certificados y los almacenes de claves de confianza al ejecutar flujos de trabajo desde el complemento Configuración o mediante la API de REST.

Administrar certificados TLS y almacenes de claves con la API de REST

Aparte de administrar certificados TLS mediante el centro de control, también puede administrar los certificados y los almacenes de claves de confianza al ejecutar flujos de trabajo desde el complemento Configuración o mediante la API de REST.

El complemento Configuración contiene flujos de trabajo para importar y eliminar certificados TLS y almacenes de claves. Para acceder a estos flujos de trabajo, desplácese hasta **Biblioteca > Flujos de trabajo > Administrador de confianza de SSL** y **Biblioteca > Flujos de trabajo > Almacenes de claves** en el vRealize Orchestrator Client. Estos flujos de trabajo también se pueden ejecutar mediante la API de REST de vRealize Orchestrator.

La API de REST del centro de control facilita el acceso a los recursos para configurar el servidor de vRealize Orchestrator. Esta API de REST del centro de control se puede utilizar con sistemas de terceros para automatizar la configuración de vRealize Orchestrator. El endpoint raíz de la API de REST del centro de control es `https://your_orchestrator_FQDN/vco/api`. Para obtener información sobre todas las llamadas de servicio disponibles que se pueden realizar a la API de REST del centro de control, consulte la documentación de la *API del centro de control de vRealize Orchestrator* en `https://your_orchestrator_FQDN/vco-controlcenter/docs`.

Eliminar un certificado TLS mediante la API de REST

Para eliminar un certificado TLS, ejecute el flujo de trabajo Eliminar certificado de confianza del complemento Configuración o mediante la API de REST.

Procedimiento

- 1 Realice una solicitud `GET` en la dirección URL del servicio Flujo de trabajo del flujo de trabajo Eliminar certificado de confianza.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name>Delete trusted certificate
```

- 2 Recupere la definición del flujo de trabajo Eliminar certificado de confianza haciendo una solicitud `GET` en la URL de la definición.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd
```

- 3 Realice una solicitud `POST` en la URL que contiene los objetos de ejecución del flujo de trabajo Eliminar certificado de confianza.

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd/executions/
```

- 4 Proporcione el nombre del certificado que desea eliminar como parámetro de entrada del flujo de trabajo Eliminar certificado de confianza en un elemento de contexto de ejecución en el cuerpo de la solicitud.

Importar certificados TLS mediante la API de REST

Puede importar certificados TLS ejecutando un flujo de trabajo desde el complemento Configuración o utilizando la API de REST.

Puede importar un certificado de confianza desde un archivo o una dirección URL. Consulte [Importar un certificado de confianza con el centro de control](#)

Procedimiento

- 1 Haga una solicitud `GET` en la URL del servicio Flujo de trabajo.

Opción	Descripción
Importar certificado de confianza desde un archivo	Importa un certificado de confianza desde un archivo.
Importar certificado de confianza desde una URL	Importa un certificado de confianza desde una dirección URL.
Importar certificado de confianza desde una URL utilizando un servidor proxy	Importa un certificado de confianza desde una dirección URL utilizando un servidor proxy.
Importar certificado de confianza desde una URL con alias de certificado	Importa un certificado de confianza con un alias de certificado, desde una dirección URL.

Para importar un certificado de confianza desde un archivo, haga la solicitud `GET` siguiente:

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Import
trusted certificate from a file
```

- 2 Recupere la definición del flujo de trabajo haciendo una solicitud `GET` en la URL de la definición.

Para recuperar la definición del flujo de trabajo Importar certificado de confianza desde un archivo, haga la solicitud `GET` siguiente:

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/
93a7bb21-0255-4750-9293-2437abe9d2e5
```

- 3 Realice una solicitud `POST` en la URL que contiene los objetos de ejecución del flujo de trabajo.

Para el flujo de trabajo Importar certificado de confianza desde un archivo, haga la solicitud `POST` siguiente:

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/
93a7bb21-0255-4750-9293-2437abe9d2e5/executions
```

- Proporcione valores para los parámetros de entrada del flujo de trabajo en un elemento de contexto de ejecución del cuerpo de la solicitud.

Parámetro	Descripción
cer	El archivo CER del que desea importar el certificado TLS. Este parámetro se aplica al flujo de trabajo Importar certificado de confianza desde un archivo.
url	La URL de la que desea importar el certificado TLS. En el caso de los servicios que no sean HTTPS, el formato admitido es <i>dirección_IP_o_nombre_DNS:puerto</i> . Este parámetro se aplica al flujo de trabajo Importar certificado de confianza desde una URL.

Creación de un almacén de claves mediante la API de REST

Puede crear un almacén de claves ejecutando el flujo de trabajo Crear un almacén de claves del complemento Configuración o utilizando la API de REST.

Procedimiento

- Haga una solicitud **GET** en la URL del servicio Flujo de trabajo del flujo de trabajo Crear un almacén de claves.

```
GET https://{host_orchestrator}:{puerto}/vco/api/workflows?conditions=name=Create a keystore
```

- Recupere la definición del flujo de trabajo Crear un almacén de claves realizando una solicitud **GET** en la URL de la definición.

```
GET https://{host_orchestrator}:{puerto}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

- Haga una solicitud **POST** en la URL que contiene los objetos de ejecución del flujo de trabajo Crear un almacén de claves.

```
POST https://{host_orchestrator}:{puerto}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/executions/
```

- Proporcione el nombre del almacén de claves que desea crear como parámetro de entrada del flujo de trabajo Crear un almacén de claves en un elemento de contexto de ejecución en el cuerpo de la solicitud.

Eliminación de un almacén de claves mediante la API de REST

Puede eliminar un almacén de claves ejecutando el flujo de trabajo Eliminar un almacén de claves del complemento Configuración o utilizando la API de REST.

Procedimiento

- 1 Haga una solicitud `GET` en la URL del servicio Flujo de trabajo del flujo de trabajo Eliminar un almacén de claves.

```
GET https://{host_orchestrator}:{puerto}/vco/api/workflows?conditions=name>Delete a
keystore
```

- 2 Recupere la definición del flujo de trabajo Eliminar un almacén de claves realizando una solicitud `GET` en la URL de la definición.

```
GET https://{host_orchestrator}:{puerto}/vco/api/workflows/
7a3389eb-1fab-4d77-860b-81b66bb45b86/
```

- 3 Haga una solicitud `POST` en la URL que contiene los objetos de ejecución del flujo de trabajo Eliminar un flujo de trabajo.

```
POST https://{host_orchestrator}:{puerto}/vco/api/workflows/
7a3389eb-1fab-4d77-860b-81b66bb45b86/executions/
```

- 4 Proporcione el almacén de claves que desee eliminar como parámetro de entrada del flujo de trabajo Eliminar un almacén de claves en un elemento de contexto de ejecución en el cuerpo de la solicitud.

Adición de una clave mediante la API de REST

Puede añadir una clave ejecutando el flujo de trabajo Añadir clave del complemento Configuración o utilizando la API de REST.

Procedimiento

- 1 Haga una solicitud `GET` en la URL del servicio Flujo de trabajo del flujo de trabajo Añadir clave.

```
GET https://{host_orchestrator}:{puerto}/vco/api/workflows?conditions=name=Add key
```

- 2 Recupere la definición del flujo de trabajo Añadir clave realizando una solicitud `GET` en la URL de la definición.

```
GET https://{host_orchestrator}:{puerto}/vco/api/workflows/6c301bff-e8fe-4ae0-
ad08-5318178594b3/
```

- 3 Haga una solicitud `POST` en la URL que contiene los objetos de ejecución del flujo de trabajo Añadir clave.

```
POST https://{host_orchestrator}:{puerto}/vco/api/workflows/6c301bff-e8fe-4ae0-
ad08-5318178594b3/executions/
```

- 4 Proporcione el almacén de claves, el alias de la clave, la clave con codificación PEM, la cadena de certificados y la contraseña de la clave como parámetros de entrada del flujo de trabajo Añadir clave en un elemento de contexto de ejecución del cuerpo de la solicitud.

Opciones de configuración adicionales

7

Puede utilizar el centro de control para cambiar el comportamiento predeterminado de vRealize Orchestrator.

Este capítulo incluye los siguientes temas:

- [Volver a configurar la autenticación](#)
- [Configurar las propiedades de ejecución de los flujos de trabajo](#)
- [Archivos de registro de vRealize Orchestrator](#)
- [Habilitar las extensiones de Opentracing y Wavefront](#)
- [Habilitar la sincronización de hora de vRealize Orchestrator](#)
- [Desactivar la sincronización de hora vRealize Orchestrator](#)
- [Configurar CIDR de Kubernetes de vRealize Orchestrator](#)
- [Actualizar la configuración de DNS para vRealize Orchestrator](#)

Volver a configurar la autenticación

Después de configurar el método de autenticación durante la configuración inicial del Centro de control, puede cambiar el proveedor de autenticación o los parámetros configurados en cualquier momento.

Cambiar el proveedor de autenticación

Para cambiar el modo de autenticación o la configuración de conexión del proveedor de autenticación, debe, en primer lugar, eliminar del registro el proveedor de autenticación existente.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 En la página **Configurar proveedor de autenticación**, haga clic en el botón **ELIMINAR DEL REGISTRO** junto al cuadro de texto de la dirección de host para eliminar del registro el proveedor de autenticación en uso.

Resultados

El proveedor de autenticación se ha eliminado del registro correctamente.

Pasos siguientes

Vuelva a configurar la autenticación en el centro de control. Consulte [Configurar un servidor de vRealize Orchestrator independiente](#).

Cambiar los parámetros de autenticación

Cuando utilice vSphere como un proveedor de autenticación en el centro de control, puede cambiar el tenant predeterminado del grupo de administradores de vRealize Orchestrator.

Requisitos previos

Configure vSphere como el proveedor de autenticación para la implementación de vRealize Orchestrator. Consulte [Configurar un servidor de vRealize Orchestrator independiente con la autenticación de vSphere](#).

Nota La autenticación de vRealize Automation no incluye estos parámetros.

Procedimiento

- 1 Inicie sesión en el centro de control como usuario **raíz**.
- 2 Seleccione **Configurar proveedor de autenticación**.
- 3 Haga clic en el botón **CAMBIAR** situado junto al cuadro de texto **Tenant predeterminado**.
- 4 Reemplace el nombre del tenant.
- 5 Haga clic en el botón **CAMBIAR** situado junto al cuadro de texto **Grupo de administradores**.

Nota Si no vuelve a configurar el grupo de administradores, este permanece vacío y ya podrá acceder al centro de control.

- 6 Introduzca el nombre de un grupo de administradores y haga clic en **BUSCAR**.
- 7 Seleccione un grupo de administradores.
- 8 Cambie el grupo de administradores.
- 9 Para finalizar la edición de los parámetros de autenticación, haga clic en **GUARDAR CAMBIOS**.

Configurar las propiedades de ejecución de los flujos de trabajo

De forma predeterminada, puede ejecutar hasta 300 flujos de trabajo por nodo; asimismo, puede poner en cola hasta 10.000 flujos de trabajo si se llega a la cantidad de flujos de trabajo en ejecución.

Cuando el nodo de vRealize Orchestrator debe ejecutar más de 300 flujos de trabajo simultáneos, las ejecuciones de flujos de trabajo pendientes se ponen en cola. Cuando finaliza la ejecución de un flujo de trabajo, empieza la ejecución del siguiente flujo de trabajo de la cola. Si se llega al máximo de flujos de trabajo en cola, el siguiente flujo de trabajo no puede ejecutarse hasta que comienza a ejecutarse uno de los flujos de trabajo pendientes.

Puede configurar las propiedades de ejecución de flujo de trabajo en la página **Opciones avanzadas** del centro de control.

Opción	Descripción
Habilitar modo seguro	Si el modo seguro está habilitado, se cancelan todos los flujos de trabajo en ejecución y no se reanudan la próxima vez que se inicie el nodo de vRealize Orchestrator.
Cantidad de flujos de trabajo en ejecución simultánea	El número de flujos de trabajo que se ejecutan simultáneamente. El valor predeterminado es 300 flujos de trabajo por nodo.
Cantidad máxima de flujos de trabajo en ejecución en la cola	Cantidad de solicitudes de ejecución de flujo de trabajo que el servidor de vRealize Orchestrator acepta antes de pasar al estado de no disponible. El valor predeterminado es 10.000 flujos de trabajo por nodo.
Cantidad máxima de ejecuciones conservadas por flujo de trabajo	Número máximo de ejecuciones de flujo de trabajo finalizadas que se mantienen como historial por flujo de trabajo. Si se sobrepasa ese número, se eliminan las ejecuciones de flujos de trabajo más antiguas. El valor predeterminado es 100 ejecuciones por flujo de trabajo.
Días de caducidad para eventos de log	Cantidad de días que los eventos de registro se mantienen en la base de datos antes de purgarse. El valor predeterminado es 15 días.

Archivos de registro de vRealize Orchestrator

De forma sistemática, el soporte técnico de VMware solicita información de diagnóstico cuando se le envía una solicitud de soporte. Dicha información de diagnóstico contiene logs y archivos de configuración específicos del producto del host en el que se ejecuta el producto.

Los registros de vRealize Orchestrator Appliance se almacenan en el directorio `/data/vco/usr/lib/vco/app-server/logs/`. Para exportar los registros de su implementación de vRealize Orchestrator Appliance, inicie sesión en la línea de comandos del dispositivo y ejecute el comando `vracli log-bundle`. El paquete de registros generado se guardará en la carpeta raíz de vRealize Orchestrator Appliance.

Persistencia del registro

Puede registrar información en cualquier tipo de script de vRealize Orchestrator, por ejemplo, flujo de trabajo, directiva o acción. Esta información tiene tipos y niveles. El tipo puede ser persistente o no persistente. El nivel puede ser `DEBUG`, `INFO`, `WARN`, `ERROR`, `TRACE` y `FATAL`.

Tabla 7-1. Crear registros persistentes y no persistentes

Nivel de registro	Tipo persistente	Tipo no persistente
DEBUG	Server.debug("texto corto", "texto largo");	System.debug("texto")
INFO	Server.log("texto corto", "texto largo");	System.log("texto");
WARN	Server.warn("texto corto", "texto largo");	System.warn("texto");
ERROR	Server.error("texto corto", "texto largo");	System.error("texto");

Registros persistentes

Los registros persistentes (registros de servidor) realizan un seguimiento de registros de ejecuciones de flujos de trabajo anteriores y se almacenan en la base de datos de vRealize Orchestrator.

Registros no persistentes

Cuando se utiliza un registro no persistente (registro del sistema) para crear scripts, el servidor de vRealize Orchestrator notifica sobre este registro a todas las aplicaciones de vRealize Orchestrator en ejecución, pero esta información no se almacena en la base de datos. Cuando se reinicia la aplicación, se pierde la información del registro. Los registros no persistentes se utilizan para fines de depuración y para información en directo. Para ver registros del sistema, debe seleccionar una ejecución de flujo de trabajo completada en el vRealize Orchestrator Client y seleccionar la pestaña **Registros**.

Configuración de registros de vRealize Orchestrator

En la página **Configurar logs** en el centro de control, puede establecer el nivel del log del servidor y del log de creación de scripts que necesite. Si alguno de los logs se genera varias veces al día, resulta complicado determinar lo que causa problemas.

El nivel de log predeterminado del log del servidor y del log de creación de scripts es **INFO**. Cambiar el nivel de log repercute en todos los mensajes nuevos que el servidor incorpora a los logs, así como en la cantidad de conexiones activas a la base de datos. El nivel de detalle de los registros disminuye en orden descendente.

Precaución Establezca el nivel de log únicamente en **DEPURAR** o en **TODO** para depurar un problema. No utilice esta configuración en un entorno de producción, ya que puede afectar gravemente al rendimiento.

Generar registros de vRealize Orchestrator

Para exportar los registros de la implementación, inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz** y ejecute el comando `vraccli log-bundle`. El paquete de registros generado se almacena en la carpeta raíz del dispositivo.

Nota Cuando hay más de una instancia de vRealize Orchestrator en un clúster, el paquete de registros incluye los registros de todas las instancias de vRealize Orchestrator que hay en el clúster.

Configurar la integración de registro con vRealize Log Insight

Puede configurar vRealize Orchestrator para que envíe su información de registro al servidor de vRealize Log Insight.

Puede configurar una integración de registro en un servidor de vRealize Log Insight a través de la línea de comandos de vRealize Orchestrator Appliance.

Nota Para obtener información sobre cómo configurar una integración de registro con un servidor syslog remoto, consulte [Crear o sobrescribir una integración de syslog en vRealize Orchestrator](#).

Requisitos previos

- Configure el servidor de vRealize Log Insight. Consulte la *documentación de vRealize Log Insight*.
- Compruebe que la versión de vRealize Log Insight es la 4.7.1 o una posterior.

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz**.
- 2 Para configurar la integración de registros con vRealize Log Insight, ejecute el comando `vracli vrli set VRLI_FQDN`.

Nota Si su instancia de vRealize Orchestrator utiliza un certificado autofirmado, puede deshabilitar la autenticación SSL si incluye el argumento opcional `-k` o `--insecure`.

Pasos siguientes

Para obtener más información sobre las opciones de configuración de vRealize Log Insight, ejecute el comando `vracli vrli -h`.

Crear o sobrescribir una integración de syslog en vRealize Orchestrator

Puede configurar vRealize Orchestrator para enviar la información de registro a uno o varios servidores syslog remotos.

El comando `vracli remote-syslog set` se utiliza para crear una integración de syslog o sobrescribir las integraciones existentes.

La integración de syslog remota de vRealize Orchestrator admite tres tipos de conexión:

- A través de UDP.
- A través de TCP sin TLS.

Nota Para crear una integración de syslog sin usar TLS, agregue la marca `--disable-ssl` al comando `vracli remote-syslog set`.

- A través de TCP con TLS.

Para obtener información sobre cómo configurar la integración de registro con vRealize Log Insight, consulte [Configurar la integración de registro con vRealize Log Insight](#).

Requisitos previos

Configure uno o varios servidores syslog remotos.

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz**.
- 2 Para crear una integración con un servidor syslog, ejecute el comando `vracli remote-syslog set`.

```
vracli remote-syslog set -id name_of_integration protocol_type://
syslog_URL_or_FQDN:syslog_port
```

Nota Si no introduce un puerto en el comando `vracli remote-syslog set`, el valor de puerto se establecerá de forma predeterminada en 514.

Nota Puede agregar un certificado a la configuración de syslog. Para agregar un archivo de certificado, utilice la marca `--ca-file`. Para agregar un certificado como texto sin formato, utilice la marca `--ca-cert`.

- 3 (opcional) Para sobrescribir una integración de syslog existente, ejecute `vracli remote-syslog set` y establezca el valor de la marca `-id` en el nombre de la integración que desea sobrescribir.

Nota De forma predeterminada, vRealize Orchestrator Appliance solicitará que confirme que desea sobrescribir la integración de syslog. Si desea omitir esta solicitud de confirmación, agregue la marca `-f` o `--force` al comando `vracli remote-syslog set`.

Pasos siguientes

Para revisar las integraciones actuales de syslog en el dispositivo, ejecute el comando `vracli remote-syslog`.

Eliminar una integración de syslog en vRealize Orchestrator

Para eliminar las integraciones de syslog de vRealize Orchestrator Appliance, puede ejecutar el comando `vracli remote-syslog unset`.

Requisitos previos

Cree una o varias integraciones de syslog en vRealize Orchestrator Appliance. Consulte [Crear o sobrescribir una integración de syslog en vRealize Orchestrator](#).

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz**.
- 2 Elimine las integraciones de syslog de vRealize Orchestrator Appliance.
 - a Para eliminar una integración de syslog específica, ejecute el comando `vracli remote-syslog unset -id Integration_name`.
 - b Para eliminar todas las integraciones de syslog de vRealize Orchestrator Appliance, ejecute el comando `vracli remote-syslog unset` sin la marca `-id`.

Nota De forma predeterminada, vRealize Orchestrator Appliance solicita que confirme que desea eliminar todas las integraciones de syslog. Si desea omitir esta solicitud de confirmación, agregue la marca `-f` o `--force` al comando `vracli remote-syslog unset`.

Habilitar el registro de depuración de Kerberos

Puede solucionar los problemas del complemento de vRealize Orchestrator modificando el archivo de configuración de Kerberos que el complemento utiliza.

El archivo de configuración de Kerberos se encuentra en el directorio `/data/vco/usr/lib/vco/app-server/conf/` de vRealize Orchestrator Appliance.

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz**.
- 2 Ejecute el comando `kubect1 -n prelude edit deployment vco-app`.
- 3 En el archivo de implementación, busque y edite la cadena `-Djava.security.krb5.conf=/usr/lib/vco/app-server/conf/krb5.conf'`.

```
-Djava.security.krb5.conf=/usr/lib/vco/app-server/conf/krb5.conf
-Dsun.security.krb5.debug=true'
```

- 4 Guarde los cambios y salga del editor de archivos.
 - 5 Ejecute el comando `kubect1 -n prelude get pods`.
- Espere a que todos los pods se estén ejecutando.

6 Compruebe que el registro de depuración de Kerberos esté habilitado.

```
kubectl -n prelude log {vco_app_name} -c vco-server-app | grep krb5
```

Compruebe que los logs contengan un mensaje similar.

```
kubectl -n prelude log vco-app-5c965f9b9d-v8srd -c vco-server-app | grep krb5
12:23:05,417 INFO 011N:75 - Sysprop: java.security.krb5.conf = /usr/lib/vco/app-server/
conf/krb5.conf
12:23:05,421 INFO 011N:75 - Sysprop: sun.security.krb5.debug = true
2019-10-22 12:23:38.521+0000 [Thread-19] INFO {} [011N] Sysprop: java.security.krb5.conf
= /usr/lib/vco/app-server/conf/krb5.conf
2019-10-22 12:23:38.525+0000 [Thread-19] INFO {} [011N] Sysprop: sun.security.krb5.debug =
true
Java config name: /usr/lib/vco/app-server/conf/krb5.conf
EType: sun.security.krb5.internal.crypto.Aes256CtsHmacSha1EType
```

Habilitar las extensiones de Opentracing y Wavefront

Las extensiones de Opentracing y Wavefront para vRealize Orchestrator proporcionan herramientas que permiten recopilar datos sobre el entorno de vRealize Orchestrator. Estos datos se pueden utilizar para solucionar problemas del sistema y los flujos de trabajo de vRealize Orchestrator.

Antes de configurar vRealize Orchestrator para usar las extensiones de Opentracing y Wavefront, debe habilitarlas en vRealize Orchestrator Appliance.

Requisitos previos

- Compruebe que el servicio SSH de vRealize Orchestrator Appliance está habilitado. Consulte [Habilitar o deshabilitar el acceso SSH a vRealize Orchestrator Appliance](#).
- Si habilitó versiones anteriores de las extensiones Opentracing o Wavefront, debe eliminarlas antes de habilitar la versión actual. Por ejemplo, si habilitó previamente la versión 8.1.0 de la extensión Wavefront, debe ejecutar el comando `rm /data/vco/usr/lib/vco/app-server/extensions/wavefront-8.1.0.jar`.

Procedimiento

- 1 Inicie sesión en vRealize Orchestrator Appliance sobre SSH como **raíz**.
- 2 Para enumerar todas las extensiones disponibles, ejecute el comando `ls /data/vco/usr/lib/vco/app-server/extensions/`.
- 3 Ejecute el siguiente comando para habilitar la extensión de Opentracing:

```
mv /data/vco/usr/lib/vco/app-server/extensions/opentracing-8.5.0.jar.inactive /
data/vco/usr/lib/vco/app-server/extensions/opentracing-8.5.0.jar
```

4 Ejecute el siguiente comando para habilitar la extensión de Wavefront:

```
mv /data/vco/usr/lib/vco/app-server/extensions/wavefront-8.5.0.jar.inactive /
data/vco/usr/lib/vco/app-server/extensions/wavefront-8.5.0.jar
```

5 Inicie sesión en el centro de control y confirme que las extensiones aparecen en la página **Propiedades de extensión**.

Pasos siguientes

Configure la integración de Opentracing y Wavefront con vRealize Orchestrator en la página **Propiedades de extensión**. Consulte [Configurar la extensión de Opentracing](#) y [Configurar la extensión de Wavefront](#).

Configurar la extensión de Opentracing

La extensión de Opentracing envía datos sobre ejecuciones de flujos de trabajo a un servidor de Jaeger. Los datos incluyen el estado del flujo de trabajo, los parámetros de entrada y salida, el usuario que inició la ejecución del flujo de trabajo y los datos del identificador de flujo de trabajo.

Requisitos previos

- Compruebe que Opentracing esté habilitado en vRealize Orchestrator Appliance. Consulte [Habilitar las extensiones de Opentracing y Wavefront](#).
- Implemente un servidor de Jaeger para usarlo en la extensión de Opentracing. Para obtener más información, consulte la [documentación Introducción a Jaeger](#).

Procedimiento

- 1 Inicie sesión en el centro de control como usuario **raíz**.
- 2 Seleccione la página **Propiedades de extensión**.
- 3 Seleccione la extensión de Opentracing.
- 4 Introduzca la dirección y el puerto del host del servidor de Jaeger.

Nota Inserte dos barras diagonales ("/") antes de introducir la dirección del servidor.

- 5 Haga clic en **Guardar**.

Resultados

Se configuró la extensión de Opentracing para vRealize Orchestrator.

Pasos siguientes

- Para acceder a la interfaz de usuario de Jaeger que contiene los datos recopilados por la extensión de Opentracing, visite la dirección del host introducida durante la configuración.
- En la opción **Servicio**, seleccione **Flujos de trabajo**.

- Para especificar qué datos desea ver, utilice la opción **Etiquetas**. Por ejemplo, para ver los datos de los flujos de trabajo con errores, introduzca **status=failed**.

Configurar la extensión de Wavefront

Utilice la extensión de Wavefront para recopilar datos de métricas sobre el sistema y los flujos de trabajo de vRealize Orchestrator.

Requisitos previos

- 1 Compruebe que Wavefront esté habilitado en vRealize Orchestrator Appliance. Consulte [Habilitar las extensiones de Opentracing y Wavefront](#).
- 2 Importe el certificado de Wavefront:
 - a Inicie sesión en el centro de control de vRealize Orchestrator como usuario **raíz**.
 - b Seleccione la página **Certificados**.
 - c Haga clic en el menú desplegable **Importar** y seleccione **Importar de URL**.
 - d Introduzca la URL de Wavefront y haga clic en **Importar**.
- 3 Configure un proxy de Wavefront. Para obtener más información, consulte [Instalar y administrar proxy de Wavefront](#).

Procedimiento

- 1 Inicie sesión en el centro de control de vRealize Orchestrator como usuario **raíz**.
- 2 Seleccione la página **Propiedades de extensión**.
- 3 Seleccione la extensión de Wavefront.
- 4 Configure las propiedades de Wavefront.

Opción	Descripción
Proxy	La dirección del proxy de Wavefront.
Host	Opcional. La dirección de host de Wavefront.
Token	Opcional. El token de API de Wavefront. Para obtener más información sobre cómo generar un token de API de Wavefront, consulte Generar un token de API .
Prefijo	Agregue etiquetas de prefijo a cada métrica enviada a Wavefront. Las etiquetas de prefijo se separan mediante un símbolo de punto.

- 5 (opcional) Seleccione **Enviar panel de control predeterminado en el siguiente inicio**.
- 6 Haga clic en **Guardar**.

Resultados

Se configuró la extensión de Wavefront para vRealize Orchestrator.

Pasos siguientes

- Para acceder a las métricas recopiladas por Wavefront, acceda al panel de control de la dirección introducida durante la configuración.
- Para obtener notificaciones sobre eventos específicos del entorno de vRealize Orchestrator, puede utilizar las alertas de Wavefront. Para obtener más información, consulte la [Documentación sobre las alertas de Wavefront](#).

Habilitar la sincronización de hora de vRealize Orchestrator

Puede habilitar la sincronización de hora en la implementación de vRealize Orchestrator con la línea de comandos de vRealize Orchestrator Appliance.

Puede configurar la sincronización de hora de la implementación de vRealize Orchestrator independiente o agrupada en clúster mediante el protocolo de comunicación Protocolo de tiempo de redes (NTP). vRealize Orchestrator admite dos configuraciones de NTP que son mutuamente excluyentes:

Configuración de NTP	Descripción
ESXi	<p>Esta configuración puede utilizarse cuando el servidor de ESXi que aloja vRealize Orchestrator Appliance está sincronizado con un servidor NTP. Si utiliza una implementación agrupada en clúster, todos los hosts ESXi deben estar sincronizados con un servidor NTP. Si desea obtener más información sobre la configuración de NTP para ESXi, consulte Configurar el protocolo de tiempo de redes (Network Time Protocol, NTP) en un host ESXi mediante vSphere Web Client.</p> <p>Nota Puede experimentar un desplazamiento del reloj si la implementación de vRealize Orchestrator se migra a un host ESXi que no esté sincronizado con un servidor NTP.</p>
systemd	<p>Esta configuración utiliza el daemon de systemd-timesyncd para sincronizar los relojes de la implementación de vRealize Orchestrator.</p> <p>Nota De forma predeterminada, el daemon de systemd-timesyncd está habilitado, pero no tiene servidores NTP configurados. Si vRealize Orchestrator Appliance utiliza una configuración de IP dinámica, el dispositivo puede utilizar cualquier servidor NTP que el protocolo DHCP reciba.</p>

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz**.

2 Habilite NTP con ESXi.

- a Ejecute el comando `vracli ntp esxi`.
- b (opcional) Para confirmar el estado de la configuración de NTP, ejecute el comando `vracli ntp status`.

3 Habilite NTP con systemd.

- a Ejecute el comando `vracli ntp systemd --set FQDN_or_IP_of_systemd_server`.

Nota Puede agregar varios servidores NTP systemd separando las direcciones de red con una coma. Cada dirección de red debe colocarse entre comillas simples. Por ejemplo, `vracli ntp systemd --set 'dirección_ntp_1','dirección_ntp_2'`

- b (opcional) Para confirmar el estado de la configuración de NTP, ejecute el comando `vracli ntp status`.

Resultados

Ha habilitado la sincronización de hora para su implementación de vRealize Orchestrator.

Pasos siguientes

Se puede producir un error en la configuración de NTP si hay una diferencia de más de 10 minutos entre el servidor NTP y la implementación de vRealize Orchestrator. Para solucionar este problema, reinicie vRealize Orchestrator Appliance.

Desactivar la sincronización de hora vRealize Orchestrator

Puede desactivar la sincronización de hora del Protocolo de tiempo de redes (NTP) en la implementación de vRealize Orchestrator con la línea de comandos de vRealize Orchestrator Appliance.

Asimismo, puede restablecer el estado predeterminado de la configuración de NTP de vRealize Orchestrator Appliance mediante la ejecución del comando `vracli ntp reset`.

Requisitos previos

Compruebe haber configurado la sincronización de hora con ESXi o systemd. Consulte [Habilitar la sincronización de hora de vRealize Orchestrator](#).

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz**.
- 2 Para desactivar la sincronización de hora con ESXi o systemd, ejecute el comando `vracli ntp disable`.
- 3 (opcional) Para confirmar el estado de la configuración de NTP, ejecute el comando `vracli ntp status`.

Configurar CIDR de Kubernetes de vRealize Orchestrator

Puede cambiar las máscaras de subred de enrutamiento entre dominios sin clases (CIDR) de Kubernetes después de la implementación.

El vRealize Orchestrator Appliance configura y ejecuta un clúster de Kubernetes. Los pods y los servicios de este clúster se implementan en subredes IPv4 independientes, representadas por el CIDR de clúster interno y el CIDR de servicio interno, respectivamente. Los valores predeterminados de las máscaras de subred establecidos durante la implementación de OVF son los siguientes:

Kubernetes network property	Default value	Property description
<code>cluster-cidr</code>	10.244.0.0/22	El CIDR utilizado para pods que se ejecutan dentro del clúster de Kubernetes.
<code>service-cidr</code>	10.244.4.0/22	El CIDR utilizado para servicios de Kubernetes dentro del clúster de Kubernetes.

Las direcciones de red CIDR predeterminadas pueden generar un conflicto con redes privadas externas que el usuario podría estar utilizando. En estos escenarios, puede cambiar la configuración de estos valores de CIDR durante o después de implementar el vRealize Orchestrator Appliance.

Nota Para obtener información sobre cómo cambiar la configuración de CIDR durante la implementación del dispositivo, consulte [Descargar e implementar vRealize Orchestrator Appliance](#).

Requisitos previos

- Compruebe que los valores de dirección CIDR admitan al menos 1024 hosts.
- El CIDR de clúster interno y el CIDR de servicio interno no deben compartir el mismo valor de subred.
- El valor de CIDR de una de las subredes no puede incluir el valor que desea agregar a la otra subred.

Nota Por ejemplo, el valor de `cluster-cidr` no puede ser **10.244.4.0/22 10.244.4.0/24**, ya que también incluiría el valor de subred de la propiedad `service-cidr`. Cada valor de subred debe agregarse por separado.

Procedimiento

- 1 Inicie sesión en vRealize Orchestrator Appliance como **usuario raíz**.
- 2 Ejecute el comando `vracli upgrade exec -y --prepare --profile k8s-subnets`.

- 3 Haga una copia de seguridad de la implementación de vRealize Orchestrator creando una instantánea de la máquina virtual (Virtual Machine, VM). Consulte [Crear una instantánea de una máquina virtual](#).

Precaución En este momento, vRealize Orchestrator 8.x no admite instantáneas de memoria. Antes de realizar la instantánea de la implementación de vRealize Orchestrator, compruebe que la opción **Crear instantánea de la memoria de la máquina virtual** esté desactivada.

- 4 Cambie los valores de las subredes CIDR de clúster y CIDR de servicio ejecutando el comando `vracli network k8s-subnets`.

```
vracli network k8s-subnets --cluster-cidr <CIDR_value> --service-cidr <CIDR_value>
```

- 5 Para finalizar el proceso de configuración de CIDR, ejecute el comando `vracli upgrade exec`.

Actualizar la configuración de DNS para vRealize Orchestrator

Un administrador puede actualizar la configuración de DNS de la implementación de vRealize Orchestrator mediante el comando `vracli network dns`.

Requisitos previos

Compruebe que el servicio SSH de vRealize Orchestrator Appliance está habilitado. Consulte [Habilitar o deshabilitar el acceso SSH a vRealize Orchestrator Appliance](#).

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance a través de SSH como **raíz**.

Nota Para las implementaciones en clúster, inicie sesión en el dispositivo de cualquier nodo del clúster.

- 2 Para establecer nuevos servidores DNS en la implementación de vRealize Orchestrator, ejecute el comando `vracli network dns set`.

```
vracli network dns set --servers DNS1,DNS2
```

- 3 Compruebe que los nuevos servidores DNS se apliquen correctamente a todos los nodos de vRealize Orchestrator mediante la ejecución del comando `vracli network dns status`.

- 4 Para detener los servicios de vRealize Orchestrator en la implementación, ejecute el siguiente conjunto de comandos:

```
/opt/scripts/svc-stop.sh  
sleep 120  
/opt/scripts/deploy.sh --onlyClean
```

- 5 Reinicie los nodos de vRealize Orchestrator y espere a que se inicien por completo.
- 6 Inicie sesión en la línea de comandos de cada nodo de vRealize Orchestrator a través de SSH y compruebe que los nuevos servidores DNS aparezcan en el archivo `/etc/resolve.conf`.
- 7 Para iniciar los servicios de vRealize Orchestrator, ejecute el script `/opt/scripts/deploy.sh` en uno de los nodos de la implementación.

Resultados

La configuración de DNS de vRealize Orchestrator se modifica según lo especificado.

Casos prácticos de configuración y solución de problemas

8

Los casos prácticos de configuración proporcionan flujos de tareas que puede realizar para cumplir con requisitos de configuración específicos de su servidor de vRealize Orchestrator y temas de solución de problemas para comprender y solucionar un problema.

Este capítulo incluye los siguientes temas:

- Comprobar el número de compilación del servidor de vRealize Orchestrator
- Configurar el complemento de vRealize Orchestrator para vSphere Web Client
- Cancelar flujos de trabajo en ejecución
- Habilitar la depuración del servidor de vRealize Orchestrator
- Cambiar el tamaño de los discos de vRealize Orchestrator Appliance
- Cómo ampliar el tamaño de la memoria de pila del servidor de vRealize Orchestrator
- Recuperación ante desastres de vRealize Orchestrator mediante Site Recovery Manager

Comprobar el número de compilación del servidor de vRealize Orchestrator

En ciertos casos, es posible que deba comprobar el número de compilación del servidor de su implementación de vRealize Orchestrator.

Para comprobar el número de compilación del servidor de vRealize Orchestrator, vaya a https://FQDN_de_su_orquestador/vco/api/about. El número de compilación del servidor se muestra en las etiquetas `<ns2:build-number>`.

Comprobar el número de compilación del servidor puede ser útil en casos prácticos como proporcionar información adicional a una solicitud de soporte (Support Request, SR) que haya registrado en el Soporte técnico de VMware. También puede comprobar el número de compilación del servidor para confirmar que la actualización a la versión más reciente de vRealize Orchestrator se haya realizado correctamente.

Configurar el complemento de vRealize Orchestrator para vSphere Web Client

Para utilizar el complemento de vRealize Orchestrator para vSphere Web Client, debe registrar vRealize Orchestrator como una extensión de vCenter Server.

Después de registrar el servidor de vRealize Orchestrator con vCenter Single Sign-On y configurarlo para que funcione con vCenter Server, debe registrar vRealize Orchestrator como extensión de vCenter Server.

Requisitos previos

- Compruebe que el acceso SSH esté habilitado para vRealize Orchestrator Appliance. Consulte [Habilitar o deshabilitar el acceso SSH a vRealize Orchestrator Appliance](#).
- Debe registrar vRealize Orchestrator con la autenticación de vSphere en el mismo Platform Services Controller que utiliza su instancia de vCenter Server para autenticarse.
- Copie `vco-plugin.zip` en vRealize Orchestrator Appliance:
 - a Descargue el archivo `vco-plugin.zip` desde [VMware Technology Network](#).
 - b Abra un cliente SSH.

Nota Para entornos Linux o MacOS, puede usar la interfaz de línea de comandos del terminal. Para entornos Windows, puede usar el cliente PuTTY.

- c Para copiar el archivo `vco-plugin.zip`, ejecute el comando de copia segura.

```
For Linux/MacOS: scp ~/<zip_download_dir>/vco-plugin.zip
root@<orchestrator_FQDN_or_IP>:/data/vco/usr/lib/vco/downloads/vco-plugin.zip
```

```
For Windows: pscp C:\<zip_download_dir>\vco-plugin.zip root@<orchestrator_FQDN_or_IP>:/
data/vco/usr/lib/vco/downloads/vco-plugin.zip
```

Procedimiento

- 1 Inicie sesión en vRealize Orchestrator Client.
- 2 Vaya a **Biblioteca > Flujos de trabajo**.
- 3 Busque el flujo de trabajo **Registro de vCenter Orchestrator como extensión de vCenter Server** y haga clic en **Ejecutar**.
- 4 Seleccione la instancia de vCenter Server con la que registrar vRealize Orchestrator.
- 5 Introduzca `https://your_orchestrator_FQDN` o la URL de servicio del equilibrador de carga que redirige las solicitudes a los nodos del servidor de vRealize Orchestrator.
- 6 Haga clic en **Ejecutar**.

Cancelar flujos de trabajo en ejecución

Puede usar el centro de control de vRealize Orchestrator para cancelar los flujos de trabajo que no finalicen correctamente.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Haga clic en **Solución de problemas**.
- 3 Cancele los flujos de trabajo en ejecución.

Opción	Descripción
Cancelar todos los ciclos de ejecución del flujo de trabajo	Introduzca un identificador de flujo de trabajo para cancelar todos los tokens de ese flujo de trabajo.
Cancelar ciclos de ejecución de flujos de trabajo por ID	Introduzca todos los identificadores de token que desea cancelar. Separe los identificadores con una coma.
Cancelar todos los flujos de trabajo en ejecución	Cancele todos los flujos de trabajo en ejecución en el servidor.

Nota Es posible que las operaciones en las que cancele flujos de trabajo por identificador no se realicen correctamente, ya que no existe una forma confiable de cancelar el hilo de ejecución inmediatamente.

Resultados

En el siguiente inicio del servidor, los flujos de trabajo se configuran en un estado cancelado.

Habilitar la depuración del servidor de vRealize Orchestrator

Puede iniciar el servidor de vRealize Orchestrator en modo de depuración si desea depurar problemas cuando está desarrollando un complemento.

Requisitos previos

Instale y configure la herramienta de línea de comandos Kubernetes en su máquina local. Consulte [Instalar y configurar kubectl](#).

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz**.
- 2 Ejecute el comando `kubectl -n prelude edit deployment vco-app`.

- 3 Para editar el archivo `YAML` de la implementación, agregue una variable de entorno al contenedor de `vco-server-app`. La variable debe agregarse en la sección `env` del contenedor de `vco-server-app`.

```
containers:
  - command:
    ...
    env:
      - name: DEBUG_PORT
        value: "your_desired_debug_port"
    ...
  name: vco-server-app
  ...
```

Nota Al agregar la variable de entorno de depuración a la sección `env`, debe seguir el formato de sangría de `YAML` que se muestra en el ejemplo anterior.

- 4 Guarde los cambios en el archivo de implementación.

Si la edición en el archivo de implementación es correcta, recibirá el mensaje `deployment.extensions/vco-app` editado.

- 5 Para generar el archivo de configuración de Kubernetes ejecute el comando `vracli dev kubeconfig`.

Dado que `kubeconfig` es un entorno de desarrollador, se le pedirá que confirme que desea continuar. Introduzca **sí** para continuar o **no** para detener.

- 6 Copie el contenido del archivo de configuración generado a partir de `apiVersion: v1` incluyendo el contenido de `client-key-data`.
- 7 Guarde el archivo de configuración de Kubernetes generado en su máquina local.
- 8 Cierre sesión en vRealize Orchestrator Appliance.
- 9 Termine de configurar el modo de depuración en su máquina local.
 - a Abra un shell de la línea de comandos.
 - b Enlace la variable de entorno `KUBECONFIG` con el archivo de configuración guardado.

Nota Este ejemplo se basa en un entorno de Linux.

```
export KUBECONFIG=/file/path/fileName
```

- c Para validar que los procesos se están ejecutando, ejecute el comando `kubectl cluster-info`.
- d Para finalizar la configuración del modo de depuración, realice la siguiente solicitud de la API de Kubernetes.

Nota El valor de la variable `localhost_debug_port` es el puerto establecido en la configuración de depuración remota del entorno de desarrollo integrado (Integrated Development Environment, IDE). El valor de la variable `vro_debug_port` se genera durante el paso 3 de este procedimiento.

```
kubectl port-forward pod/vco_app_pod_ID localhost_debug_port:vro_debug_port
```

Importante Al configurar la herramienta de depuración, proporcione la configuración de IP y DNS de la máquina local en la que ejecutó el comando de reenvío del puerto.

Resultados

Ha configurado la depuración del servidor de vRealize Orchestrator Appliance.

Cambiar el tamaño de los discos de vRealize Orchestrator Appliance

Para modificar el tamaño de los discos de vRealize Orchestrator Appliance, edite la configuración de tamaño de disco de la máquina virtual de vRealize Orchestrator Appliance en vSphere.

Requisitos previos

Compruebe que el servicio SSH de vRealize Orchestrator Appliance está habilitado. Consulte [Habilitar o deshabilitar el acceso SSH a vRealize Orchestrator Appliance](#).

Procedimiento

- 1 Compruebe el espacio de disco disponible actualmente en vRealize Orchestrator Appliance.

Nota Los discos de vRealize Orchestrator Appliance necesitan al menos un 20 % de espacio de disco disponible.

- a Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance mediante SSH como **raíz**.
- b Ejecute el comando `vracli disk-mgr`.

- 2 Cambie el tamaño del disco de la máquina virtual de vRealize Orchestrator Appliance en vSphere.
 - a Inicie sesión en el vSphere Client como **administrador**.
 - b Haga clic con el botón secundario en la máquina virtual y seleccione **Editar configuración**.
 - c En la pestaña **Hardware virtual**, expanda **Disco duro** para ver y cambiar la configuración de disco, y haga clic en **Aceptar**.

Para obtener más información sobre el cambio de tamaño de los discos de las máquinas virtuales de vSphere, consulte *Cambiar la configuración del disco virtual en Administrar máquinas virtuales de vSphere*.

- 3 Active el cambio de tamaño automático en Photon OS.
 - a Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance mediante SSH como **raíz**.
 - b Ejecute el comando `vracli disk-mgr resize`.

Nota Puede realizar un seguimiento del progreso del procedimiento de cambio de tamaño del disco en `/var/log/vmware/prelude/disk_resize.log`.

Cambió el tamaño de los discos de vRealize Orchestrator Appliance.

- 4 Compruebe que el procedimiento de cambio de tamaño del disco se ha hecho correctamente ejecutando el comando `disk-mgr`.

```
vracli disk-mgr
```

Pasos siguientes

Para solucionar problemas relacionados con el procedimiento de cambio de tamaño del disco, consulte el artículo de la base de conocimientos [KB 79925](#).

Cómo ampliar el tamaño de la memoria de pila del servidor de vRealize Orchestrator

El tamaño de la memoria de pila del servidor de vRealize Orchestrator se puede ampliar mediante la edición del archivo `values.yaml`.

Puede ajustar el tamaño de la memoria de pila del servidor de vRealize Orchestrator, de modo que el entorno de orquestación pueda administrar cargas de trabajo que van cambiando. Por ejemplo, puede aumentar la memoria de pila de la implementación de vRealize Orchestrator si está pensando en administrar varias instancias de vCenter Server.

Requisitos previos

- Habilite el acceso SSH a vRealize Orchestrator Appliance. Consulte [Habilitar o deshabilitar el acceso SSH a vRealize Orchestrator Appliance](#).

- Aumente la RAM de la máquina virtual en la que vRealize Orchestrator se implementa hasta el siguiente incremento adecuado. Para obtener información sobre el aumento de la RAM de una máquina virtual en vSphere, consulte *Cambiar la configuración de la memoria en Administrar máquinas virtuales de vSphere*.

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance mediante SSH como **raíz**.
- 2 Vaya al directorio `/opt/charts/vco/`.
- 3 Con el editor que prefiera, edite el archivo `values.yaml`.

```
vi values.yaml
```

- 4 Modifique los parámetros `serverMemoryLimit`, `serverMemoryRequest` y `serverJvmHeapMax`.
 - a Establezca el valor de la memoria de pila editando el parámetro `serverJvmHeapMax`.
 - b Actualice los valores de los parámetros `serverMemoryLimit` y `serverMemoryRequest`.

Precaución El parámetro `serverMemoryLimit` debe ser 2 GB mayor que el valor establecido en el parámetro `serverJvmHeapMax`. El parámetro `serverMemoryRequest` debe ser 1 GB mayor que el valor establecido en el parámetro `serverJvmHeapMax`. A continuación se muestra un ejemplo de configuración de memoria:

```
serverMemoryLimit: 8G
serverMemoryRequest: 7G
serverJvmHeapMax: 6G
```

Nota Para los entornos en clúster, realice los pasos anteriores en todos los nodos del clúster.

- 5 Guarde los cambios en el archivo `values.yaml` y desplácese hasta el directorio `/opt/scripts`.
- 6 Ejecute el comando `deploy.sh`.

Resultados

Se modificó el tamaño de la memoria de pila del servidor de vRealize Orchestrator.

Recuperación ante desastres de vRealize Orchestrator mediante Site Recovery Manager

Debe configurar Site Recovery Manager para proteger vRealize Orchestrator. Asegure esta protección completando las tareas de configuración comunes para Site Recovery Manager.

Preparar el entorno

Debe asegurarse de cumplir los siguientes requisitos previos antes de empezar a configurar Site Recovery Manager.

- Compruebe que vSphere 6.0 o posterior esté instalado en los sitios protegidos y de recuperación.
- Compruebe que utiliza Site Recovery Manager 8.1 o una versión posterior.
- Compruebe que se haya configurado vRealize Orchestrator.

Configurar máquinas virtuales para vSphere Replication

Debe configurar las máquinas virtuales para vSphere Replication o la replicación basada en matrices para utilizar Site Recovery Manager.

Para habilitar vSphere Replication en las máquinas virtuales necesarias, siga estos pasos.

Procedimiento

- 1 En vSphere Web Client, seleccione una máquina virtual en la que se deba activar vSphere Replication y haga clic en **Acciones > Todas las acciones de replicación de vSphere > Configurar replicación**.
- 2 En la ventana **Tipo de replicación**, seleccione **Replicar en vCenter Server** y haga clic en **Siguiente**.
- 3 En la ventana **Destino**, seleccione el vCenter para el sitio de recuperación y haga clic en **Siguiente**.
- 4 En la ventana **Servidor de replicación**, seleccione un servidor de vSphere Replication y haga clic en **Siguiente**.
- 5 En la ventana **Ubicación de destino**, haga clic en **Editar** y seleccione el almacén de datos de destino, en el que se guardarán los archivos replicados; a continuación, haga clic en **Siguiente**.
- 6 En la ventana **Opciones de replicación**, mantenga la configuración predeterminada y haga clic en **Siguiente**.
- 7 En la ventana **Configuración de recuperación**, indique el tiempo para **Objetivo de punto de recuperación** y **Punto en instancias de tiempo**; a continuación, haga clic en **Siguiente**.
- 8 En la ventana **Listo para completar**, compruebe la configuración y haga clic en **Finalizar**.
- 9 Repita estos pasos para todas las máquinas virtuales en las que debe activarse vSphere Replication.

Crear grupos de protección

Cree grupos de protección para permitir que Site Recovery Manager proteja máquinas virtuales.

Los grupos de protección se pueden organizar en carpetas. La pestaña **Grupos de protección** muestra los nombres de los grupos de protección, pero no se indica en qué carpeta se colocan. Si tiene dos grupos de protección con el mismo nombre en diferentes carpetas, podría resultar difícil distinguirlos. Por lo tanto, asegúrese de que los nombres de los grupos de protección sean exclusivos en todas las carpetas. En entornos en los que no todos los usuarios tengan privilegios de visualización para todas las carpetas, evite colocar grupos de protección en carpetas para garantizar la exclusividad de los nombres de los grupos de protección.

Cuando cree los grupos de protección, espere para asegurarse de que las operaciones finalicen el modo esperado. Asegúrese de que Site Recovery Manager crea el grupo de protección y de que la protección de las máquinas virtuales en el grupo sea correcta.

Requisitos previos

Compruebe que ha realizado una de las tareas siguientes:

- Ha incluido las máquinas virtuales en almacenes de datos para los que ha configurado la replicación basada en matrices.
- Se cumplen los requisitos de *Requisitos previos de los grupos de protección de la directiva de almacenamiento* y se han revisado las *Limitaciones de los grupos de protección de directiva de almacenamiento* en la guía *Administración de Site Recovery Manager*.
- Ha configurado vSphere Replication en las máquinas virtuales.
- Ha realizado una combinación de algunas de las acciones anteriores o de todas ellas.

Procedimiento

- 1 En vSphere Client o en vSphere Web Client, haga clic en **Site Recovery > Abrir Site Recovery**.
- 2 En la pestaña de inicio de Site Recovery, seleccione un par de sitios y haga clic en **Ver detalles**.
- 3 Seleccione la pestaña **Grupos de protección** y haga clic en **Nuevo** para crear un grupo de protección.
- 4 En la página Nombre y dirección, introduzca un nombre y una descripción para el grupo de protección, seleccione una dirección y haga clic en **Siguiente**.
- 5 En la página Tipo de grupo de protección, seleccione el tipo de grupo de protección y haga clic en **Siguiente**.

Opción	Acción
Crear un grupo de protección de replicación basada en matrices	Seleccione Grupos de almacenes de datos (replicación basada en matrices) y escoja un par de matrices.
Crear un grupo de protección de vSphere Replication	Seleccione Máquinas virtuales individuales (vSphere Replication) .
Crear un grupo de protección de políticas de almacenamiento	Seleccione Directivas de almacenamiento (replicación basada en matrices) .

- 6 Seleccione los grupos de almacenes de datos, las máquinas virtuales o las directivas de almacenamiento que desee agregar al grupo de protección.

Opción	Acción
Grupos de protección de replicación basada en matrices	Seleccione los grupos de almacenes de datos y haga clic en Siguiente . Cuando selecciona un grupo de almacenes de datos, las máquinas virtuales que contiene el grupo aparecen en la tabla Máquinas virtuales.
Grupos de protección de vSphere Replication	Seleccione las máquinas virtuales en la lista y haga clic en Siguiente . Solo aparecen en la lista las máquinas virtuales que ha configurado para vSphere Replication y que todavía no están en un grupo de protección.
Grupos de protección de políticas de almacenamiento	Seleccione las políticas de almacenamiento en la lista y haga clic en Siguiente .

- 7 En la página Plan de recuperación, también puede agregar el grupo de protección a un plan de recuperación.

Opción	Acción
Agregar a un plan de recuperación existente	Agrega el grupo de protección a un plan de recuperación existente.
Agregar a un plan de recuperación nuevo	Agrega el grupo de protección a un plan de recuperación nuevo. Si selecciona esta opción, debe introducir un nombre para el plan de recuperación.
No agregar a un plan de recuperación ahora	Seleccione esta opción si no desea agregar el grupo de protección a un plan de recuperación.

- 8 Revise la configuración y haga clic en **Finalizar**.

Puede supervisar el progreso de la creación del grupo de protección en la pestaña **Grupo de protección**.

- En el caso de una replicación basada en matrices y grupos de protección de vSphere Replication, si Site Recovery Manager ha aplicado correctamente las asignaciones de inventario a las máquinas virtuales protegidas, el estado de protección del grupo de protección es *correcto*.
- En el caso de grupos de protección de políticas de almacenamiento, si Site Recovery Manager ha protegido correctamente todas las máquinas virtuales asociadas con la política de almacenamiento, el estado de protección del grupo de protección es *correcto*.
- En el caso de una replicación basada en matrices y grupos de protección de vSphere Replication, si no configuró las asignaciones de inventario o si Site Recovery Manager no pudo aplicarlas, el estado de protección del grupo de protección es *no configurado*.
- En el caso de grupos de protección de políticas de almacenamiento, si Site Recovery Manager no pudo proteger todas las máquinas virtuales asociadas con la política de almacenamiento, el estado de protección del grupo de protección es *no configurado*.

Pasos siguientes

En el caso de una replicación basada en matrices y grupos de protección de vSphere Replication, si el estado de protección de los grupos de protección es *no configurado*, aplique las asignaciones de inventario a las máquinas virtuales:

- Para aplicar asignaciones de inventario de todo el sitio o para comprobar que las asignaciones de inventario que ya ha establecido sean válidas, consulte *Configurar asignaciones de inventario* en la guía *Administración de Site Recovery Manager*. Para aplicar estas asignaciones a todas las máquinas virtuales, consulte *Aplicar asignaciones de inventario a todos los miembros de un grupo de protección* en la guía *Administración de Site Recovery Manager*.
- Para aplicar las asignaciones de inventario a cada máquina virtual del grupo de protección de forma individual, consulte *Configurar asignaciones de inventario para una máquina virtual individual en un grupo de protección* en la guía *Administración de Site Recovery Manager*.

En el caso de grupos de protección de políticas de almacenamiento, si el estado de protección del grupo de protección es *no configurado*, compruebe que cumple los requisitos de *Requisitos previos de los grupos de protección de la directiva de almacenamiento* y que ha revisado las *Limitaciones de los grupos de protección de directiva de almacenamiento* en la guía *Administración de Site Recovery Manager*.

Crear un plan de recuperación

Cree un plan de recuperación para determinar cómo Site Recovery Manager recupera las máquinas virtuales.

Procedimiento

- 1 En vSphere Client o vSphere Web Client, haga clic en **Site Recovery > Abrir Site Recovery**.
- 2 En la pestaña de inicio de Site Recovery, seleccione un par de sitios y haga clic en **Ver detalles**.
- 3 Seleccione la pestaña **Planes de recuperación** y haga clic en **Nuevo** para crear un plan de recuperación.
- 4 Especifique un nombre, una descripción y una dirección para el plan, seleccione una carpeta y haga clic en **Siguiente**.
- 5 Seleccione el tipo de grupo en el menú.

Opción	Descripción
Grupos de protección para máquinas virtuales individuales o grupos de almacenes de datos	Seleccione esta opción para crear un plan de recuperación que contenga replicación basada en matrices y grupos de producción de vSphere Replication.
Grupos de protección de políticas de almacenamiento	<p>Seleccione esta opción para crear un plan de recuperación que contenga grupos de protección de políticas de almacenamiento.</p> <p>Si utiliza un almacenamiento ampliado, seleccione esta opción.</p>

- 6 Seleccione uno o varios grupos de protección para la recuperación del plan y haga clic en **Siguiente**.

- 7 En el menú desplegable **Red de prueba**, seleccione una red que se utilice durante la recuperación de prueba y haga clic en **Siguiente**.

Si no hay asignaciones de nivel de sitio, la opción predeterminada **Usar la asignación de nivel de sitio** crea una red de prueba aislada.

- 8 Revise la información de resumen y haga clic en **Finalizar** para crear el plan de recuperación.

Organizar planes de recuperación en carpetas

Para controlar el acceso de diferentes usuarios o grupos a los planes de recuperación, puede organizar sus planes de recuperación en carpetas.

La organización de los planes de recuperación en carpetas resulta útil si tiene una gran cantidad de ellos. Puede limitar el acceso a los planes de recuperación. Para ello, debe colocarlos en carpetas y asignar diferentes permisos a las carpetas para distintos usuarios o grupos. Para obtener información sobre cómo asignar permisos a carpetas, consulte *Asignar funciones y permisos de Site Recovery Manager* en la guía *Administración de Site Recovery Manager*.

Procedimiento

- 1 En la pestaña de inicio de **Site Recovery**, seleccione un par de sitios y haga clic en **Ver detalles**.
- 2 Haga clic en la pestaña **Planes de recuperación** y, en el panel izquierdo, haga clic con el botón secundario en **Planes de recuperación** y en **Nueva carpeta**.
- 3 Introduzca un nombre para la carpeta que va a crear y haga clic en **Agregar**.
- 4 Agregue los planes de recuperación nuevos o existentes a la carpeta.

Opción	Descripción
Crear un plan de recuperación nuevo	Haga clic con el botón secundario en la carpeta y seleccione Nuevo plan de recuperación .
Agregar un plan de recuperación existente	Haga clic con el botón secundario en un plan de recuperación del árbol de inventario y haga clic en Mover . Seleccione una carpeta de destino y haga clic en Mover .

Editar un plan de recuperación

Puede editar un plan de recuperación para cambiar las propiedades especificadas al crearlo. Para ello, puede hacerlo desde el sitio protegido o desde el sitio de recuperación.

Procedimiento

- 1 En vSphere Client o vSphere Web Client, haga clic en **Site Recovery > Abrir Site Recovery**.
- 2 En la pestaña de inicio de **Site Recovery**, seleccione un par de sitios y haga clic en **Ver detalles**.

- 3 Haga clic en la pestaña **Planes de recuperación**, haga clic con el botón secundario en un plan de recuperación y haga clic en **Editar**.
- 4 (opcional) Cambie el nombre o la descripción del plan y, a continuación, haga clic en **Siguiente**.

No podrá cambiar la dirección ni la ubicación del plan de recuperación.

- 5 (opcional) Seleccione o anule la selección de uno o varios grupos de protección para agregarlos al plan o eliminarlos de él, y haga clic en **Siguiente**.
- 6 (opcional) En el menú desplegable, seleccione otra red de prueba en el sitio de recuperación y, a continuación, haga clic en **Siguiente**.
- 7 Revise la información de resumen y haga clic en **Finalizar** para realizar los cambios especificados en el plan de recuperación.

Puede supervisar la actualización del plan en la vista **Tareas recientes**.

Establecimiento de las propiedades del sistema

9

Puede establecer las propiedades del sistema para cambiar el comportamiento predeterminado de Orchestrator.

Este capítulo incluye los siguientes temas:

- Establecer el acceso al sistema de archivos del servidor para flujos de trabajo y acciones
- Establecer el acceso a los comandos del sistema operativo para los flujos de trabajo y las acciones
- Establecer acceso de JavaScript a clases de Java
- Establecer la propiedad de tiempo de espera personalizado
- Agregar un conector JDBC para el complemento SQL de vRealize Orchestrator

Establecer el acceso al sistema de archivos del servidor para flujos de trabajo y acciones

En vRealize Orchestrator, los flujos de trabajo y las acciones tienen el acceso limitado a unos determinados directorios del sistema de archivos. Puede ampliar el acceso a otras partes del sistema de archivos del servidor modificando el archivo de configuración `js-io-rights.conf`.

Reglas del archivo `js-io-rights.conf` que permiten el acceso de escritura al sistema de vRealize Orchestrator

El archivo `js-io-rights.conf` contiene reglas que permiten el acceso de escritura a los directorios definidos en el sistema de archivos del servidor.

Contenido obligatorio del archivo `js-io-rights.conf`

Cada línea del archivo `js-io-rights.conf` debe contener la siguiente información:

- Un signo más (+) o menos (-) para indicar si los derechos se permiten o se deniegan
- Los niveles de los derechos de lectura (r), escritura (w) y ejecución (x)

- La ruta de acceso en la que se aplicarán los derechos

Nota La carpeta raíz del archivo `js-io-rights.conf` siempre es `/var/run/vco`. En el sistema de archivos de vRealize Orchestrator Appliance, esta carpeta se encuentra en `/data/vco/var/run/vco`. Todo el contenido con acceso al sistema de archivos de vRealize Orchestrator se debe asignar en esa carpeta raíz.

Contenido predeterminado del archivo `js-io-rights.conf`

El contenido predeterminado del archivo de configuración `js-io-rights.conf` en Orchestrator Appliance es el siguiente:

```
-rwx /
+rwx /var/run/vco
+rx /etc/vco
-rwx /etc/vco/app-server/security/
+rx /var/log/vco/
```

Las dos primeras líneas del archivo de configuración predeterminado `js-io-rights.conf` permiten los siguientes derechos de acceso:

-rwx /

Se deniega cualquier tipo de acceso al sistema de archivos.

+rwx /var/run/vco

Se permite el acceso de lectura, escritura y ejecución en el directorio `/var/run/vco`.

Reglas en el archivo `js-io-rights.conf`

vRealize Orchestrator resuelve los derechos de acceso en el orden en el que aparecen en el archivo `js-io-rights.conf`. Cada línea puede reemplazar las líneas anteriores.

Importante Puede permitir el acceso a todas las partes del sistema de archivos estableciendo `+rwx /` en el archivo `js-io-rights.conf`. Sin embargo, esto entraña un riesgo de seguridad elevado.

Establecer el acceso al sistema de archivos del servidor para flujos de trabajo y acciones

Para cambiar las partes del sistema de archivos del servidor a las que pueden acceder los flujos de trabajo y la API de vRealize Orchestrator, modifique el archivo de configuración `js-io-rights.conf`. El archivo `js-io-rights.conf` se crea cuando un flujo de trabajo intenta acceder al sistema de archivos del servidor de vRealize Orchestrator.

Procedimiento

- 1 Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance como **raíz**.
- 2 Desplácese hasta el directorio `/data/vco/var/run/vco/`.

- 3 Abra el archivo de configuración `js-io-rights.conf` en un editor de texto.
- 4 Añada las líneas pertinentes al archivo `js-io-rights.conf` para permitir o denegar el acceso a áreas del sistema de archivos.

Por ejemplo, la siguiente línea deniega los derechos de ejecución en el directorio `/data/vco/var/run/vco/noexec`:

```
-x /data/vco/var/run/vco/noexec
```

`/data/vco/var/run/vco/noexec` conserva los derechos de ejecución, pero `/data/vco/var/run/vco/noexec/bar` no. Se puede seguir leyendo y escribiendo en los dos directorios.

Resultados

Ha modificado los derechos de acceso al sistema de archivos de los flujos de trabajo y la API de vRealize Orchestrator.

Establecer el acceso a los comandos del sistema operativo para los flujos de trabajo y las acciones

La API de vRealize Orchestrator ofrece una clase de script, `Command`, que ejecuta comandos en el sistema operativo del host de servidor de vRealize Orchestrator. Para impedir el acceso no autorizado al host del servidor, las aplicaciones de vRealize Orchestrator no tienen permiso de forma predeterminada para ejecutar la clase `Command`. Si las aplicaciones de vRealize Orchestrator requieren permiso para ejecutar comandos en el sistema operativo del host, puede activar la clase de script `Command`.

Para conceder permiso para utilizar la clase `Command`, hay que establecer una propiedad del sistema de configuración de vRealize Orchestrator.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Haga clic en **Propiedades del sistema**.
- 3 Haga clic en **Nuevo**.
- 4 En el cuadro de texto **Clave**, escriba `com.vmware.js.allow-local-process`.
- 5 En el cuadro de texto **Valor**, escriba `true`.
- 6 En el cuadro de texto **Descripción**, escriba una descripción para la propiedad del sistema.
- 7 Haga clic en **Agregar**.
- 8 Haga clic en **Guardar cambios** en el menú emergente.
Aparecerá un mensaje que indica que se ha guardado correctamente.
- 9 Espere a que el servidor de vRealize Orchestrator se reinicie.

Resultados

Ha otorgado permisos a aplicaciones de vRealize Orchestrator para ejecutar comandos locales en el sistema operativo del host de servidor de vRealize Orchestrator.

Nota Al establecer la propiedad del sistema `com.vmware.js.allow-local-process` en `true`, permite que la clase de script `Command` se escriba en cualquier lugar del sistema de archivos. Esta propiedad reemplaza todos los permisos de acceso al sistema que haya establecido en el archivo `js-io-rights.conf` solo para la clase de script `Command`. Los permisos de acceso al sistema de archivos que haya establecido en el archivo `js-io-rights.conf` se siguen aplicando a todas las demás clases de script que no sean `Command`.

Establecer acceso de JavaScript a clases de Java

vRealize Orchestrator restringe de forma predeterminada el acceso de JavaScript a un conjunto limitado de clases de Java. Si necesita que JavaScript acceda a una mayor cantidad de clases de Java, debe establecer una propiedad del sistema de vRealize Orchestrator.

Permitir un acceso sin restricciones del motor de JavaScript a la máquina virtual de Java puede comportar problemas de seguridad. Los scripts formados incorrectamente o malintencionados podrían tener acceso a todos los componentes del sistema a los que tiene acceso el usuario que ejecuta el servidor de vRealize Orchestrator. En consecuencia, el motor de JavaScript de vRealize Orchestrator solo puede acceder de forma predeterminada a las clases del paquete `java.util.*`.

Si se necesita acceso de JavaScript a clases que no estén en el paquete `java.util.*`, puede enumerar en un archivo de configuración los paquetes de Java a los que JavaScript puede tener acceso. A continuación, establezca la propiedad del sistema `com.vmware.scripting.rhino-class-shutter-file` para que apunte a este archivo.

Procedimiento

- 1 Cree un archivo de configuración de texto para guardar la lista de paquetes de Java a los que JavaScript puede tener acceso.

Por ejemplo, para permitir que JavaScript tenga acceso a todas las clase del paquete `java.net` y a la clase `java.lang.Object`, añada el contenido siguiente al archivo.

```
java.net.*
java.lang.Object
```

- 2 Introduzca un nombre para el archivo de configuración.
- 3 Guarde el archivo de configuración en un subdirectorio de `/data/vco/usr/lib/vco`.

Nota El archivo de configuración no se puede guardar en otro directorio.

- 4 Inicie sesión en el centro de control como **raíz**.
- 5 Haga clic en **Propiedades del sistema**.

- 6 Haga clic en **Nuevo**.
- 7 En el cuadro de texto **Clave**, escriba `com.vmware.scripting.rhino-class-shutter-file`.
- 8 En el cuadro de texto **Valor**, escriba `vco/usr/lib/vco/su_subdirectorio_de_archivo_de_configuración`.
- 9 En el cuadro de texto **Descripción**, escriba una descripción para la propiedad del sistema.
- 10 Haga clic en **Agregar**.
- 11 Haga clic en **Guardar cambios** en el menú emergente.
Aparecerá un mensaje que indica que se ha guardado correctamente.
- 12 Espere a que el servidor de vRealize Orchestrator se reinicie.

Resultados

El motor de JavaScript tiene acceso a las clases de Java que ha especificado.

Establecer la propiedad de tiempo de espera personalizado

Cuando vCenter Server está sobrecargado, el tiempo que tarda en devolver la respuesta al servidor de vRealize Orchestrator es superior los 20.000 milisegundos establecidos de forma predeterminada. Para evitar esta situación, debe modificar el archivo de configuración de vRealize Orchestrator para aumentar el período de tiempo de espera predeterminado.

Si el período de tiempo de espera predeterminado se agota antes de que se completen determinadas operaciones, el registro del servidor de vRealize Orchestrator contiene errores.

```
Operation 'getPropertyContent' total time : '5742228' for 1823 calls, mean
time : '3149.0', min time : '0', max time : '32313' Timeout, unable to get
property 'info' com.vmware.vmo.plugin.vi4.model.TimeoutException
```

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Haga clic en **Propiedades del sistema**.
- 3 Haga clic en **Nuevo**.
- 4 En el cuadro de texto **Clave**, escriba `com.vmware.vmo.plugin.vi4.waitUpdatesTimeout`.
- 5 En el cuadro de texto **Valor**, escriba el nuevo período de tiempo de espera en milisegundos.
- 6 (opcional) Escriba una descripción para la propiedad del sistema en el cuadro de texto **Descripción**.
- 7 Haga clic en **Agregar**.
- 8 Haga clic en **Guardar cambios** en el menú emergente.
Aparecerá un mensaje que indica que se ha guardado correctamente.

9 Reinicie el servidor de Orchestrator.

Resultados

El valor establecido reemplaza la configuración de tiempo de espera predeterminada de 20.000 segundos.

Agregar un conector JDBC para el complemento SQL de vRealize Orchestrator

En este ejemplo se demuestra cómo se puede agregar un conector MySQL para el complemento SQL de vRealize Orchestrator.

Procedimiento

- 1 Agregue el archivo `connector.jar` de MySQL a vRealize Orchestrator Appliance.
 - a Inicie sesión en la línea de comandos de vRealize Orchestrator Appliance mediante SSH como **raíz**.
 - b Desplácese hasta el directorio `/data/vco/var/run/vco`.

```
cd /data/vco/var/run/vco
```

- c Cree un directorio `plugins/SQL/lib/`.

```
mkdir -p plugins/SQL/lib/
```

- d Copie el archivo `connector.jar` de MySQL de su equipo local al directorio `/data/vco/var/run/vco/plugins/SQL/lib/` mediante un comando de copia segura (SCP).

```
scp ~/local_machine_dir/your_mysql_connector.jar root@orchestrator_FQDN_or_IP:/data/vco/var/run/vco/plugins/SQL/lib/
```

Nota También puede utilizar otros métodos para copiar el archivo `connector.jar` en vRealize Orchestrator Appliance (como PSCP).

- 2 Agregue la nueva propiedad de MySQL al centro de control.
 - a Inicie sesión en el centro de control como usuario **raíz**.
 - b Seleccione **Propiedades del sistema**.
 - c Haga clic en **Nuevo**.
 - d En **Clave**, introduzca `o11n.plugin.SQL.classpath`.

- e En **Valor**, introduzca `/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar`.

Nota El cuadro de texto de valores puede incluir varios conectores JDBC. Los conectores JDBC están separados por un punto y coma (;). Por ejemplo:

```
/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar;/var/run/vco/plugins/SQL/lib/your_mssql_connector.jar;/var/run/vco/plugins/SQL/lib/your_other_connector.jar
```

- f (opcional) Introduzca una descripción para la propiedad del sistema de MySQL.
- g Haga clic en **Agregar** y espere a que se reinicie el servidor de vRealize Orchestrator.

Nota No guarde el archivo connector.jar de JDBC en otro directorio ni establezca otro valor en la propiedad `o11n.plugin.SQL.classpath`. De hacerlo, el conector JDBC no estaría disponible para la implementación de vRealize Orchestrator.

Pasos a seguir

10

Cuando haya instalado y configurado vRealize Orchestrator, puede usar vRealize Orchestrator para automatizar los procesos que se repiten con frecuencia relativos a la administración del entorno virtual.

- Inicie sesión en el vRealize Orchestrator Client, y ejecute y programe flujos de trabajo en los objetos de inventario de vCenter Server u otros objetos a los que vRealize Orchestrator accede mediante sus complementos. Consulte *Usar el cliente de VMware vRealize Orchestrator*.
- Duplique y modifique los flujos de trabajo de vRealize Orchestrator estándar, y escriba sus propias acciones y flujos de trabajo para automatizar las operaciones en vCenter Server.
- Para ampliar la funcionalidad de la plataforma de vRealize Orchestrator, desarrolle complementos.
- Administre el inventario de vRealize Orchestrator en varias instancias de vRealize Orchestrator con la integración de un repositorio de Git remoto. Consulte *Uso del cliente de VMware vRealize Orchestrator*.
- Ejecute flujos de trabajo en los objetos de inventario de vSphere mediante vSphere Web Client.