

Instalación y configuración de VMware vRealize Orchestrator

vRealize Orchestrator 7.6

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

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

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

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

Copyright © 2008-2019 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

Tipos de usuarios de Orchestrator y responsabilidades relacionadas 10

Arquitectura de Orchestrator 11

Complementos de Orchestrator 11

2 Requisitos del sistema de Orchestrator 13

Requisitos de hardware del Orchestrator Appliance 13

Navegadores compatibles con vRealize Orchestrator 14

Requisitos de la base de datos de Orchestrator 14

Software incluido en Orchestrator Appliance 14

Compatibilidad con nivel de internacionalización 14

Puertos de red de vRealize Orchestrator 15

3 Configurar componentes de vRealize Orchestrator 18

Configuración de vCenter Server 18

Métodos de autenticación 19

4 Instalar vRealize Orchestrator 20

Descargar e implementar vRealize Orchestrator Appliance 20

Encender vRealize Orchestrator Appliance y abrir la página de inicio 22

Cambiar la contraseña raíz 22

Habilitar o deshabilitar el inicio de sesión de administrador de SSH en el dispositivo de vRealize Orchestrator 23

Configurar los ajustes de red para vRealize Orchestrator Appliance 23

5 Configuración inicial 25

Configurar un servidor de Orchestrator independiente 25

Configurar un servidor de Orchestrator independiente con la autenticación de vRealize Automation 25

Configurar un servidor de Orchestrator independiente con autenticación de vSphere 27

Puertos de red de vRealize Orchestrator 29

Conexión con una base de datos de Orchestrator 30

Administrar certificados 30

Administrar certificados de Orchestrator 31

Configurar los complementos de vRealize Orchestrator 33

Administrar complementos de vRealize Orchestrator	34
Instalar o actualizar un complemento de vRealize Orchestrator	34
Desinstalar un complemento	35
Disponibilidad y escalabilidad de Orchestrator	36
Configurar un clúster de instancias de vRealize Orchestrator en VAMI	37
Supervisar un clúster de Orchestrator	38
Habilitar el modo sincrónico para el clúster de Orchestrator	39
Promover un nodo de réplica de Orchestrator al nodo principal	39
Eliminar un nodo de clúster de Orchestrator	40
Configuración del Programa de mejora de la experiencia del cliente	40
Categorías de información que recibe VMware	41
Participe en el programa de mejora de la experiencia de cliente (CEIP)	41
6 Usar los servicios de la API	42
Administración de certificados SSL a través de la API de REST	42
Eliminación de un certificado SSL utilizando la API de REST	43
Importar certificados SSL mediante la API de REST	43
Creación de un almacén de claves mediante la API de REST	45
Eliminación de un almacén de claves mediante la API de REST	45
Adición de una clave mediante la API de REST	46
Automatización de la configuración de Orchestrator utilizando la API de REST del centro de control	46
7 Opciones de configuración adicionales	48
Volver a configurar la autenticación	48
Cambiar el proveedor de autenticación	48
Cambiar los parámetros de autenticación	49
Exportar la configuración de Orchestrator	50
Importar la configuración de Orchestrator	51
Configurar las propiedades de ejecución de los flujos de trabajo	52
Archivos de log de Orchestrator	52
Registro de la persistencia	53
Configuración de registros de Orchestrator	54
Filtrar los registros de Orchestrator	55
Configurar la integración del registro con el servidor remoto	55
Añadir controladores de interfaz de red	56
Configurar rutas estáticas	56
Habilitar las extensiones de Opentracing y Wavefront	57
Configurar la extensión de Opentracing	58
Configurar la extensión de Wavefront	59
8 Resolución de problemas y casos de uso de configuración	61

Configurar el complemento de vRealize Orchestrator para vSphere Web Client	61
Eliminación de la autenticación de Orchestrator del registro	62
Cambio de certificados SSL	62
Adición de un certificado a un almacén local	63
Cambio del certificado del sitio de administración de Orchestrator Appliance	64
Cancelar flujos de trabajo en ejecución	64
Activación de la depuración del servidor de Orchestrator	65
Realizar una copia de seguridad de la configuración y elementos de Orchestrator	66
Copia de seguridad y restauración de vRealize Orchestrator	69
Copia de seguridad de vRealize Orchestrator	69
Restaurar una instancia de a vRealize Orchestrator	70
Recuperación ante desastres de Orchestrator mediante Site Recovery Manager	71
Configurar máquinas virtuales para vSphere Replication	72
Crear grupos de protección	72
Crear un plan de recuperación	74
Organización de planes de recuperación en carpetas	74
Editar un plan de recuperación	75

9 Establecimiento de las propiedades del sistema 77

Desactivación del acceso al cliente de Orchestrator por parte de usuarios que no son administradores	77
Establecer el acceso al sistema de archivos del servidor para flujos de trabajo y acciones	78
Reglas del archivo js-io-rights.conf que permiten el acceso de escritura al sistema de Orchestrator	78
Establecer el acceso al sistema de archivos del servidor para flujos de trabajo y acciones	79
Establecer el acceso a los comandos del sistema operativo para los flujos de trabajo y las acciones	80
Establecer acceso de JavaScript a clases de Java	81
Establecimiento de la propiedad de tiempo de espera personalizado	82

10 Procedimiento a partir de aquí 84

Iniciar sesión en el cliente heredado de Orchestrator desde la consola web de Orchestrator Appliance	84
--	----

Instalación y configuración de VMware vRealize Orchestrator

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

Público objetivo

Esta información está destinada a los administradores de vSphere con conocimientos avanzados, así como a los administradores del sistema con experiencia 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](#)
- [Tipos de usuarios de Orchestrator y responsabilidades relacionadas](#)
- [Arquitectura de Orchestrator](#)
- [Complementos de Orchestrator](#)

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. Orchestrator es una plataforma abierta que se puede ampliar con nuevos complementos y bibliotecas, y que se puede integrar en arquitecturas más grandes a través de una API de REST.

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

Persistencia

Las bases de datos de nivel de producción se utilizan para almacenar información relevante, como procesos, estados de flujo de trabajo y la configuración de Orchestrator.

Administración central

Con Orchestrator, los procesos se administran de forma centralizada. 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, la supervisión de flujos de trabajo, el acceso y la configuración de registros unificados, así como la correlación entre las ejecuciones de flujo de trabajo y los recursos del sistema. El mecanismo de registro de Orchestrator se optimiza con un archivo de registro adicional que recopila distintas métricas del rendimiento del motor de Orchestrator.

Control de versiones

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

Motor de creación de scripts

El motor de JavaScript de Rhino de Mozilla permite generar bloques de creación para la plataforma de Orchestrator. 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 Orchestrator
- Bloques de creación personalizados creados por el cliente
- Objetos que los complementos añaden a Orchestrator

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

Motor de políticas

Puede utilizar el motor de políticas para supervisar y generar eventos con el fin de reaccionar ante los cambios de condiciones en el servidor de Orchestrator 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.

Cliente de Orchestrator

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. Para obtener más información, consulte *Uso del cliente de vRealize Orchestrator*.

Nota Para obtener información sobre el cliente heredado de Orchestrator basado en Java (obsoleto), consulte *Uso del cliente heredado de VMware vRealize Orchestrator*.

Desarrollo y recursos

La página de inicio de 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 Orchestrator para enviar solicitudes al servidor de Orchestrator.

Seguridad

Orchestrator proporciona las funciones avanzadas siguientes 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.
- Secure Sockets Layer (SSL) para proporcionar comunicaciones cifradas entre el cliente de escritorio y el servidor, y 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 la misma clave de cifrado.

Tipos de usuarios de Orchestrator y responsabilidades relacionadas

Orchestrator proporciona diferentes herramientas e interfaces basadas en las responsabilidades específicas de las funciones de usuarios globales. En Orchestrator, puede tener usuarios con todos los derechos, que sean parte de un grupo de administradores (Administradores), y usuarios con derechos limitados, que no sean parte de un grupo de administradores (Usuarios finales).

Usuarios con todos los derechos

Los administradores y los desarrolladores de Orchestrator tienen los mismos derechos administrativos, pero están divididos en lo concerniente a las responsabilidades.

Administradores

Esta función tiene acceso completo a todas las funcionalidades de la plataforma de Orchestrator. Las responsabilidades administrativas básicas incluyen lo siguiente:

- Instalar y configurar Orchestrator
- Administrar los derechos de acceso para Orchestrator y las aplicaciones
- Importar y exportar paquetes
- Ejecutar flujos de trabajo y programar tareas
- Administrar el control de versiones de los elementos importados
- Crear nuevos flujos de trabajo y complementos

Desarrolladores

Este tipo de usuario tiene acceso completo a todas las funcionalidades de la plataforma de Orchestrator. Los desarrolladores tienen acceso a la interfaz del cliente de Orchestrator y cuentan con las responsabilidades siguientes:

- Crear aplicaciones para extender la funcionalidad de la plataforma de Orchestrator
- Automatizar procesos personalizando los flujos de trabajo y creando flujos de trabajo y complementos nuevos

Usuarios con derechos limitados

Usuarios finales

Los usuarios finales pueden ejecutar y programar flujos de trabajo y políticas que los administradores o los desarrolladores ponen a disposición en el cliente de Orchestrator.

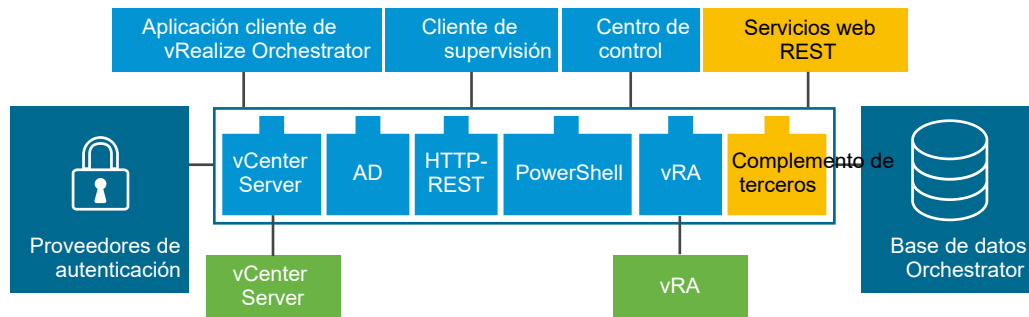
Arquitectura de Orchestrator

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

Orchestrator proporciona una serie de complementos estándar, incluido uno para vCenter Server y para vRealize Automation, para permitirle orquestar tareas en los diferentes entornos que exponen los complementos.

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. Orchestrator se conecta a un proveedor de autenticación para administrar cuentas de usuario y a una base de datos para almacenar información de los flujos de trabajo que ejecuta. Puede acceder a Orchestrator, a los objetos que expone y a los flujos de trabajo de Orchestrator a través de la interfaz del cliente de Orchestrator o a través de servicios web. La supervisión y configuración de los flujos de trabajo y servicios de Orchestrator se realiza a través del cliente de supervisión y el centro de control.

Figura 1-1. Arquitectura de VMware vRealize Orchestrator



Complementos de Orchestrator

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

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 el uso de los complementos, puede automatizar la prestación de nuevos servicios tecnológicos o bien adaptar las capacidades de la infraestructura y los servicios de aplicaciones de vRealize Automation. Además, puede utilizar la arquitectura abierta de complementos de Orchestrator para desarrollar complementos que le permitan acceder a otras aplicaciones.

Los complementos de Orchestrator que desarrolla VMware se distribuyen como archivos .vmoapp. Para obtener más información acerca de los complementos de Orchestrator que desarrolla y distribuye VMware, consulte [Complementos externos de vRealize Orchestrator](#). Para obtener más información sobre complementos de Orchestrator de terceros, consulte [Intercambio de soluciones de VMware](#).

Requisitos del sistema de Orchestrator

2

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

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

Este capítulo incluye los siguientes temas:

- [Requisitos de hardware del Orchestrator Appliance](#)
- [Navegadores compatibles con vRealize Orchestrator](#)
- [Requisitos de la base de datos de Orchestrator](#)
- [Software incluido en Orchestrator Appliance](#)
- [Compatibilidad con nivel de internacionalización](#)
- [Puertos de red de vRealize Orchestrator](#)

Requisitos de hardware del Orchestrator Appliance

El Orchestrator Appliance es una máquina virtual preconfigurada basada en Linux. Antes de implementar el dispositivo, compruebe que el sistema cumpla los requisitos mínimos de hardware.

El Orchestrator Appliance presenta los siguientes requisitos de hardware:

- 2 CPU
- 6 GB de memoria
- Disco duro de 17 GB

No reduzca el tamaño predeterminado de la memoria, ya que el servidor de Orchestrator requiere al menos 2 GB de memoria libre.

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

Requisitos de la base de datos de Orchestrator

El servidor de Orchestrator incluye una base de datos de PostgreSQL preconfigurada que está lista para la producción.

A partir de vRealize Orchestrator 7.5, no se admite la integración de bases de datos externas. Solo se puede utilizar la base de datos de PostgreSQL preconfigurada.

Software incluido en Orchestrator Appliance

Orchestrator Appliance es una máquina virtual preconfigurada y optimizada para ejecutar Orchestrator. El dispositivo se distribuye con software preinstalado.

El paquete de Orchestrator Appliance contiene el siguiente software:

- SUSE Linux Enterprise Server 11, Update 3 para VMware, edición de 64 bits
- PostgreSQL
- Orchestrator

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

Nota Para usar Orchestrator Appliance en un entorno de producción, debe configurar el servidor de Orchestrator para que se autentique a través de vRealize Automation o vSphere. Para obtener más información sobre cómo configurar un proveedor de autenticación, consulte [Configurar un servidor de Orchestrator independiente](#).

Compatibilidad con nivel de internacionalización

El centro de control de Orchestrator incluye la localización en español, francés, alemán, chino tradicional, chino simplificado, coreano y japonés. El cliente de Orchestrator admite el nivel de internacionalización 1.

Compatibilidad con caracteres no ASCII en Orchestrator

Aunque el cliente de Orchestrator no está traducido, se puede ejecutar en sistemas operativos distintos del inglés y admite texto que no sea ASCII.

Tabla 2-1. Compatibilidad con caracteres no ASCII en la GUI de Orchestrator

Compatibilidad con caracteres no ASCII				
Elemento de Orchestrator	Campo de descripción	Campo de nombre	Parámetros de entrada y salida	Atributos
Acción	Sí	No	No	No
Carpeta	Sí	Sí	-	-
Elemento de configuración	Sí	Sí	-	No
Paquete	Sí	Sí	-	-
Política	Sí	Sí	-	-
Plantilla de políticas	Sí	Sí	-	-
Elemento de recursos	Sí	Sí	-	-
Flujo de trabajo	Sí	Sí	No	No
Grupo de visualización de presentación del flujo de trabajo y paso de entrada	Sí	Sí	-	-

Puertos de red de vRealize Orchestrator

vRealize Orchestrator utiliza puertos específicos para comunicarse con otros sistemas. Estos puertos tienen un valor predeterminado que no se puede cambiar.

Puertos de configuración predeterminados

Para proporcionar el servicio de vRealize Orchestrator, debe establecer los puertos predeterminados y configurar el firewall para que permita las conexiones TCP entrantes.

Nota Si utiliza complementos personalizados, podrían ser necesarios otros puertos.

Tabla 2-2. Puertos de configuración predeterminados de VMware vRealize Orchestrator

Puerto	Número	Protocolo	Origen	Destino	Descripción
Interfaz de administración de dispositivos virtuales	5480	TCP			El puerto de acceso a la interfaz de configuración del sistema de dispositivos.
Dispositivo de vRealize Orchestrator	5488 5489	TCP			El puerto utilizado internamente por el dispositivo de vRealize Orchestrator para las actualizaciones.

Tabla 2-2. Puertos de configuración predeterminados de VMware vRealize Orchestrator (continuación)

Puerto	Número	Protocolo	Origen	Destino	Descripción
Puerto de servidor HTTP	80	TCP	Navegador web de usuario final	Servidor de vRealize Orchestrator	Opcional. Las solicitudes enviadas al puerto web HTTP 80 predeterminado de vRealize Orchestrator se redirigen al puerto web HTTPS 8281 predeterminado.
Puerto de servidor HTTP	8280	TCP	Navegador web de usuario final	Servidor de vRealize Orchestrator	Las solicitudes enviadas al puerto web HTTP 8280 predeterminado de Orchestrator se redirigen al puerto web HTTPS 8281 predeterminado.
Puerto de servidor HTTPS	8281	TCP	Navegador web de usuario final	Servidor de vRealize Orchestrator	El puerto de acceso para la página de inicio de vRealize Orchestrator.
Puerto de acceso HTTPS de configuración web	8283	TCP	Navegador web de usuario final	Configuración de vRealize Orchestrator	El puerto de acceso SSL para el cliente de vRealize Orchestrator.

Puertos de comunicación externos

Debe configurar el firewall para permitir las conexiones de salida de modo que vRealize Orchestrator se pueda comunicar con servicios externos.

Tabla 2-3. Puertos de comunicación externos de VMware vRealize Orchestrator

Número de puerto	Protocolo	Origen	Destino	Descripción
123	UDP	Servidor de vRealize Orchestrator	Servidor NTP	El puerto predeterminado para conectarse directamente a NTP en lugar de usar la hora del host.
25	TCP	Servidor de vRealize Orchestrator	Servidor SMTP	El puerto que se utiliza para las notificaciones de correo electrónico.
443	TCP	Servidor de vRealize Orchestrator	API de vCenter Server	El puerto de comunicación API de vCenter Server que utiliza vRealize Orchestrator para obtener la infraestructura virtual y la información de máquina virtual de las instancias orquestadas de vCenter Server.
4.000	UDP	Servidor de vRealize Orchestrator	Servidor SNMP	El puerto predeterminado para escuchar capturas de SNMP en el complemento SNMP.
514	UDP	Servidor de vRealize Orchestrator	Servidor de Syslog	El puerto para enviar mensajes de eventos de Syslog.

Tabla 2-3. Puertos de comunicación externos de VMware vRealize Orchestrator (continuación)

Número de puerto	Protocolo	Origen	Destino	Descripción
5432	TCP	Servidor de vRealize Orchestrator	Servidor de PostgreSQL	El puerto que se utiliza para comunicarse con el servidor de PostgreSQL que se configura como base de datos de vRealize Orchestrator.
5434	TCP	Servidor de vRealize Orchestrator	Servidor de PostgreSQL	El puerto que utiliza el servicio de PostgreSQL Manager para la tolerancia a errores de la base de datos.

Configurar componentes de vRealize Orchestrator

3

Cuando descarga e implementa vRealize Orchestrator Appliance, el servidor de vRealize Orchestrator está preconfigurado. Después de la implementación, el servicio se inicia 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.
- Para entornos de vRealize Orchestrator en clúster, instale y configure un servidor de equilibrio de carga y configúrelo para distribuir la carga de trabajo entre dos o más 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 Orchestrator hace que Orchestrator tenga que administrar más sesiones. Cuando hay demasiadas sesiones activas, 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 Puede ejecutar varias instancias de vCenter Server en distintas máquinas virtuales en la configuración de Orchestrator si la red posee suficiente ancho de banda y latencia. Si utiliza una LAN para mejorar las comunicaciones entre Orchestrator y vCenter Server, es indispensable contar con una línea de 100 Mb.

Métodos de autenticación

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

Cuando descargue e implemente el Orchestrator Appliance, debe configurar una conexión con un vRealize Automation o vSphere.

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

Descargue e instale vRealize Orchestrator Appliance implementándolo a partir de una plantilla.

Requisitos previos

- Compruebe que vCenter Server esté instalado y en ejecución.
- Compruebe que el host donde se implementa vRealize Orchestrator Appliance cumpla los requisitos de hardware mínimos. Para obtener más información, consulte [Requisitos de hardware del 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 vSphere Web Client como administrador.
- 2 En vSphere Web Client, seleccione un objeto de inventario que sea un objeto principal válido de una máquina virtual, como 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 implementada, 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 implementada.

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 (opcional) Configure la red y haga clic en **Siguiente**.

De forma predeterminada, vRealize Orchestrator Appliance utiliza DHCP. Puede cambiar esta configuración y asignar una dirección IP fijo desde la consola web del dispositivo.

- 12 Seleccione las opciones que quiera activar y establezca la contraseña inicial para la cuenta de usuario raíz.

La contraseña inicial debe tener como mínimo ocho caracteres de longitud.

Importante La contraseña de la cuenta raíz de Orchestrator Appliance caduca transcurridos 365 días. Para incrementar el tiempo de caducidad de una cuenta, inicie la sesión en Orchestrator Appliance como usuario raíz y ejecute `passwd -x number_of_days name_of_account`. Si desea aumentar la contraseña raíz de Orchestrator Appliance hasta el infinito, ejecute `passwd -x 99999 root`.

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

Resultados

vRealize Orchestrator Appliance se habrá implementado correctamente.

Encender vRealize Orchestrator Appliance y abrir la página de inicio

Para usar vRealize Orchestrator Appliance, primero debe encenderlo y obtener una dirección IP para el dispositivo virtual.

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 Una vez que se encienda el dispositivo, seleccione la pestaña **Resumen** para ver la dirección IP de vRealize Orchestrator Appliance.
- 4 En un navegador web, vaya a la dirección del host de su máquina virtual de vRealize Orchestrator Appliance.

`https://su_nombre_de_host_de_orchestrator/vco.`

Cambiar la contraseña raíz

Por razones de seguridad, se puede cambiar la contraseña raíz de vRealize Orchestrator Appliance.

De forma predeterminada, la contraseña de la cuenta raíz de vRealize Orchestrator Appliance caduca a los 365 días. Si lo desea, puede aumentar la caducidad de la cuenta raíz. Para ello, debe iniciar sesión en vRealize Orchestrator Appliance a través de un cliente SSH y ejecutar `passwd -x número_de_días nombre_de_cuenta`. Si desea aumentar la contraseña raíz de vRealize Orchestrator Appliance hasta el infinito, ejecute `passwd -x 99999 root`.

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 interfaz VAMI de vRealize Orchestrator como **raíz**.
Acceda a la interfaz VAMI en `https://su_nombre_de_host_de_orchestrator:5480`.
- 2 Seleccione la pestaña **Administrador**.
- 3 En el cuadro de texto **Contraseña actual del administrador**, indique la contraseña raíz actual.
- 4 Introduzca la nueva contraseña en los cuadros de texto **Nueva contraseña del administrador** y **Vuelva a escribir la nueva contraseña del administrador**.
- 5 Haga clic en **Guardar configuración**.

Resultados

Ha cambiado correctamente la contraseña del usuario raíz de Linux de vRealize Orchestrator Appliance.

Habilitar o deshabilitar el inicio de sesión de administrador de SSH en el dispositivo de vRealize Orchestrator

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 interfaz VAMI de vRealize Orchestrator como **raíz**.
Acceda a la interfaz VAMI en `https://su_nombre_de_host_de_orchestrator:5480`.
- 2 En la pestaña **Administrador**, haga clic en **Servicio SSH habilitado** para habilitar o deshabilitar el servicio SSH de vRealize Orchestrator.
- 3 (opcional) Haga clic en **Inicio de sesión SSH de administrador habilitado** para habilitar o deshabilitar el acceso raíz a vRealize Orchestrator Appliance mediante SSH.
- 4 Haga clic en **Guardar configuración**.

Resultados

Cuando se habilita, **Estado de SSH** aparece como *En ejecución*. Cuando se deshabilita, **Estado de SSH** aparece como *Detenido*.

Configurar los ajustes de red para vRealize Orchestrator Appliance

Configure los ajustes de red para vRealize Orchestrator Appliance para asignar una dirección IP estática y defina la configuración del proxy.

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 interfaz VAMI de vRealize Orchestrator como **raíz**.
Acceda a la interfaz VAMI en `https://su_nombre_de_host_de_orchestrator:5480`.
- 2 En la pestaña **Red**, haga clic en **Dirección**.

- 3 Seleccione el método mediante el cual vRealize Orchestrator Appliance obtiene la configuración de la dirección IP.

Opción	Descripción
DHCP	Obtiene la configuración de la dirección IP de un servidor DHCP. Esta es la configuración predeterminada.
Estático	Usa una configuración de dirección IP estática. Si selecciona esta opción, se le pedirá que introduzca una dirección IP, una máscara de usuario (para IPv4), un prefijo (para IPv6) y la información de la puerta de enlace.

En función de la configuración de red, es posible que tenga que seleccionar los tipos de direcciones IPv4 e IPv6.

- 4 Haga clic en **Guardar configuración**.
- 5 (opcional) Para configurar un servidor proxy, seleccione la pestaña **Proxy**.
- 6 (opcional) Después de configurar los ajustes del proxy, haga clic en **Guardar configuración**.

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, o la supervisión y la configuración de los registros de vRealize Orchestrator.

Este capítulo incluye los siguientes temas:

- [Configurar un servidor de Orchestrator independiente](#)
- [Puertos de red de vRealize Orchestrator](#)
- [Conexión con una base de datos de Orchestrator](#)
- [Administrar certificados](#)
- [Configurar los complementos de vRealize Orchestrator](#)
- [Disponibilidad y escalabilidad de Orchestrator](#)
- [Configuración del Programa de mejora de la experiencia del cliente](#)

Configurar un servidor de Orchestrator independiente

Aunque Orchestrator Appliance es una máquina virtual basada en Linux y preconfigurada, debe seguir al asistente para la configuración antes de acceder al Centro de control de Orchestrator.

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

Para preparar el Orchestrator Appliance para su uso, debe configurar los ajustes del host y el proveedor de autenticación. Puede configurar Orchestrator para autenticar a través del registro de componentes de vRealize Automation.

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, y compruebe que el servidor de vRealize Automation se esté ejecutando. Consulte la documentación de vRealize Automation.

Si tiene previsto crear un clúster:

- Configure un equilibrador de carga para distribuir el tráfico entre varias instancias de vRealize Orchestrator. Para obtener más información, consulte la documentación acerca del equilibrio de carga de vRealize Orchestrator.

Procedimiento

- 1 Acceda al centro de control para iniciar el asistente para configuración.
 - a Vaya a `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter`.
 - b Inicie sesión como **raíz** con la contraseña que introdujo durante la implementación de OVA.
- 2 Haga clic en **CAMBIAR** para configurar el nombre de host en el que se podrá acceder al centro de control.

Nota Si se dispone a configurar un clúster de Orchestrator, escriba el nombre de host del servidor virtual del equilibrador de carga.

- 3 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**.
 - c Haga clic en **Aceptar certificado**.
 - d En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de la cuenta de usuario que está configurada para la conexión de SSO en vRealize Automation. Haga clic en **REGISTRAR**.

De forma predeterminada, la cuenta SSO es de **administrador** 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 En la lista de grupos, haga clic en el nombre del grupo para seleccionarlo.
 - g Haga clic en **GUARDAR CAMBIOS**.

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

Resultados

La configuración del centro de control se ha llevado a cabo correctamente.

Pasos siguientes

- Compruebe que **VRA** 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 Orchestrator se reinicia automáticamente pasados dos minutos. La verificación de la configuración inmediatamente después de la finalización del proceso puede devolver un estado de configuración no válido.

Configurar un servidor de Orchestrator independiente con autenticación de vSphere

Para registrar el servidor de Orchestrator con un servidor de vCenter Single Sign-On, utilice 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 vCenter Server con vCenter Single Sign-On en ejecución. Para obtener información, 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. Para obtener más información, consulte la documentación acerca del equilibrio de carga de vRealize Orchestrator.

Procedimiento

- 1 Acceda al centro de control para iniciar el asistente para configuración.
 - a Vaya a `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter`.
 - b Inicie sesión como **raíz** con la contraseña que introdujo durante la implementación de OVA.
- 2 Haga clic en **CAMBIAR** para configurar el nombre de host en el que se podrá acceder al centro de control.

Nota Si se dispone a configurar un clúster de Orchestrator, escriba el nombre de host del servidor virtual del equilibrador de carga.

3 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 el mismo 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 Orchestrator. En los entornos de alta disponibilidad de Orchestrator, debe replicar las instancias de PCS detrás del servidor del equilibrador de carga de Orchestrator.

- c Haga clic en **Aceptar certificado**.
- d En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de la cuenta de administrador local del 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\vcadmins**.

- f En la lista de grupos, haga clic en el nombre del grupo para seleccionarlo.
- g Haga clic en **GUARDAR CAMBIOS**.

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

Resultados

La configuración del centro de control 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 Orchestrator se reinicia automáticamente pasados dos minutos. La verificación de la configuración inmediatamente después de la finalización del proceso puede devolver un estado de configuración no válido.

Puertos de red de vRealize Orchestrator

vRealize Orchestrator utiliza puertos específicos para comunicarse con otros sistemas. Estos puertos tienen un valor predeterminado que no se puede cambiar.

Puertos de configuración predeterminados

Para proporcionar el servicio de vRealize Orchestrator, debe establecer los puertos predeterminados y configurar el firewall para que permita las conexiones TCP entrantes.

Nota Si utiliza complementos personalizados, podrían ser necesarios otros puertos.

Tabla 5-1. Puertos de configuración predeterminados de VMware vRealize Orchestrator

Puerto	Número	Protocolo	Origen	Destino	Descripción
Interfaz de administración de dispositivos virtuales	5480	TCP			El puerto de acceso a la interfaz de configuración del sistema de dispositivos.
Dispositivo de vRealize Orchestrator	5488 5489	TCP			El puerto utilizado internamente por el dispositivo de vRealize Orchestrator para las actualizaciones.
Puerto de servidor HTTP	80	TCP	Navegador web de usuario final	Servidor de vRealize Orchestrator	Opcional. Las solicitudes enviadas al puerto web HTTP 80 predeterminado de vRealize Orchestrator se redirigen al puerto web HTTPS 8281 predeterminado.
Puerto de servidor HTTP	8280	TCP	Navegador web de usuario final	Servidor de vRealize Orchestrator	Las solicitudes enviadas al puerto web HTTP 8280 predeterminado de Orchestrator se redirigen al puerto web HTTPS 8281 predeterminado.
Puerto de servidor HTTPS	8281	TCP	Navegador web de usuario final	Servidor de vRealize Orchestrator	El puerto de acceso para la página de inicio de vRealize Orchestrator.
Puerto de acceso HTTPS de configuración web	8283	TCP	Navegador web de usuario final	Configuración de vRealize Orchestrator	El puerto de acceso SSL para el cliente de vRealize Orchestrator.

Puertos de comunicación externos

Debe configurar el firewall para permitir las conexiones de salida de modo que vRealize Orchestrator se pueda comunicar con servicios externos.

Tabla 5-2. Puertos de comunicación externos de VMware vRealize Orchestrator

Número de puerto	Protocolo	Origen	Destino	Descripción
123	UDP	Servidor de vRealize Orchestrator	Servidor NTP	El puerto predeterminado para conectarse directamente a NTP en lugar de usar la hora del host.
25	TCP	Servidor de vRealize Orchestrator	Servidor SMTP	El puerto que se utiliza para las notificaciones de correo electrónico.
443	TCP	Servidor de vRealize Orchestrator	API de vCenter Server	El puerto de comunicación API de vCenter Server que utiliza vRealize Orchestrator para obtener la infraestructura virtual y la información de máquina virtual de las instancias orquestadas de vCenter Server.
4.000	UDP	Servidor de vRealize Orchestrator	Servidor SNMP	El puerto predeterminado para escuchar capturas de SNMP en el complemento SNMP.
514	UDP	Servidor de vRealize Orchestrator	Servidor de Syslog	El puerto para enviar mensajes de eventos de Syslog.
5432	TCP	Servidor de vRealize Orchestrator	Servidor de PostgreSQL	El puerto que se utiliza para comunicarse con el servidor de PostgreSQL que se configura como base de datos de vRealize Orchestrator.
5434	TCP	Servidor de vRealize Orchestrator	Servidor de PostgreSQL	El puerto que utiliza el servicio de PostgreSQL Manager para la tolerancia a errores de la base de datos.

Conexión con una base de datos de Orchestrator

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

Cuando descarga e implementa Orchestrator Appliance, el servidor de Orchestrator se configura para funcionar con la base de datos de PostgreSQL preinstalada en el dispositivo.

La base de datos Orchestrator PostgreSQL preconfigurada está lista para la producción. Todas las transacciones de Orchestrator PostgreSQL se controlan automáticamente con la interfaz VAMI.

Nota A partir de vRealize Orchestrator 7.5, ya no se admiten bases de datos externas como Oracle o Microsoft SQL.

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 Orchestrator](#)

Los certificados de Orchestrator se pueden administrar en la página **Certificados** del centro de control o bien desde el cliente de Orchestrator mediante los flujos de trabajo de administrador de confianza de SSL en la categoría de flujo de trabajo Configuración.

Administrar certificados de Orchestrator

Los certificados de Orchestrator se pueden administrar en la página **Certificados** del centro de control o bien desde el cliente de Orchestrator mediante los flujos de trabajo de administrador de confianza de SSL en la categoría de flujo de trabajo Configuración.

Importar un certificado al almacén de confianza de Orchestrator

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

Puede cargar el certificado SSL en 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. Para obtener más información sobre la importación de un archivo de certificado con codificación PEM, consulte Importar un certificado de confianza a través del centro de control .

Generar un certificado de servidor autofirmado

Orchestrator Appliance incluye un certificado autofirmado que se genera automáticamente a partir de la configuración de red del dispositivo. Si la configuración de red del dispositivo cambia, debe generar manualmente otro certificado autofirmado. Puede crear un certificado autofirmado 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.

Puede generar un certificado autofirmado en la pestaña **Certificado SSL del servidor de Orchestrator** en la página **Certificados** del centro de control.

Opción	Descripción
Algoritmo de firma	Algoritmo de cifrado para generar una firma digital.
Nombre común	Nombre del host del servidor de Orchestrator.
Organización	Nombre de su organización. Por ejemplo, VMware .
Unidad organizativa	Nombre de la unidad organizativa. Por ejemplo, I+D .
Código de país	Abreviatura del código de país. Por ejemplo, ES .

Orchestrator genera un certificado de servidor exclusivo para su entorno. Los detalles de la clave pública del certificado figuran en la pestaña **Certificado SSL del servidor de Orchestrator**. La clave privada se almacena en la tabla `vmo_keystore` de la base de datos de Orchestrator.

Importar un certificado SSL del servidor de Orchestrator

vRealize Orchestrator utiliza un certificado SSL para identificarse ante los clientes y servidores remotos durante la comunicación segura. De forma predeterminada, Orchestrator incluye un certificado SSL autofirmado que se genera automáticamente según la configuración de red del dispositivo. Puede importar un certificado SSL firmado por una entidad de certificación para prevenir errores de confianza de certificados.

Debe importar un certificado firmado por una entidad de certificación como archivo con codificación PEM que contiene la clave pública y la privada.

Nota Después de generar o importar un certificado de servidor SSL, actualice la pestaña **Certificado SSL del servidor de Orchestrator** para ver los detalles del nuevo certificado. También debe reiniciar el servicio del configurador de Orchestrator.

```
service vco-configurator restart
```

Certificado de firma de paquetes

Los paquetes que se exportan de un servidor de 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.

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.

Nota Orchestrator Appliance incluye un certificado de firma de paquetes autofirmado que se genera de modo automático durante la configuración inicial de Orchestrator. El certificado de firma de paquetes se puede cambiar; después de haberlo hecho, todos los paquetes que se exporten posteriormente se firman con el nuevo certificado.

Importar un certificado de confianza a través del centro de control

Para comunicarse con otros servidores de forma segura, el servidor de Orchestrator debe poder comprobar su identidad. Para ello, puede que tenga que importar el certificado SSL de la entidad remota al almacén de confianza de 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.

Requisitos previos

Busque el nombre del dominio completo del servidor al que desea que Orchestrator se conecte con SSL.

Procedimiento

- 1 Inicie sesión en Orchestrator Appliance sobre SSH como **raíz**.
- 2 Ejecute un comando para recuperar el certificado del servidor remoto.

```
openssl s_client -connect nombre_host_o_DNS:puerto_seguro
```

- a Si usa un puerto no cifrado, utilice `starttls` y el protocolo requerido con el comando `openssl`.

```
openssl s_client -connect nombre_host_o_dns:puerto -starttls smtp
```

- 3 Copie el texto desde la etiqueta -----BEGIN CERTIFICATE----- a la etiqueta -----END CERTIFICATE----- en un editor de texto y guárdelo como archivo.
- 4 Inicie sesión en el centro de control como **raíz**.
- 5 Vaya a la página **Certificados**.
- 6 En la pestaña **Certificados de confianza**, haga clic en **Importar** y seleccione la opción **Importar de un archivo con codificación PEM**.
- 7 Desplácese hasta el archivo del certificado y haga clic en **Importar**.

Resultados

Se importó correctamente el certificado de servidor remoto al almacén de confianza de Orchestrator.

Configurar los complementos de vRealize Orchestrator

Los complementos de vRealize Orchestrator predeterminados se configuran mediante flujos de trabajo específicos del complemento que se ejecutan en el vRealize Orchestrator Client.

vRealize Orchestrator Appliance proporciona acceso a una biblioteca preinstalada de complementos predeterminados. Estos complementos predeterminados se pueden configurar mediante la ejecución de flujos de trabajo específicos del vRealize Orchestrator Client.

Por ejemplo, al introducir las etiquetas *AMQP* y *Configuración* en el cuadro de texto de búsqueda de la biblioteca de flujos de trabajo, se proporcionan los flujos de trabajo que se utilizan para administrar las suscripciones y los agentes de AMQP.

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.

Cambiar el nivel de registro de complementos

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

Instalar o actualizar un complemento nuevo

Con los complementos de vRealize Orchestrator, el servidor de vRealize Orchestrator puede integrarse con otros productos de software. vRealize Orchestrator Appliance incluye un conjunto de complementos preinstalados. También 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. Las extensiones de archivo que pueden usarse son `.vmoapp` y `.dar`. Un archivo `.vmoapp` puede contener una colección de varios archivos `.dar` y puede instalarse como una aplicación. Un archivo `.dar` contiene todos los recursos asociados con un complemento.

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

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

Deshabilitar un complemento

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

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

Instalar o actualizar un complemento de vRealize Orchestrator

Puede instalar o actualizar complementos de terceros con 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.

Desinstalar un complemento

Puede utilizar el centro de control de vRealize Orchestrator para eliminar complementos de terceros. Después de eliminar el complemento del centro de control, debe eliminar el paquete asociado del cliente de vRealize Orchestrator.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Seleccione **Administrar complementos**.
- 3 Seleccione el complemento que desea desinstalar y haga clic en el icono de eliminación del lado derecho.
- 4 Confirme que desea eliminar el complemento y, a continuación, haga clic en **Eliminar**.
- 5 Iniciar sesión en el cliente de vRealize Orchestrator como **administrador**
- 6 Seleccione **Activos > Paquetes**.
- 7 Desplácese hasta el paquete asociado al complemento eliminado y haga clic en **Eliminar**.

Nota Para encontrar el paquete relevante, introduzca una etiqueta específica del complemento en el cuadro de texto de búsqueda. Por ejemplo, puede encontrar el paquete del complemento de Site Recovery Manager introduciendo la etiqueta **SRM**.

- 8 Seleccione **Eliminar el paquete, su contenido, pero mantener todos los elementos compartidos** y haga clic en **Eliminar**.
- 9 Inicie sesión en el cliente heredado de Orchestrator como administrador.
- 10 En el menú **Herramientas** de la esquina superior derecha, seleccione **Preferencias del usuario**.
- 11 En la página **General**, seleccione la casilla de verificación **Permitir la eliminación de una carpeta no vacía**.
- 12 Haga clic en **Guardar y cerrar**.

Ahora puede eliminar una carpeta completa, incluidos los flujos de trabajo y las subcarpetas, con un único clic.
- 13 Haga clic en la pestaña **Flujo de trabajo**.
- 14 Elimine la carpeta del complemento que quiere desinstalar.
- 15 Haga clic en la pestaña **Acciones**.
- 16 Elimine los módulos de acción del complemento que quiere desinstalar.
- 17 Reinicie los servicios de vRealize Orchestrator.

Resultados

Ha quitado todos los flujos de trabajo personalizados, acciones, políticas, configuraciones, parámetros y recursos relativos al complemento.

Disponibilidad y escalabilidad de Orchestrator

Para incrementar la disponibilidad de los servicios de Orchestrator, inicie varias instancias del servidor de 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.

Clúster de Orchestrator

Varias instancias del servidor de 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 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 Orchestrator dejase de responder. Si una instancia activa del servidor de 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 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.

Orchestrator no proporciona una herramienta integrada para supervisar el estado del clúster y enviar notificaciones de conmutación por error. Puede supervisar el estado del clúster mediante un componente externo, por ejemplo un equilibrador de carga. Para comprobar si un nodo se está ejecutando, puede utilizar el servicio de la API de REST de estado del sistema en la dirección `https://your_orchestrator_server_IP_or_DNS_name:8281/vco/api/healthstatus` y comprobar el estado del nodo o en `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/docs/` para supervisar el estado del Centro de control.

Configurar un clúster de instancias de vRealize Orchestrator en VAMI

A partir de vRealize Orchestrator 7.5, todas las operaciones de agrupación en clústeres se llevan a cabo con la interfaz de VAMI de Orchestrator Appliance.

Un clúster de Orchestrator está formado por al menos dos instancias de Orchestrator que comparten una base de datos. Debe configurar un clúster nuevo de Orchestrator o añadir nodos nuevos a un clúster existente desde la interfaz de VAMI de Orchestrator. Hay tres tipos de nodos en el clúster de Orchestrator.

Tipo de nodo	Definición
Nodo principal	Cada clúster de Orchestrator tiene un nodo principal. Todos los nodos del clúster comparten la base de datos PostgreSQL del nodo principal. La base de datos principal se puede ejecutar en los modos síncrono y asíncrono. El nodo principal debe estar en buen estado para que el clúster funcione correctamente.
Nodo de réplica	Los nodos de réplica son instancias de Orchestrator unidas al nodo principal de Orchestrator.
Nodo de réplica sincronizada	Si se habilita el modo síncrono, el estado de un nodo de réplica se promueve a nodo de réplica sincronizada. La réplica sincronizada permite la conmutación por error automática del nodo principal.

Requisitos previos

- Configure al menos dos nodos de servidor independientes. Para obtener más información, consulte [Configurar un servidor de Orchestrator independiente](#).
- Sincronice los relojes de las máquinas virtuales en las que están instaladas las instancias de Orchestrator.
- Configure un equilibrador de carga para distribuir el tráfico por varias instancias de Orchestrator.

Procedimiento

- 1 Inicie sesión en la interfaz de VAMI como usuario **raíz**.

Acceda a la interfaz VAMI en https://IP_o_DNS_de_su_servidor_orchestrator:5480.

- 2 Seleccione la pestaña **Clúster** e introduzca las credenciales del nodo de Orchestrator que hará de nodo principal del clúster.

Para los entornos en clúster de Orchestrator existentes, introduzca las credenciales del nodo principal del clúster de Orchestrator.

- 3 Haga clic en **Unirse a clúster**.

- 4 Revise la información del certificado del nodo y haga clic en **Aceptar**.

- 5 La operación de agrupación en clústeres sincroniza el contenido de los nodos de Orchestrator y une el nodo de réplica a la base de datos PostgreSQL del nodo principal.

Pasos siguientes

Compruebe que el clúster esté bien configurado en la página **Validar configuración** del centro de control de Orchestrator.

Nota De acuerdo con la configuración del nodo del clúster, el servidor de Orchestrator se reinicia automáticamente al cabo de 2 minutos. La verificación de la configuración inmediatamente después de la finalización del proceso puede devolver un estado de clúster no válido.

Supervisar un clúster de Orchestrator

Después de crear un clúster, puede supervisar los estados de los nodos del clúster.

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 Orchestrator que se han unido en un clúster.

Estado de sincronización de la configuración	Descripción
EN EJECUCIÓN	El servicio de Orchestrator está disponible y puede aceptar solicitudes.
EN ESPERA	<p>El servicio de 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 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 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 Orchestrator se reinicia automáticamente.

Habilitar el modo sincrónico para el clúster de Orchestrator

Puede configurar un clúster de la base de datos de Orchestrator para que se ejecute en modo sincrónico.

El modo sincrónico permite la conmutación por error automática de la base de datos principal de Orchestrator. El proceso promueve uno de los nodos de réplica al estado **Réplica sincronizada**. Si se produce un error en el nodo principal actual, la réplica sincronizada se promueve automáticamente al nodo principal. La réplica sincronizada recibe todas las transacciones finalizadas de la base de datos del nodo principal.

Requisitos previos

Configure un clúster de Orchestrator que esté formado por al menos tres nodos de Orchestrator.

Procedimiento

- 1 Inicie sesión en la interfaz de VAMI como usuario **raíz**.

Acceda a la interfaz VAMI en https://IP_o_DNS_de_su_servidor_orchestrator:5480.

- 2 Seleccione la pestaña **Clúster**.

- 3 Haga clic en **Modo sincrónico**.

- 4 Uno de los nodos del clúster se promueve al estado de una **réplica sincronizada**.

Para confirmar que la operación de sincronización se ha efectuado correctamente, compruebe que el estado del modo de réplica de la pestaña **Clúster** es **La base de datos está en modo sincrónico**.

Promover un nodo de réplica de Orchestrator al nodo principal

Puede volver a configurar un clúster de Orchestrator promoviendo un nodo de réplica a un nodo principal.

Los nodos de Orchestrator se pueden promover tanto en el modo asincrónico como en el modo sincrónico.

Nota Los clústeres de Orchestrator en modo sincrónico disponen de una función de conmutación por error automática. De esta forma, si se produce un error en el nodo principal actual, el nodo de réplica sincronizada se convertirá automáticamente en el nuevo nodo principal.

Requisitos previos

Configure un clúster de Orchestrator que esté formado por al menos dos instancias de Orchestrator.

Procedimiento

- 1 Inicie sesión en la interfaz de VAMI como usuario **raíz**.
Acceda a la interfaz VAMI en https://IP_o_DNS_de_su_servidor_orchestrator:5480.
- 2 Seleccione la pestaña **Clúster**.
- 3 Haga clic en la opción **Promover** situada al lado del nodo de réplica que desea promover al estado del nuevo nodo principal.
- 4 En la parte superior izquierda de la interfaz de usuario de VAMI se muestra el mensaje **Se ha promovido correctamente al nuevo nodo principal** y el estado del nodo pasa a ser **PRINCIPAL**.

Eliminar un nodo de clúster de Orchestrator

Puede eliminar un nodo de réplica de Orchestrator del clúster de Orchestrator, de manera que pueda sustituirlo o reducir su capacidad.

Solo se pueden eliminar nodos de réplica del clúster. Para eliminar un nodo principal, primero debe promover un nodo de réplica para sustituirlo. Para obtener más información, consulte [Promover un nodo de réplica de Orchestrator al nodo principal](#).

Procedimiento

- 1 Inicie sesión en la interfaz de VAMI como usuario **raíz**.
Acceda a la interfaz VAMI en https://IP_o_DNS_de_su_servidor_orchestrator:5480.
- 2 Seleccione la pestaña **Clúster**.
- 3 Seleccione el comando **Eliminar** situado al lado del nodo de réplica.
- 4 Confirme que desea eliminar el nodo de réplica del clúster y haga clic en **Aceptar**.

Nota Debe eliminar del servidor del equilibrador de carga el nombre de host del nodo de réplica eliminado.

- 5 El nodo de Orchestrator se elimina del clúster y, en la parte superior izquierda de la interfaz de usuario, aparece el mensaje **El nodo se ha eliminado correctamente**.

Configuración del Programa de mejora de la experiencia del cliente

Si decide participar en el Programa de mejora de la experiencia de cliente, VMware recibe información anónima que le permite mejorar la calidad, la fiabilidad 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 o abandonar el CEIP de este producto, consulte [Participe en el programa de mejora de la experiencia de cliente \(CEIP\)](#).

Participe en el programa de mejora de la experiencia de cliente (CEIP)

Únase al programa de mejora de la experiencia del cliente del centro de control

Procedimiento

- 1 Inicie sesión en el centro de control como usuario **raíz** y abra la página **Programa de mejora de la experiencia de cliente**.
- 2 Seleccione la casilla de verificación **Únase al programa de mejora de la experiencia del cliente** para habilitar CEIP o desmarque la casilla de verificación para deshabilitar el programa y, a continuación, haga clic en **Guardar**.
- 3 (opcional) Desmarque la casilla de verificación de **Detección automática del proxy** si desea agregar un host proxy manualmente.

Usar los servicios de la API

6

Para configurar Orchestrator mediante el centro de control, puede modificar la configuración del servidor de Orchestrator utilizando la API de REST de Orchestrator, la API de REST del centro de control o la utilidad de la línea de comandos, almacenados en el dispositivo.

El complemento Configuración se incluye de forma predeterminada en el paquete de Orchestrator. Puede acceder a los flujos de trabajo del complemento Configuración desde la biblioteca de flujos de trabajo de Orchestrator o la API de REST de Orchestrator. Con estos flujos de trabajo, puede cambiar la configuración del certificado de confianza y el almacén de claves del servidor de Orchestrator. Para obtener información sobre todas las llamadas de servicio de la API de REST de Orchestrator disponibles, consulte la documentación de *referencia de la API de REST de Orchestrator*, en https://orchestrator_server_IP_or_DNS_name:8281/vco/api/docs.

- **Administración de certificados SSL y de almacenes de claves mediante la API de REST**

Además de administrar certificados SSL mediante el centro de control, puede administrar certificados de confianza y almacenes de claves cuando ejecuta flujos de trabajo desde el complemento Configuración o mediante la API de REST.

- **Automatización de la configuración de Orchestrator utilizando la API de REST del centro de control**

La API de REST del centro de control proporciona acceso a los recursos para configurar el servidor de Orchestrator. Puede utilizar la API de REST del centro de control con sistemas de terceros para automatizar la configuración de Orchestrator.

Administración de certificados SSL y de almacenes de claves mediante la API de REST

Además de administrar certificados SSL mediante el centro de control, puede administrar certificados de confianza y almacenes de claves cuando ejecuta 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 SSL y almacenes de claves. Puede acceder a estos flujos de trabajo navegando a **Biblioteca > Configuración > Administrador de confianza de SSL y Biblioteca > Configuración > Almacenes de claves**, respectivamente, en la vista Flujos de trabajo del cliente de Orchestrator. También puede ejecutar estos flujos de trabajo mediante la API de REST de Orchestrator.

Eliminación de un certificado SSL utilizando la API de REST

Puede eliminar un certificado SSL ejecutando el flujo de trabajo Eliminar certificado de confianza 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 certificado de confianza.

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

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

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

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

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

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

Importar certificados SSL mediante la API de REST

Puede importar certificados SSL 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. Para obtener información sobre cómo importar certificados en Orchestrator mediante el centro de control, consulte [Administrar certificados de Orchestrator](#).

Procedimiento

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

Opción	Descripción
Importar certificado de confianza de 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://{host_orchestrator}:{puerto}/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://{host_orchestrator}:{puerto}/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://{host_orchestrator}:{puerto}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5/
executions
```

- 4 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 SSL. 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 SSL. 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

- 1 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
```

- 2 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/
```

- 3 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/
```

- 4 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.

Automatización de la configuración de Orchestrator utilizando la API de REST del centro de control

La API de REST del centro de control proporciona acceso a los recursos para configurar el servidor de Orchestrator. Puede utilizar la API de REST del centro de control con sistemas de terceros para automatizar la configuración de Orchestrator.

El endpoint raíz de la API de REST del centro de control es `https://`

`IP_servidor_orchestrator_onombre_DNS:8283/vco-controlcenter/api`. Para obtener información sobre todas las llamadas de servicio disponibles que puede realizar en la API de REST del centro de control, consulte la documentación *Referencia de la API de REST del centro de control* en `https://IP_servidor_orchestrator_o_nombre_DNS:8283/vco-controlcenter/docs`.

Utilidad de línea de comandos

La utilidad de línea de comandos de Orchestrator permite automatizar la configuración de Orchestrator.

Acceda a la utilidad de línea de comandos iniciando sesión en Orchestrator Appliance como raíz a través de SSH. La utilidad se encuentra en `/var/lib/vco/tools/configuration-cli/bin`. Para ver la opciones de configuración disponibles, ejecute `./vro-configure.sh --help`.

Opciones de configuración adicionales

7

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

Este capítulo incluye los siguientes temas:

- [Volver a configurar la autenticación](#)
- [Exportar la configuración de Orchestrator](#)
- [Importar la configuración de Orchestrator](#)
- [Configurar las propiedades de ejecución de los flujos de trabajo](#)
- [Archivos de log de Orchestrator](#)
- [Añadir controladores de interfaz de red](#)
- [Configurar rutas estáticas](#)
- [Habilitar las extensiones de Opentracing y Wavefront](#)
- [Configurar la extensión de Opentracing](#)
- [Configurar la extensión de Wavefront](#)

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.

Requisitos previos

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.
- 3 En la sección **SERVICIO DE IDENTIDADES**, haga clic en **ELIMINAR DEL REGISTRO** para eliminar las credenciales del servidor.

Resultados

El proveedor de autenticación se ha eliminado del registro correctamente.

Pasos siguientes

Vuelva a configurar la autenticación en el Centro de control. Para obtener más información, consulte [Configurar un servidor de Orchestrator independiente con la autenticación de vRealize Automation](#) o [Configurar un servidor de Orchestrator independiente con autenticación de vSphere](#).

Cambiar los parámetros de autenticación

Cuando utilice vRealize Automation como un proveedor de autenticación en el centro de control, es posible que desee cambiar el tenant predeterminado del grupo de administradores de Orchestrator. Cuando se utiliza la autenticación de vSphere, puede cambiar el grupo de administradores.

Requisitos previos

- Inicie sesión en el centro de control como **raíz**.
- Seleccione el modo de autenticación y configure los ajustes de conexión del proveedor de autenticación.

Procedimiento

- 1 Cambie el tenant predeterminado.

Nota Solo puede cambiar el tenant predeterminado si utiliza el modo de autenticación de vRealize Automation.

- a En la página **Configurar proveedor de autenticación** en el centro de control, haga clic en el botón **CAMBIAR** situado junto al cuadro de texto **Tenant predeterminado**.
- b En el cuadro de texto, sustituya el nombre del tenant predeterminado existente por el que desee utilizar.

- c 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.

- d Escriba el nombre de un grupo de administradores y haga clic en **BUSCAR**.
- e En la lista de grupos, haga doble clic en el nombre del grupo para seleccionarlo.
- f Haga clic en **GUARDAR CAMBIOS**.

Se cerrará la sesión en el centro de control y se le redirigirá a la pantalla de inicio de sesión Single Sign-On.

2 Cambie el grupo de administradores.

- a Haga clic en el botón **CAMBIAR** situado junto al cuadro de texto **Grupo de administradores**.
- b Escriba el nombre de un grupo de administradores y haga clic en **BUSCAR**.
- c En la lista de grupos, haga doble clic en el nombre del grupo para seleccionarlo.
- d Haga clic en **GUARDAR CAMBIOS**.

Se cerrará la sesión en el centro de control y se le redirigirá a la pantalla de inicio de sesión Single Sign-On.

Exportar la configuración de Orchestrator

El centro de control proporciona un mecanismo para exportar la configuración de Orchestrator a un archivo local. Puede utilizar el mecanismo para tomar una instantánea de la configuración del sistema en cualquier momento e importar dicha configuración a una nueva instancia de Orchestrator.

Debe exportar y guardar la configuración de forma regular, en especial cuando realiza modificaciones, lleva a cabo tareas de mantenimiento o actualiza el sistema.

Importante Guarde en un lugar seguro el archivo con la configuración exportada, ya que contiene información administrativa confidencial.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Haga clic en **Exportar o importar configuración**.
- 3 Seleccione el tipo de archivos que quiere exportar.

Nota Si selecciona **Exportar configuraciones de complementos** y las configuraciones de complementos contienen propiedades cifradas, también debe seleccionar **Exportar configuración de servidor** para descifrar correctamente los datos al importar.

- 4 (opcional) Escriba una contraseña para proteger el archivo de configuración.

Utilice la misma contraseña cuando importe la configuración más tarde.

- 5 Haga clic en **Exportar**.

Resultados

Orchestrator crea un archivo `orchestrator-config-export-hostname-dateReference.zip` que se descarga en el equipo local. Puede utilizar este archivo para clonar o restaurar el sistema.

Importar la configuración de Orchestrator

Puede restablecer una configuración de sistema exportada previamente después de reinstalar Orchestrator o si se produce un error en el sistema.

Si utiliza el procedimiento de importación para clonar la configuración de Orchestrator, la configuración del complemento vCenter Server deja de ser válida y no funciona, ya que se genera un nuevo ID de complemento vCenter Server.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Haga clic en **Exportar/importar configuración** y vaya a la pestaña **Importar configuración**.
- 3 Busque y seleccione el archivo `.zip` que ha exportado desde su instalación anterior.

Nota La sintaxis predeterminada para el archivo de configuración exportado es `orchestrator-config-export-hostname-dateofexport_timeofexport.zip`

- 4 (opcional) Introduzca la contraseña que utilizó al exportar la configuración.
Este paso es innecesario si no exportó la configuración con una contraseña.
- 5 Seleccione el tipo de importación:

Opción	Descripción
Integrado	Se migra a una instancia de Orchestrator que está integrada en vRealize Automation.
Externo	Se migra a un Orchestrator externo.
Réplica	Replica la misma instancia de Orchestrator.

- 6 Haga clic en **Importar**.

Resultados

El nuevo sistema replica la configuración antigua según el tipo de importación seleccionado. El servicio del servidor de Orchestrator se reinicia automáticamente.

Pasos siguientes

Compruebe que Orchestrator esté configurado correctamente en la página **Validar configuración** del centro de control.

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 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.

En la página **Opciones avanzadas** del centro de control, puede configurar las propiedades de ejecución de los flujos de trabajo.

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 Orchestrator.
Cantidad de flujos de trabajo en ejecución simultánea	Cantidad máxima de flujos de trabajo del nodo de Orchestrator que se ejecutan a la vez.
Cantidad máxima de flujos de trabajo en ejecución en la cola	Cantidad de solicitudes de ejecución de flujo de trabajo que el nodo de Orchestrator acepta antes de pasar al estado de no disponible.
Cantidad máxima de ejecuciones conservadas por flujo de trabajo	Cantidad máxima de ejecuciones de flujos de trabajo concluidos que se conservan como historial por flujo de trabajo en un clúster. Si se sobrepasa ese número, se eliminan las ejecuciones de flujos de trabajo más antiguas.
Días de caducidad para eventos de log	Cantidad de días que los eventos de log del clúster se mantienen en la base de datos antes de purgarse.
Elaborar perfiles de todas las ejecuciones de flujos de trabajo	Habilita y deshabilita la generación automática de perfiles de flujos de trabajo. Si se habilita, la generación de perfiles de flujos de trabajo genera datos de métricas en todas las ejecuciones de flujos de trabajo.
Intervalo para distribuir las estadísticas de Workflow Profiler	Intervalo durante el que se distribuirán las estadísticas de Profiler por todas las instancias de Orchestrator del entorno.

Archivos de log de 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.

Puede descargar un paquete zip que incluye los archivos de log y de configuración de Orchestrator desde el menú **Exportar logs** del centro de control.

Tabla 7-1. Lista de archivos de log de Orchestrator

Nombre de archivo	Ubicación	Descripción
scripting.log	/var/log/vco/app-server	Proporciona mensajes de log de creación de scripts de los flujos de trabajo y las acciones. Utilice el archivo scripting.log para aislar ejecuciones de flujos de trabajo y de acciones de las operaciones normales de Orchestrator. Esta información también se incluye en el archivo server.log.
server.log	/var/log/vco/app-server	Proporciona información sobre todas las actividades que hay en el servidor de Orchestrator. Analice el archivo server.log cuando depure Orchestrator o cualquier otra aplicación que se ejecute en Orchestrator.
metrics.log	/var/log/vco/app-server	Contiene información de tiempo de ejecución del servidor. La información se añade a este archivo de log cada 5 minutos.
localhost_access_log.txt	/var/log/vco/app-server	Contiene el registro de solicitudes HTTP del servidor.
localhost_access_log.fecha.txt	/var/log/vco/configuration	Contiene el registro de solicitudes HTTP del servicio del centro de control.
controlcenter.log	/var/log/vco/configuration	Archivo de log del servicio del centro de control.

Registro de la persistencia

Puede registrar información de cualquier script de Orchestrator, por ejemplo flujo de trabajo, política 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 7-2. Creación de 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 del servidor) efectúan el seguimiento de los registros de ejecución de flujos de trabajo completados y se guardan en la base de datos de Orchestrator. Para ver registros del servidor, debe seleccionar un flujo de trabajo, una ejecución completada de flujo de trabajo o una política y, a continuación, hacer clic en la pestaña **Eventos** en el cliente de Orchestrator.

Registros no persistentes

Si se utiliza un registro no persistente (registro del sistema) para crear scripts, el servidor de Orchestrator notifica este registro a todas las aplicaciones de Orchestrator que se ejecutan; sin embargo, esta información no se guarda en la base de datos. La información del registro se pierde cuando se reinicia la aplicación. Los registros no persistentes se utilizan para depuración y para información activa. Para ver registros del sistema, debe seleccionar un flujo de trabajo, una ejecución completada de flujo de trabajo en el cliente de Orchestrator y, a continuación, hacer clic en **Registros** en la pestaña **Esquema**.

Configuración de registros de Orchestrator

En la página **Configurar registros** del centro de control, puede definir el nivel de registro del servidor que necesite. Si alguno los registros se genera varias veces al día, resulta complicado determinar lo que causa problemas.

El nivel de registro predeterminado del registro del servidor y del registro de creación de scripts es INFO. Cambiar el nivel de registro repercute en todos los mensajes nuevos que el servidor incorpora a los registros, 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 registro 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.

Configuración de rotación de registros

Para evitar que el registro del servidor tenga un tamaño demasiado grande, puede establecer la cantidad y el tamaño máximos del archivo modificando los valores de los cuadros de texto **Cantidad máxima de archivos** y **Tamaño máximo de archivo (MB)**.

Exportar archivos de registro de Orchestrator

En la página **Exportar registros** del Centro de control, puede generar un archivo ZIP de información para solucionar problemas que contiene archivos de configuración, servidor, contenedor y de registro de instalación.

La información de registro se guarda en un archivo ZIP llamado `vco-logs-date_hour.zip`.

Nota Cuando hay más de una instancia de Orchestrator en un clúster, el archivo ZIP incluye los registros de todas las instancias de Orchestrator incluidas en el clúster.

Filtrar los registros de Orchestrator

Puede filtrar los registros del servidor de Orchestrator para la ejecución de un flujo de trabajo específico y recopilar datos de diagnóstico sobre la ejecución del flujo de trabajo.

Los registros de Orchestrator contienen mucha información útil que puede supervisar en tiempo real. Cuando se ejecutan varias instancias del mismo flujo de trabajo al mismo tiempo, puede realizar un seguimiento de las distintas ejecuciones del flujo de trabajo filtrando los datos de diagnóstico de cada ejecución en el registro en directo de Orchestrator.

Nota Si tiene más de una instancia de Orchestrator en un clúster, el registro en directo muestra solo los registros del nodo local de Orchestrator.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Haga clic en el **Registro en directo**.
- 3 En la barra de búsqueda, introduzca los parámetros de búsqueda.

Por ejemplo, puede filtrar los registros por un nombre de usuario, nombre de flujo de trabajo, identificador de flujo de trabajo o identificador de token.
- 4 (opcional) Seleccione **Distinguir mayúsculas y minúsculas** y **Filtro (grep)** para filtrar aún más los resultados de búsqueda.

Mediante la selección de **filtro (grep)** el registro en directo solo muestra las líneas que coinciden con los parámetros de búsqueda.

Resultados

El registro en directo de Orchestrator se filtra según los parámetros de búsqueda definidos.

Pasos siguientes

Puede usar herramientas de análisis de registro de terceros si desea filtrar registros antiguos a los que no se puede acceder a través de la página **Registro en directo** del Centro de control.

Configurar la integración del registro con el servidor remoto

Puede configurar Orchestrator para que envíe registros a sistemas de registro remotos, como vRealize Log Insight u otros servidores syslog.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Desplácese hasta el menú **Integración de registro**.
- 3 Active la opción **Habilitar registro en un servidor de registros remoto**.

- 4 Configure las opciones de integración del registro.
 - a Seleccione el tipo de sistema de registro.
 - b Introduzca el nombre de host y el valor de puerto del servidor de registro remoto.
 - c Seleccione el protocolo utilizado para enviar eventos de registro al servidor de registro remoto.
- 5 Para finalizar la configuración de la integración del registro en el servidor remoto, haga clic en **Guardar**.

Añadir controladores de interfaz de red

vRealize Orchestrator es compatible con varios controladores de interfaz de red (NIC). Una vez concluida la instalación, puede añadir NIC al dispositivo de Orchestrator.

Requisitos previos

Instale completamente vRealize Orchestrator en el entorno de vCenter Server.

Procedimiento

- 1 En vCenter Server, añada NIC a cada dispositivo de vRealize Orchestrator.
 - a Haga clic con el botón secundario en el dispositivo y seleccione **Editar configuración**.
 - b Añada NIC VMXNET3.
 - c Si el dispositivo está encendido, reinícielo.
- 2 Inicie sesión en la interfaz de administración de dispositivos de vRealize Orchestrator como usuario raíz.

<https://IP-dispositivo-orchestrator:5480>
- 3 Seleccione **Red** y compruebe que haya varios NIC disponibles.
- 4 Seleccione **Dirección** y configure la dirección IP para los NIC.

Tabla 7-3. Ejemplo de configuración de NIC

Configuración	Valor
Tipo de dirección IPv4	Estático
Dirección IPv4	172.22.0.2
Máscara de red	255.255.255.0

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

Configurar rutas estáticas

A la hora de añadir NIC a una instalación de vRealize Orchestrator, si necesita rutas estáticas, abra una sesión del símbolo del sistema para configurarlas.

Requisitos previos

Añada varios NIC a los dispositivos de vRealize Orchestrator.

Procedimiento

- 1 Inicie sesión en la línea de comandos del dispositivo de vRealize Orchestrator como usuario raíz.
- 2 Abra el archivo de rutas en un editor de texto.
`/etc/sysconfig/network/routes`
- 3 Busque la línea `default` de la puerta de enlace predeterminada, pero no la modifique.

Nota En los casos en los que se deba cambiar la puerta de enlace predeterminada, utilice la interfaz de administración de vRealize Orchestrator.

- 4 Debajo de la línea `default`, añada nuevas líneas para las rutas estáticas. Por ejemplo:

```
default 10.10.10.1 - -
172.30.30.0 192.168.100.1 255.255.255.0 eth0
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

- 5 Guarde y cierre el archivo de rutas.
- 6 Reinicie el dispositivo.
- 7 En los clústeres de alta disponibilidad, repita el proceso para cada dispositivo.

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. El estado del servicio SSH se puede comprobar en la pestaña **Administrador** de la interfaz VAMI de vRealize Orchestrator.

Procedimiento

- 1 Inicie sesión en vRealize Orchestrator Appliance con un cliente SSH como usuario **raíz**.
Acceda a vRealize Orchestrator Appliance en `https://su_nombre_de_host_de_orchestrator:5480`.

- 2 Vaya al directorio de extensiones.

```
cd /var/lib/vco/app-server/extensions
```

- 3 Ejecute el comando `ls` para enumerar todas las extensiones de vRealize Orchestrator disponibles.

- 4 Habilite las extensiones de Wavefront y Opentracing.

```
mv opentracing-7.6.0.jar.inactive opentracing-7.6.0.jar
```

```
mv wavefront-7.6.0.jar.inactive wavefront-7.6.0.jar
```

- 5 Vuelva a ejecutar el comando `ls` y confirme que las extensiones no terminan con `.inactive`.

Pasos siguientes

Configure la integración de Opentracing y Wavefront con vRealize Orchestrator en la página **Propiedades de extensión** del centro de control. Para obtener más información, consulte [Configurar la extensión de Opentracing](#) y [Configurar la extensión de Wavefront](#).

Configurar la extensión de Opentracing

La extensión de Opentracing envía datos sobre las 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

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

Procedimiento

- 1 Inicie sesión en el centro de control de Orchestrator como usuario **raíz**.
- 2 Vaya a 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

Ha configurado la extensión de Opentracing de 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 Orchestrator.

Requisitos previos

- 1 Confirme que Wavefront esté habilitado en Orchestrator Appliance. Para obtener más información, consulte [Habilitar las extensiones de Opentracing y Wavefront](#).
- 2 Importe el certificado de Wavefront:
 - a Inicie sesión en el centro de control de Orchestrator como usuario **raíz**.
 - b Vaya a 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 Orchestrator como usuario **raíz**.
- 2 Vaya a 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 del 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

Ha configurado la extensión de Wavefront de 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 Orchestrator, puede utilizar las alertas de Wavefront. Para obtener más información, consulte la [Documentación sobre las alertas de Wavefront](#).

Resolución de problemas y casos de uso de configuración

8

Puede configurar el servidor de Orchestrator para que funcione con el dispositivo vCenter Server, desinstalar los complementos de Orchestrator o cambiar los certificados autofirmados.

Los casos de uso de configuración proporcionan flujos de tareas que pueden llevarse a cabo para cumplir determinados requisitos de configuración del servidor de Orchestrator, así como temas de resolución de problemas para comprender y solucionar problemas, en caso de que exista una solución.

Este capítulo incluye los siguientes temas:

- [Configurar el complemento de vRealize Orchestrator para vSphere Web Client](#)
- [Eliminación de la autenticación de Orchestrator del registro](#)
- [Cambio de certificados SSL](#)
- [Cancelar flujos de trabajo en ejecución](#)
- [Activación de la depuración del servidor de Orchestrator](#)
- [Realizar una copia de seguridad de la configuración y elementos de Orchestrator](#)
- [Copia de seguridad y restauración de vRealize Orchestrator](#)
- [Recuperación ante desastres de Orchestrator mediante Site Recovery Manager](#)

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

Debe registrar vRealize Orchestrator con la autenticación de vSphere en el mismo Platform Services Controller que utiliza su instancia de vCenter Server para autenticarse.

Procedimiento

- 1 Inicie sesión en el cliente de vRealize Orchestrator.
- 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 (opcional) Introduzca `https://su_nombre_de_host_de_orchestrator:8281` 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**.

Eliminación de la autenticación de Orchestrator del registro

Elimine del registro a Orchestrator como solución de Single Sign-On en la página Configurar proveedor de autenticación del centro de control.

Para volver a configurar la autenticación de Orchestrator vCenter Single Sign-On o de vRealize Automation, primero se debe eliminar del registro la autenticación de Orchestrator.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Haga clic en **Configurar proveedor de autenticación**.
- 3 Haga clic en **Eliminar del registro**.
- 4 (opcional) Para eliminar los datos de registro del servidor de identidades, proporcione sus credenciales.
- 5 Haga clic en **Eliminar del registro** en la sección **Servicio de identidad**.

Resultados

Ha eliminado la instancia del servidor de Orchestrator del registro correctamente.

Cambio de certificados SSL

De forma predeterminada, el servidor de Orchestrator utiliza un certificado SSL autofirmado para comunicarse remotamente con el cliente de Orchestrator. Puede cambiar los certificados SSL si, por ejemplo, la política de seguridad de su empresa requiere que se usen sus certificados SSL.

Cuando intenta utilizar Orchestrator a través de una conexión a Internet SSL de confianza y abre el centro de control en un navegador web, recibe una advertencia que indica que la conexión no es de confianza en caso de utilizar Mozilla Firefox, o que indica que se han detectado problemas con el certificado de seguridad del sitio web, si usa Internet Explorer.

Después de hacer clic en **Pasar a este sitio web (no recomendado)**, aunque haya importado el certificado SSL en el almacén de confianza, sigue viendo el error de certificado en rojo en la barra de direcciones del navegador web. Puede trabajar con Orchestrator en el navegador web, pero un sistema de terceros podría no funcionar correctamente cuando intenta acceder a la API a través de HTTPS.

También puede recibir una advertencia de certificado si inicia el cliente de Orchestrator e intenta conectar el servidor de Orchestrator a través de una conexión SSL.

Puede resolver el problema instalando un certificado firmado por una entidad de certificación (CA) comercial. Para dejar de recibir advertencias sobre certificados del cliente de Orchestrator, añada su certificado raíz de CA al almacén de claves de Orchestrator en el equipo en que esté instalado el cliente de Orchestrator.

Adición de un certificado a un almacén local

Una vez que haya recibido un certificado de una entidad de certificación, debe añadirlo a su almacén local para que funcione con el centro de control y no se generen advertencias ni mensajes de error relativos a los certificados.

Este flujo de trabajo describe el proceso de añadir un certificado a su almacén local mediante Internet Explorer.

- 1 Abra Internet Explorer y vaya a `https://IP_servidor_orchestrator_o_nombre_DNS:8283/`.
- 2 Cuando se le solicite, haga clic en **Pasar a este sitio web (no recomendado)**.
El error de certificado aparece en el lado derecho de la barra de direcciones en Internet Explorer.
- 3 Haga clic en el error de certificado y seleccione **Ver certificados**.
- 4 Haga clic en **Instalar certificado**.
- 5 En la página de bienvenida del **Asistente para importación de certificados**, haga clic en **Siguiente**.
- 6 En la ventana **Almacén de certificados**, seleccione **Colocar todos los certificados en el siguiente almacén**.
- 7 Busque y seleccione **Entidades de certificación raíz de confianza**.
- 8 Complete el asistente y reinicie Internet Explorer.
- 9 Vaya al servidor de Orchestrator a través de su conexión SSL.

Ya no recibirá ninguna advertencia ni aparecerá el error de certificado en la barra de direcciones.

Otros sistemas y aplicaciones, como VMware Service Manager, deben tener acceso a las API de REST de Orchestrator a través de una conexión SSL.

Cambio del certificado del sitio de administración de Orchestrator Appliance

Orchestrator Appliance utiliza Light HTTPd para ejecutar su propio sitio de administración. Puede cambiar el certificado SSL del sitio de administración de Orchestrator Appliance si, por ejemplo, la política de seguridad de su empresa requiere que se usen sus certificados SSL.

Requisitos previos

De forma predeterminada, el certificado SSL y la clave privada de Orchestrator Appliance se almacenan en un archivo PEM, ubicado en `/opt/vmware/etc/lighttpd/server.pem`. Para instalar un nuevo certificado, asegúrese de exportar el nuevo certificado SSL y la clave privada desde el almacén de claves de Java en un archivo PEM.

Procedimiento

- 1 Inicie sesión en la consola de Linux de Orchestrator Appliance como raíz.
- 2 Localice el archivo `/opt/vmware/etc/lighttpd/lighttpd.conf` y ábralo en un editor.
- 3 Busque la línea siguiente:

```
#### SSL engine
ssl.engine = "enable"
ssl.pemfile = "/opt/vmware/etc/lighttpd/server.pem"
```

- 4 Cambie el atributo `ssl.pemfile` para que apunte al archivo PEM que contiene el nuevo certificado SSL y la nueva clave privada.
- 5 Guarde el archivo `lighttpd.conf`.
- 6 Ejecute el comando siguiente para reiniciar el servidor light-httpd.

```
service vami-lighttpd restart
```

Resultados

Ha cambiado correctamente el certificado del sitio de administración de Orchestrator Appliance.

Cancelar flujos de trabajo en ejecución

Puede usar el centro de control para cancelar flujos de trabajo que no finalizan 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.

Pasos siguientes

Verifique que los flujos de trabajo se cancelan desde la página **Inspeccionar flujos de trabajo** en el centro de control.

Activación de la depuración del servidor de Orchestrator

Puede iniciar el servidor de Orchestrator en modo de depuración para depurar los problemas durante el desarrollo de un complemento.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Haga clic en **Depuración de Orchestrator**.
- 3 Haga clic en **Habilitar depuración**.
- 4 (opcional) Introduzca un puerto diferente del predeterminado.
- 5 (opcional) Haga clic en **Suspender**.

Al seleccionar esta opción, debe adjuntar un depurador antes de iniciar el servidor de Orchestrator.

- 6 Haga clic en **Guardar**.
- 7 Abra la página Opciones de inicio en el centro de control y haga clic en **Reiniciar**.

Resultados

El servidor de Orchestrator se suspende al inicio hasta que se adjunta un depurador remoto de Java al puerto definido.

Realizar una copia de seguridad de la configuración y elementos de Orchestrator

Haga una copia de seguridad de la configuración del servidor personalizado de Orchestrator y los elementos del flujo de trabajo para garantizar su reutilización en otras instancias de Orchestrator.

Si edita los flujos de trabajo, acciones, directivas o elementos de configuración estándares y, a continuación, importa un paquete que contiene los mismos elementos con una versión posterior de Orchestrator, se pierden los cambios realizados en los elementos. Puede impedir la pérdida de flujos de trabajo personalizados y de otros elementos; para ello, deberá exportarlos antes de migrar la instancia de Orchestrator.

Cada instancia del servidor de Orchestrator tiene certificados exclusivos y cada instancia del complemento vCenter Server tiene un identificador único. Los certificados y el identificador único definen la identidad del servidor de Orchestrator y del complemento vCenter Server. Si no realiza una copia de seguridad de los elementos de Orchestrator o exporta la configuración de Orchestrator con el fin de efectuar una copia de seguridad, asegúrese de cambiar estos identificadores.

Requisitos previos

Implemente y configure una nueva instancia de servidor de Orchestrator. Consulte [Configurar un servidor de Orchestrator independiente](#).

Procedimiento

- 1 Exporte la configuración de Orchestrator.
 - a Inicie sesión en el centro de control como **raíz**.
 - b Haga clic en **Exportar o importar configuración**.
 - c Seleccione los tipos de archivos que quiere exportar.
 - d (opcional) Proteja el archivo de configuración introduciendo una contraseña.
Utilice la misma contraseña cuando importe la configuración.
 - e Haga clic en **Exportar**.
- 2 Inicie sesión en la aplicación cliente de Orchestrator.
- 3 Cree un paquete que contenga todos los elementos de Orchestrator que haya creado o editado.
 - a En la vista **Administrar**, haga clic en la pestaña **Paquetes**.
 - b Haga clic en el botón de menú en la barra de título de la lista Paquetes y seleccione **Agregar paquete**.

- c Escriba un nombre para el paquete nuevo y haga clic en **Aceptar**.
La sintaxis de los nombres de paquetes es *dominio.su_compañía.carpeta.package_name*.
Por ejemplo, `com.vmware.myfolder.mypackage`.
- d Haga clic con el botón secundario en el paquete y seleccione **Editar**.
- e En la pestaña **General**, añada una descripción para el paquete.
- f En la pestaña **Flujos de trabajo**, añada flujos de trabajo al paquete.
- g (opcional) Agregue plantillas de políticas, acciones, elementos de configuración, elementos de recursos, derechos de acceso y complementos al paquete.
- h Haga clic en **Guardar y cerrar**.

4 Exporte el paquete.

- a Haga clic con el botón secundario en el paquete que quiera exportar y seleccione **Exportar paquete**.
- b Busque y seleccione la ubicación donde desee guardar el paquete.
- c (opcional) Utilice el certificado correspondiente para firmar el paquete.
- d (opcional) Imponga restricciones al paquete exportado.
- e (opcional) Para aplicar restricciones al contenido del paquete exportado, anule la selección de las opciones correspondientes.

Opción	Descripción
Exportar historial de versiones	El historial de versiones del paquete no se exportará.
Exportar los valores de la configuración	Los valores de atributos de los elementos de configuración del paquete no se exportarán.
Exportar etiquetas globales	Las etiquetas globales del paquete no se exportarán.

Nota La opción **Exportar los valores SecureString de la configuración** está desactivada de forma predeterminada. La exportación de estos valores de la configuración puede causar un problema de seguridad. Debe usarse con precaución.

- f Haga clic en **Guardar**.

5 Importe la configuración de Orchestrator que exportó anteriormente a la nueva instancia de servidor de Orchestrator.

- a Inicie sesión en Control Center de la nueva instancia de Orchestrator como **raíz**.
- b Haga clic en **Exportar/importar configuración** y vaya a la pestaña **Importar configuración**.
- c Navegue para seleccionar el archivo .zip exportado desde la instalación anterior.

- d Escriba la contraseña utilizada mientras exportaba la configuración.

Este paso no es necesario si no ha especificado una contraseña.

- e Seleccione el tipo de importación.

- f Haga clic en **Importar**.

6 Importe el paquete que ha exportado en la nueva instancia de Orchestrator.

- a Inicie sesión en la aplicación cliente de Orchestrator de la nueva instancia de Orchestrator.

- b En el menú desplegable del cliente de Orchestrator, seleccione **Administrar**.

- c Haga clic en la pestaña **Paquetes**.

- d Haga clic en el botón de menú en la barra de título de la lista Paquetes y seleccione **Importar paquete**.

- e Busque y seleccione el paquete que desea importar y haga clic en **Abrir**.

Aparece información de certificado sobre el exportador.

- f Revise los detalles de importación del paquete y seleccione **Importar** o **Importar y confiar en proveedor**.

Se abre la ventana Importar paquete. Si la versión de un elemento de paquete importado es posterior a la del servidor, el sistema selecciona el elemento para importar de forma automática.

- g Seleccione los elementos que desea importar.

Nota Anule la selección de los elementos personalizados de los que existan versiones posteriores.

- h (opcional) Anule la selección de la casilla de verificación **Importar los valores de la configuración** si no desea importar los valores de atributo de los elementos de configuración del paquete.

- i En el menú desplegable, seleccione si desea importar etiquetas desde el paquete.

Opción	Descripción
Importar etiquetas pero conservar los valores existentes	Importa las etiquetas del paquete sin sobrescribir los valores de etiqueta existentes.
Importar etiquetas y sobrescribir los valores existentes	Importa las etiquetas del paquete y sobrescribe los valores de estas.
No importar etiquetas	No importa las etiquetas del paquete.

- j Haga clic en **Importar elementos seleccionados**.

Resultados

Ha realizado una copia de seguridad de la configuración y los elementos de Orchestrator correctamente.

Copia de seguridad y restauración de vRealize Orchestrator

Puede utilizar vSphere Data Protection para realizar una copia de seguridad y restaurar una máquina virtual (MV) que contenga una instancia de vRealize Orchestrator.

vSphere Data Protection es una solución de copia de seguridad y restauración basada en disco de VMware diseñada para entornos vSphere. vSphere Data Protection se integra totalmente con vCenter Server. Con vSphere Data Protection, puede administrar las tareas de copia de seguridad y almacenamiento en las ubicaciones de almacenamiento desduplicadas. Después de implementar y configurar vSphere Data Protection, puede acceder a vSphere Data Protection utilizando la interfaz de vSphere Web Client para seleccionar, programar, configurar y administrar las copias de seguridad y restauraciones de máquinas virtuales. Durante una copia de seguridad, vSphere Data Protection crea un snapshot en modo inactivo de la máquina virtual. La desduplicación se lleva a cabo automáticamente con cada operación de copia de seguridad.

Para obtener información sobre cómo implementar y configurar vSphere Data Protection, consulte la documentación *Administración de la protección de datos de vSphere*.

Copia de seguridad de vRealize Orchestrator

Puede efectuar una copia de seguridad de la instancia de vRealize Orchestrator como máquina virtual.

Para asegurarse de realizar una copia de seguridad conjunta de todos los componentes de una máquina virtual de un solo producto, almacene las máquinas virtuales del entorno de vRealize Orchestrator en una única carpeta de vCenter Server; a continuación, cree un trabajo de política de copia de seguridad para dicha carpeta.

Requisitos previos

- Verifique que el dispositivo de vSphere Data Protection se haya implementado y configurado. Para obtener información sobre cómo implementar y configurar vSphere Data Protection, consulte la documentación de *Administración de vSphere Data Protection*.
- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.
- 2 Seleccione el dispositivo vSphere Data Protection en el menú desplegable **Dispositivo VDP**; a continuación, haga clic en **Conectar**.
- 3 En la pestaña **Introducción**, haga clic en **Crear trabajo de copia de seguridad**.

- 4 Haga clic en **Imágenes de invitados** para efectuar la copia de seguridad de la instancia de vRealize Orchestrator; a continuación, haga clic en **Siguiente**.
- 5 Seleccione **Imagen completa** para efectuar la copia de seguridad de toda la máquina virtual; a continuación, haga clic en **Siguiente**.
- 6 Expanda el árbol **Máquinas virtuales** y seleccione la casilla de verificación de la máquina virtual de vRealize Orchestrator.
- 7 Siga las indicaciones para programar la copia de seguridad, establecer la política de retención y asignar un nombre al trabajo de copia de seguridad.

Para obtener más información sobre cómo efectuar una copia de seguridad y restaurar máquinas virtuales, consulte la documentación de *Administración de vSphere Data Protection*.

El trabajo de copia de seguridad figura en la lista de trabajos de copia de seguridad en la pestaña **Copia de seguridad**.

- 8 (opcional) Abra la pestaña **Copia de seguridad** y seleccione el trabajo de copia de seguridad; a continuación, haga clic en **Realizar copia de seguridad ahora** para efectuar la copia de seguridad de vRealize Orchestrator.

Nota También es posible esperar a que la copia de seguridad se inicie de manera automática conforme a lo que se haya programado.

El proceso de la copia de seguridad aparece en la página **Tareas recientes**.

Resultados

La imagen de la máquina virtual figura en la lista de copias de seguridad en la pestaña **Restaurar**.

Pasos siguientes

Abra la pestaña **Restaurar** y compruebe que la imagen de la máquina virtual figure en la lista de copias de seguridad.

Restaurar una instancia de a vRealize Orchestrator

Puede restaurar una instancia de vRealize Orchestrator en su ubicación original o en otra del mismo vCenter Server.

Requisitos previos

- Verifique que el dispositivo de vSphere Data Protection se haya implementado y configurado. Para obtener información sobre cómo implementar y configurar vSphere Data Protection, consulte la documentación de *Administración de vSphere Data Protection*.
- Cree una copia de seguridad de la instancia de vRealize Orchestrator. Consulte [Copia de seguridad de vRealize Orchestrator](#).

- Utilice vSphere Web Client para iniciar sesión en la instancia de vCenter Server que administra el entorno. Inicie sesión como el usuario con privilegios de administrador que se utilizó durante la configuración de vSphere Data Protection.

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **vSphere Data Protection**.
- 2 Seleccione el dispositivo de vSphere Data Protection en el menú desplegable **Dispositivo VDP**; a continuación, haga clic en **Conectar**.
- 3 Abra la pestaña **Restaurar**.
- 4 En la lista de tareas de copia de seguridad, seleccione la copia de seguridad de vRealize Orchestrator que desee restaurar.

Nota Si tiene varias máquinas virtuales, debe restaurarlas de forma simultánea para que estén sincronizadas.

- 5 Para restaurar su instancia de vRealize Orchestrator en el mismo vCenter Server, haga clic en el icono **Restore**; a continuación, siga las instrucciones para establecer la ubicación en el vCenter Server en el que va a restaurar vRealize Orchestrator.

No seleccione **Encender**, ya que el dispositivo debe ser el último componente que se encienda. Para obtener información sobre cómo efectuar una copia de seguridad y restaurar una máquina virtual, consulte la documentación de *Administración de vSphere Data Protection*.

Aparece un mensaje que indica que la restauración se ha iniciado correctamente.

- 6 (opcional) Encienda los hosts de base de datos si son externos y restaure la configuración del equilibrador de carga.
- 7 Encienda vRealize Orchestrator Appliance.

Resultados

La máquina virtual de vRealize Orchestrator aparece en el inventario de vCenter Server.

Pasos siguientes

Compruebe que vRealize Orchestrator se haya configurado correctamente en la página **Validar configuración** del centro de control.

Recuperación ante desastres de 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.

- Verifique que vSphere 5.5 esté instalado en los sitios protegidos y de recuperación.
- Compruebe que está utilizando Site Recovery Manager 5.8.
- 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.

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
- Ha configurado vSphere Replication en las máquinas virtuales
- Ha realizado una combinación de las acciones anteriores o todas ellas

Procedimiento

- 1 En vSphere Web Client, seleccione **Site Recovery > Grupos de protección**.
- 2 En la pestaña **Objetos**, haga clic en el icono para crear un grupo de protección.
- 3 En la página de tipos de grupos de protección, seleccione el sitio protegido, el tipo de replicación y haga clic en **Siguiente**.

Opción	Acción
Grupos de replicación basada en matrices	Seleccione Replicación basada en matrices y seleccione un par de matrices.
Grupo de protección de vSphere Replication	Seleccione vSphere Replication .

- 4 Seleccione máquinas virtuales o grupos de almacenes de datos para añadir 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 .
Grupos de protección de vSphere Replication	Seleccione las máquinas virtuales en la lista y haga clic en Siguiente .

Cuando crea grupos de protección de vSphere Replication, solo aparecen en la lista las máquinas virtuales que ha configurado para vSphere Replication y que todavía no están en un grupo de protección.

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

Puede supervisar el progreso de creación del grupo de protección en la pestaña **Objetos** bajo **Grupos de protección**.

Resultados

- 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.

- 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.

Crear un plan de recuperación

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

Procedimiento

- 1 En vSphere Web Client, seleccione **Site Recovery** > **Planes de recuperación**.
- 2 En la pestaña **Objetos**, haga clic en el icono para crear un plan de recuperación.
- 3 Especifique un nombre y una descripción para el plan, seleccione una carpeta y haga clic en **Siguiente**.
- 4 Seleccione un sitio de recuperación y haga clic en **Siguiente**.
- 5 Seleccione el tipo de grupo en el menú.

Opción	Descripción
Grupos de protección de VM	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	Seleccione esta opción para crear un plan de recuperación que contenga grupos de protección de políticas de almacenamiento.

El valor predeterminado es **Grupos de protección de VM**.

Nota Si se utiliza el almacenamiento ampliado, seleccione **Grupos de protección de políticas de almacenamiento** para el tipo de grupo.

- 6 Seleccione uno o varios grupos de protección para la recuperación del plan y haga clic en **Siguiente**.
- 7 Haga clic en el valor **Red de prueba**, seleccione una red para utilizar durante la recuperación de prueba y haga clic en **Siguiente**.

La opción predeterminada es crear una red aislada automáticamente.

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

Organización de planes de recuperación en carpetas

Puede crear carpetas en las que organizar planes de recuperación.

Organizar los planes de recuperación en carpetas es resulta útil si tiene muchos planes de recuperación. Puede limitar el acceso a planes de recuperación colocándolos en carpetas, y asignando diferentes permisos de acceso a las carpetas para diferentes usuarios o grupos.

Procedimiento

- 1 En la vista Inicio de vSphere Web Client, haga clic en **Site Recovery**.
- 2 Expanda **Árboles de inventario** y haga clic en **Planes de recuperación**.
- 3 Seleccione la pestaña **Objetos relacionados** y haga clic en **Carpetas**.
- 4 Haga clic en el icono **Crear carpeta**, asigne un nombre a la carpeta que se va a crear y haga clic en **Aceptar**.
- 5 Añada planes de recuperación nuevos o ya creados a la carpeta.

Opción	Descripción
Crear nuevo plan de recuperación	Haga clic con el botón derecho en la carpeta y seleccione Crear plan de recuperación .
Añadir un plan de recuperación ya creado	Arrastre y coloque planes de recuperación del árbol de inventario en la carpeta.

- 6 (opcional) Para cambiar el nombre de una carpeta o eliminarla, haga clic con el botón derecho en la carpeta; a continuación, seleccione **Cambiar nombre de carpeta** o **Eliminar carpeta**, respectivamente.

Las carpetas solo se pueden eliminar si están vacías.

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 Web Client, seleccione **Site Recovery > Planes de recuperación**.
- 2 Haga clic con el botón secundario en un plan de recuperación y seleccione **Editar plan**.
También puede editar un plan de recuperación haciendo clic en el icono **Editar plan de recuperación** de la vista **Pasos de recuperación** en la pestaña **Supervisar**.
- 3 (opcional) Cambie el nombre o la descripción del plan en el cuadro de texto **Nombre del plan de recuperación** y haga clic en **Siguiente**.
- 4 En la página Sitio de recuperación, haga clic en **Siguiente**.
No se puede cambiar el sitio 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) Haga clic en la red de prueba para seleccionar otra red de prueba en el sitio de recuperación; 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:

- [Desactivación del acceso al cliente de Orchestrator por parte de usuarios que no son administradores](#)
- [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](#)
- [Establecimiento de la propiedad de tiempo de espera personalizado](#)

Desactivación del acceso al cliente de Orchestrator por parte de usuarios que no son administradores


Puede configurar el servidor de Orchestrator para que deniegue el acceso al cliente de Orchestrator a todos los usuarios que no sean miembros del grupo de administradores de Orchestrator.

De forma predeterminada, todos los usuarios que tienen permisos de ejecución pueden conectarse al cliente de Orchestrator. Sin embargo, puede limitar el acceso al cliente de Orchestrator a los administradores de Orchestrator estableciendo una propiedad del sistema de configuración de Orchestrator.

Importante Si la propiedad no se configura o se establece en false, Orchestrator permite el acceso a todos los usuarios al cliente de Orchestrator.

Procedimiento

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

- 3 Haga clic en el icono **Añadir** (.
- 4 En el cuadro de texto **Clave**, escriba `com.vmware.o11n.smart-client-disabled`.
- 5 En el cuadro de texto **Valor**, escriba `true`.
- 6 (opcional) En el cuadro de texto **Descripción**, escriba `Disable Orchestrator client connection`.
- 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

Ha desactivado el acceso al cliente de Orchestrator de todos los usuarios que no sean miembros del grupo de administradores de Orchestrator.

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

En 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 de Orchestrator `js-io-rights.conf`.

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

Importante Antes de modificar el archivo `js-io-rights.conf`, debe detener el servicio del centro de control de vRealize Orchestrator. De lo contrario, el archivo `js-io-rights.conf` se revertirá a la configuración predeterminada. Consulte [Establecer el acceso al sistema de archivos del servidor para flujos de trabajo y acciones](#).

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

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
-rwx /etc/vco/app-server/security/
+rx /etc/vco
+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

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 consola de Linux de vRealize Orchestrator Appliance como usuario **raíz**.
- 2 Detenga el servicio del centro de control de vRealize Orchestrator.

```
service vco-configurator stop
```

- 3 Vaya a `/etc/vco/app-server`.
- 4 Abra el archivo de configuración `js-io-rights.conf` en un editor de texto.

- 5 Agregue las líneas necesarias al archivo `js-io-rights.conf`.

Por ejemplo, la línea siguiente deniega los derechos de ejecución en el directorio `/ruta_a_carpeta/noexec`:

```
-x /ruta_a_carpeta/noexec
```

`/ruta_a_carpeta/noexec` retiene derechos de ejecución, pero no es el caso de `/ruta_a_carpeta/noexec/bar`. Se puede seguir leyendo y escribiendo en los dos directorios.

- 6 Para aplicar los cambios, ejecute el mandato siguiente.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh sync-local
```

- 7 Inicie el servicio del centro de control de vRealize Orchestrator.

```
service vco-configurator start
```

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

Concede permiso para utilizar la clase `Command` estableciendo una propiedad del sistema de configuración de Orchestrator.

Procedimiento

- 1 Inicie sesión en el centro de control como **raíz**.
- 2 Haga clic en **Propiedades del sistema**.
- 3 Haga clic en el icono **Añadir** ()
- 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**.

- Haga clic en **Guardar cambios** en el menú emergente.

Aparecerá un mensaje que indica que se ha guardado correctamente.

- Reinicie el servidor de Orchestrator.

Resultados

Ha otorgado permisos a aplicaciones de Orchestrator para ejecutar comandos locales en el sistema operativo que aloja al servidor de 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

De forma predeterminada, Orchestrator restringe 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 Orchestrator para permitir este acceso.

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 Orchestrator. En consecuencia, de forma predeterminada, el motor de JavaScript de Orchestrator solo puede acceder 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 Guarde el archivo de configuración con el nombre correspondiente y en el lugar adecuado.
- 3 Inicie sesión en el centro de control como **raíz**.
- 4 Haga clic en **Propiedades del sistema**.

- 5 Haga clic en el icono **Añadir** ().
- 6 En el cuadro de texto **Clave** escriba `com.vmware.scripting.rhino-class-shutter-file`.
- 7 En el cuadro de texto **Valor**, escriba la ruta del archivo de configuración.
- 8 Escriba una descripción para la propiedad del sistema en el cuadro de texto **Descripción**.
- 9 Haga clic en **Agregar**.
- 10 Haga clic en **Guardar cambios** en el menú emergente.
Aparecerá un mensaje que indica que se ha guardado correctamente.
- 11 Reinicie el servidor de Orchestrator.

Resultados

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


Establecimiento de la propiedad de tiempo de espera personalizado

Cuando vCenter Server está sobrecargado, devolver la respuesta al servidor de Orchestrator tarda más tiempo que los 20.000 milisegundos establecidos de forma predeterminada. A fin de evitar esta situación, debe modificar el archivo de configuración de Orchestrator para que incremente el periodo de tiempo de espera predeterminado.

Si el periodo de tiempo de espera predeterminado caduca antes de la conclusión de determinadas operaciones, el registro del servidor de 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 el icono **Añadir** ().
- 4 En el cuadro de texto **Clave**, escriba `com.vmware.vmo.plugin.vi4.waitUpdatesTimeout`.
- 5 En el cuadro de texto **Valor**, indique el nuevo periodo 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 **Añadir**.
- 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 milisegundos.

Procedimiento a partir de aquí

10

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

- Inicie sesión en el cliente de Orchestrator; a continuación, ejecute y programe flujos de trabajo en los objetos de inventario de vCenter Server u otros objetos a los que acceda Orchestrator mediante sus complementos. Consulte *Uso del cliente de VMware vRealize Orchestrator*.
- Duplique y modifique los flujos de trabajo estándar de Orchestrator; escriba sus propios flujos de trabajo y acciones para automatizar operaciones en vCenter Server.
- Desarrolle complementos y servicios web para ampliar la plataforma Orchestrator.
- Ejecute flujos de trabajo en los objetos de inventario de vSphere mediante vSphere Web Client.

Este capítulo incluye los siguientes temas:

- [Iniciar sesión en el cliente heredado de Orchestrator desde la consola web de Orchestrator Appliance](#)

Iniciar sesión en el cliente heredado de Orchestrator desde la consola web de Orchestrator Appliance

Para realizar tareas generales de administración o editar y crear flujos de trabajo, debe iniciar sesión en la interfaz del cliente heredado de Orchestrator.

La interfaz del cliente heredado de Orchestrator está pensada para desarrolladores con derechos administrativos que quieren desarrollar flujos de trabajo, acciones y otros elementos personalizados.

Importante Asegúrese de que los relojes de Orchestrator Appliance y de la máquina del cliente heredado de Orchestrator están sincronizados.

Requisitos previos

- Descargue e implemente Orchestrator Appliance.
- Compruebe que el dispositivo esté listo y en ejecución.
- Instale Java de 64 bits en la estación de trabajo en la que ejecutará el cliente heredado de Orchestrator.

Nota No se admite Java de 32 bits.

Procedimiento

- 1 En un navegador web, vaya a la dirección IP de su máquina virtual de Orchestrator Appliance.
`http://orchestrator_appliance_ip`

- 2 Haga clic en **Iniciar cliente de Orchestrator**.

- 3 Introduzca la dirección IP o el nombre de dominio de Orchestrator Appliance en el cuadro de texto **Nombre de host**.

La dirección IP de Orchestrator Appliance se muestra de forma predeterminada.

- 4 Inicie sesión utilizando el nombre de usuario y la contraseña del cliente heredado de Orchestrator.

Dependiendo de si utiliza vRealize Automation o vSphere como proveedor de autenticación, introduzca las credenciales respectivas para conectarse al cliente heredado de Orchestrator.

Si el multi-tenancy está habilitado en su entorno de Orchestrator, escriba el nombre de usuario, la contraseña y el ID de tenant del administrador de tenants o el administrador del sistema.

- 5 En la ventana **Advertencia de seguridad**, seleccione una opción para controlar la advertencia de certificado.

El cliente heredado de Orchestrator se comunica con el servidor de Orchestrator mediante un certificado SSL. Una entidad de certificación de confianza no firma el certificado durante la instalación. Aparecerá una advertencia de certificado cada vez que se conecte al servidor de Orchestrator.

Opción	Descripción
Omitir	Se sigue utilizando el certificado SSL actual. El mensaje de advertencia volverá a aparecer cuando se reconecte al mismo servidor de Orchestrator o cuando trate de sincronizar un flujo de trabajo con un servidor de Orchestrator remoto.
Cancelar	La ventana se cierra y el proceso de inicio de sesión se detiene.
Instalar este certificado y no mostrar más advertencias de seguridad.	Active esta casilla y haga clic en Omitir para instalar el certificado y dejar de recibir advertencias de seguridad.

El certificado SSL predeterminado se puede cambiar por un certificado firmado por una entidad de certificación. Para obtener más información sobre cómo cambiar certificados SSL, consulte *Instalación y configuración de VMware vRealize Orchestrator*.

Pasos siguientes

Puede importar un paquete, desarrollar flujos de trabajo o establecer derechos de acceso raíz en el sistema.