Instalación y configuración de VMware vRealize Orchestrator

vRealize Orchestrator 7.2

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

ES-002396-01

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Contenido

Instalación 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.

Información actualizada

Esta *instalación y configuración de VMware vRealize Orchestrator* se actualiza con cada versión del producto o cuando sea necesario.

Esta tabla proporciona el historial de actualizaciones de la *instalación y configuración de VMware vRealize Orchestrator*.

Revisión	Descripción
ES-002396-01	■ Se ha actualizado "Migrar un vRealize Orchestrator 6.x externo en Windows a vRealize Automation 7.2," página 72. ■ Se ha actualizado "Migrar un dispositivo virtual vRealize Orchestrator 6.x externo a vRealize Automation 7.2," página 74. ■ Se ha actualizado "Migrar un vRealize Orchestrator 7.x externo a vRealize Automation 7.2," página 76. ■ Se ha actualizado Capítulo 9, "Configure el servidor integrado de vRealize Orchestrator," página 79. ■ Se ha actualizado la guía Equilibrio de carga de vRealize Orchestrator.
ES-002396-00	Versión inicial.

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 cubre los siguientes temas:

Funciones clave de la plataforma de Orchestrator

Orchestrator se compone de tres capas: una plataforma de orquestación que proporciona las funciones 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.

La lista siguiente presenta las funciones clave de Orchestrator.

Persistencia Las bases de datos de grado de producción se utilizan para guardar información relevante, como procesos, estados de flujos de trabajo y configuraciones.

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

La interfaz del centro de control 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 vRealize Orchestrator se optimiza con un archivo de registro adicional que recopila distintas métricas del rendimiento para el motor de vRealize 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 la tecnología conectada. Las políticas pueden añadir eventos desde la plataforma o cualquiera de los complementos, lo que permite administrar los cambios de condiciones en cualquiera de las tecnologías integradas.

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.

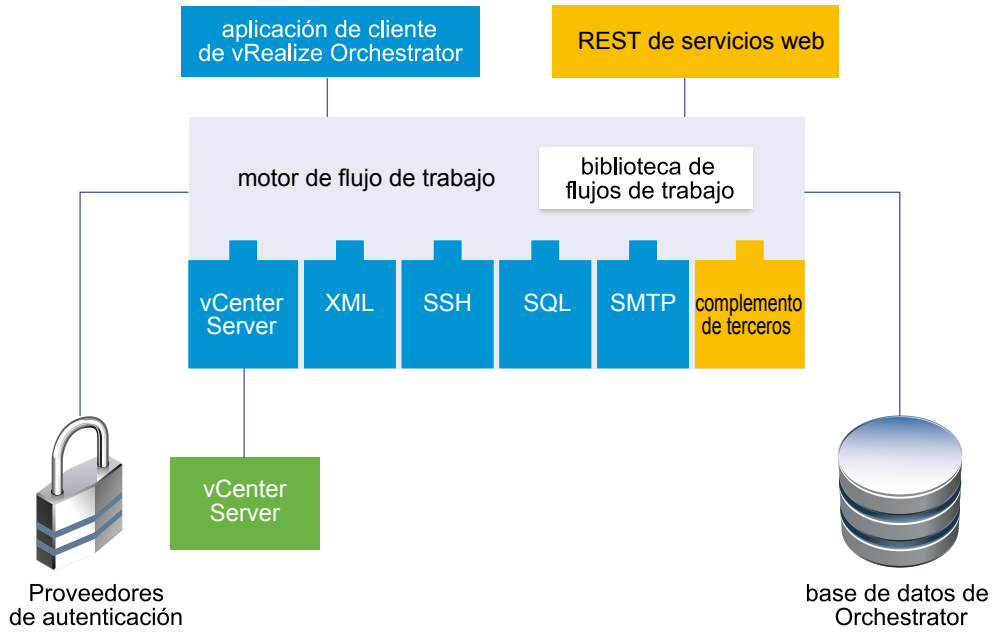
Arquitectura de Orchestrator

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, para permitirle orquestar tareas en los entornos diferentes que exponen los complementos.

Asimismo, Orchestrator presenta una arquitectura abierta para permitirle conectar aplicaciones externas de otros proveedores 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, los flujos de trabajo de Orchestrator y los objetos que expone desde la interfaz del cliente de Orchestrator o bien desde servicios web.

Figura 1-1. Arquitectura de VMware vRealize Orchestrator



Complementos de Orchestrator

Los complementos permiten usar Orchestrator para acceder a tecnologías y aplicaciones externas, y para controlarlas. El uso de una tecnología externa en un complemento de Orchestrator le permite incorporar objetos y funciones en flujos de trabajo que tienen acceso a los objetos y las funciones de la tecnología externa.

Las tecnologías externas a las que se accede a través de los complementos pueden ser 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 estándar para incorporar en flujos de trabajo dichas tecnologías, como la API de VMware vCenter Server y funciones de correo electrónico. El uso de los complementos le permite automatizar la prestación de nuevos servicios de TI, o bien adaptar las funciones de los servicios de aplicaciones e infraestructuras 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 desarrollados y distribuidos por VMware se facilitan como archivos `.vmoapp`. Para obtener más información acerca de los complementos de Orchestrator que implementa y distribuye VMware, consulte http://www.vmware.com/support/pubs/vco_plugins_pubs.html. Para obtener más información acerca de los complementos de Orchestrator de terceros, consulte https://solutionexchange.vmware.com/store/vco.

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 cubre los siguientes temas:

Requisitos de hardware para Orchestrator Appliance

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

Orchestrator Appliance tiene la siguiente configuración de hardware:

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

No reduzca el tamaño de memoria predeterminado, ya que el servidor de Orchestrator requiere como mínimo 2 GB de memoria libre.

Servicios de directorio compatibles

Si tiene previsto utilizar un servidor LDAP para autenticación, asegúrese de instalar y configurar un servidor LDAP válido.

NOTA: La autenticación LDAP está en desuso y no se admitirá en futuras versiones.

Orchestrator admite los tipos de servicios de directorio siguientes.

- Windows Server Active Directory

- OpenLDAP

IMPORTANTE: Varios dominios que no estén en el mismo árbol y tengan una confianza bidireccional son incompatibles y no funcionan con Orchestrator. El árbol de dominios es la única configuración compatible con Active Directory de varios dominios. La confianza externa y de bosque son incompatibles.

Navegadores compatibles con Orchestrator

El centro de control requiere un navegador web.

Utilice uno de los navegadores siguientes para conectarse al centro de control.

- Microsoft Internet Explorer 10 o posterior
- Mozilla Firefox
- Google Chrome

Requisitos de la base de datos de Orchestrator

El servidor de Orchestrator requiere una base de datos. La base de datos preconfigurada en Orchestrator PostgreSQL está lista para la producción. También puede utilizar una base de datos externa, en función del entorno.

Para obtener una lista de las versiones compatibles de base de datos, consulte Matriz de interoperabilidad de productos de VMware.

Software incluido en Orchestrator Appliance

Orchestrator Appliance es una máquina virtual preconfigurada que se ha optimizado para ejecutar Orchestrator. El dispositivo se distribuye con software preinstalado.

El paquete de Orchestrator Appliance contiene el software siguiente:

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

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

La configuración de LDAP en curso predeterminada solo es adecuada para experimentación y para pruebas. Para utilizar Orchestrator Appliance en un entorno de producción, debe configurar un nuevo directorio de servicios, además de configurar el servidor de Orchestrator para que trabaje con él. También puede configurar el servidor de Orchestrator para autenticar mediante vRealize Automation, vSphere o vCenter Single Sign-On. Para obtener más información sobre la configuración externa de LDAP o Single Sign-On, consulte “Seleccionar el tipo de autenticación,” página 34.

Para obtener más información sobre la configuración de una base de datos para entornos de producción, consulte “Configurar la base de datos de Orchestrator,” página 22.

NOTA: La autenticación LDAP está en desuso y no se admitirá en futuras versiones.

Requisitos de las contraseñas

Cuando configure la contraseña raíz de Orchestrator Appliance, debe cumplir los requisitos predefinidos de las contraseñas.

La contraseña raíz que define al implementar Orchestrator Appliance de una plantilla OVF debe contener un mínimo de ocho caracteres.

Si se cambia una contraseña de usuario local desde el centro de control, la contraseña nueva no se acepta a menos que cumpla todos los requisitos.

- La contraseña debe tener como mínimo ocho caracteres de longitud.
- La contraseña debe tener al menos un número.
- La contraseña debe tener al menos una letra en mayúscula.
- La contraseña debe tener al menos una letra en minúscula.
- La contraseña debe tener al menos un carácter especial.

NOTA: Los caracteres no ASCII o ASCII extendido no se admiten. Tales caracteres podrían ser válidos al definir la contraseña; sin embargo, generan errores durante las operaciones de guardar y unir un nodo de Orchestrator a un clúster.

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	-	-

Compatibilidad con caracteres no ASCII para bases de datos de Oracle

Para almacenar caracteres en el formato correcto en una base de datos de Oracle, establezca el parámetro `NLS_CHARACTER_SET` en `AL32UTF8` antes de configurar la conexión de la base de datos y de crear una estructura de tabla para Orchestrator. Esta configuración es fundamental para un entorno internacionalizado.

Configurar componentes de Orchestrator 3

Cuando descarga e implementa Orchestrator Appliance, el servidor de 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 Orchestrator:

- Instale y configure una base de datos, y configure Orchestrator para que conecte con ella.
- Instale y configure un proveedor de autenticación, y configure Orchestrator para que funcione con él.

Este capítulo cubre los siguientes temas:

Configuración de vCenter Server

Si se incrementa el número de instancias de vCenter en la configuración de Orchestrator, dicha plataforma debe administrar más sesiones. Cada sesión activa se traduce en actividad en la instancia correspondiente de vCenter Server; asimismo, demasiadas sesiones activas pueden hacer que Orchestrator tenga tiempos de espera cuando 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 dispone de latencia y ancho de banda suficientes. Si utiliza una LAN para mejorar las comunicaciones entre Orchestrator y vCenter Server, es imprescindible una línea de 100 Mb.

Métodos de autenticación

Para autenticar y administrar los permisos del usuario, Orchestrator requiere una conexión a un servidor LDAP, una conexión a un servidor Single Sign-On o una conexión a vRealize Automation.

NOTA: La autenticación LDAP está en desuso y no se admitirá en futuras versiones.

Cuando descarga e implementa Orchestrator Appliance, el servidor de Orchestrator se configura previamente para funcionar con el servidor LDAP de ApacheDS en curso distribuido con el dispositivo. La configuración de LDAP en curso predeterminada solo es adecuada para fines de pruebas. Para utilizar Orchestrator en un entorno de producción, debe configurar un servidor LDAP, un servidor vCenter Single Sign-On o una conexión con vRealize Automation y configurar Orchestrator para que funcione con ellos.

Conéctese al servidor LDAP que esté físicamente más cerca del servidor de Orchestrator para evitar tiempos de respuesta más prolongados para las consultas LDAP que ralentizan el rendimiento del sistema. Orchestrator admite los tipos de servicio Active Directory y OpenLDAP.

Para mejorar el rendimiento de las consultas LDAP, mantenga la base de búsqueda de grupos y usuarios al mínimo. Limite los usuarios a los grupos de destino que necesitan acceso, en lugar de incluir organizaciones enteras con muchos usuarios que no necesitan acceso. Los recursos que necesita dependen de la combinación de la base de datos y el servicio de directorio que elija. Para obtener recomendaciones, consulte la documentación del servidor LDAP.

Para utilizar el método de autenticación de vCenter Single Sign-On, primero debe instalar vCenter Single Sign-On. Debe configurar el servidor de Orchestrator para que utilice el servidor vCenter Single Sign-On que ha instalado y configurado.

Puede utilizar la autenticación de Single Sign-On a través de vRealize Automation y vSphere desde la configuración de autenticación del centro de control.

Configurar la base de datos de Orchestrator

Orchestrator necesita una base de datos para almacenar flujos de trabajo y acciones.

Cuando descarga e implementa Orchestrator Appliance, el servidor de Orchestrator se preconfigura para funcionar con la base de datos PostgreSQL preinstalada en el dispositivo. La configuración de la base de datos predeterminada de Orchestrator Appliance está lista para la producción. Ahora bien, para utilizar Orchestrator en un entorno de producción de alta carga, debe una configurar una base de datos aparte y configurar Orchestrator para que trabaje con ella desde el centro de control.

El servidor de Orchestrator es compatible con bases de datos de Oracle, Microsoft SQL Server y PostgreSQL.

El flujo de trabajo habitual para configurar la base de datos de Orchestrator tiene los pasos siguientes:

1 Cree una base de datos. Para obtener más información sobre cómo crear una base de datos, consulte la documentación del proveedor.

2 Habilite la conexión remota para la base de datos.

3 Configure los parámetros de conexión de la base de datos. Para obtener más información, consulte "Configurar la conexión de la base de datos de Orchestrator," página 41.

Si tiene previsto configurar un clúster de Orchestrator, debe configurar la base de datos para que acepte varias conexiones de las diferentes instancias de servidor de Orchestrator en el clúster.

La configuración de la base de datos puede afectar al rendimiento de Orchestrator. Instale la base de datos en un equipo en el que no esté instalado el servidor de Orchestrator. De este modo, se asegura de que la máquina virtual de Java y el servidor de la base de datos no compartan CPU, RAM y E/S.

La ubicación de la base de datos es importante, ya que prácticamente cada actividad del servidor de Orchestrator activa operaciones en la base de datos. Para evitar la latencia en la conexión de la base de datos, conecte al servidor de la base de datos geográficamente más próximo al servidor de Orchestrator y que esté en la red con el ancho de banda más grande.

El tamaño de la base de datos de Orchestrator varía según la configuración y la administración de los tokens de flujo de trabajo. Asigne alrededor de 50 KB para cada objeto de vCenter Server y 4 KB para la ejecución de cada flujo de trabajo.

ADVERTENCIA: Verifique que al menos disponga de 1 GB de espacio en el disco del equipo en el que se instala la base de datos de Orchestrator.

Si el disco duro no dispone de espacio suficiente, el servidor y el cliente de Orchestrator podrían funcionar de forma incorrecta.

Instalación y actualización de Orchestrator 4

Orchestrator cuenta con un componente de servidor y un componente de cliente.

El cliente instalable de Orchestrator puede ejecutarse en máquinas de 64 bits con Windows, Linux y Mac.

Para utilizar Orchestrator, debe iniciar sel servicio del servidor de Orchestrator y luego iniciar el cliente de Orchestrator.

Puede cambiar la configuración predeterminada de Orchestrator utilizando el centro de control de Orchestrator.

Este capítulo cubre los siguientes temas:

Descargar e implementar Orchestrator Appliance

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

Prerequisitos

- Compruebe que vCenter Server esté instalado y en ejecución.
- Verifique que el host en que se implementa el dispositivo cumpla los requisitos de hardware mínimos. Para obtener más información, consulte "Requisitos de hardware para Orchestrator Appliance," página 17.
- 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 Revise los detalles de la plantilla OVF y haga clic en **Siguiente**.

6 Acepte los términos del contrato de licencia y haga clic en **Siguiente**.

7 Introduzca un nombre y una ubicación para el dispositivo implementado, y haga clic en **Siguiente**.

8 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**.

9 Seleccione un formato en el que guardar el disco virtual y el almacenamiento del dispositivo.

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 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`.

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

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

12 Revise la página Listo para completar y haga clic en **Finalizar**.

Orchestrator Appliance se habrá implementado correctamente.

Encendido de Orchestrator Appliance y apertura de la página Inicio

Para utilizar Orchestrator Appliance, primero lo debe encender 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 derecho en Orchestrator Appliance y seleccione **Conectar > Encender**.

3 En la pestaña **Resumen**, observe la dirección IP de Orchestrator Appliance.

4 En un navegador web, vaya a la dirección IP de su máquina virtual de Orchestrator Appliance.

http://*orchestrator_appliance_ip*

Cambio de la contraseña raíz

Por motivos de seguridad, puede cambiar la contraseña raíz de Orchestrator Appliance.

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 el comando `passwd –x 99999 root`.

Prerequisitos

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

Procedimiento

1 En un navegador web, vaya a https://*orchestrator_appliance_ip*:5480.

2 Escriba el nombre de usuario y la contraseña del dispositivo.

3 Haga clic en la pestaña **Administración**.

4 En el cuadro de texto **Contraseña actual del administrador**, escriba la contraseña raíz actual.

5 Escriba la nueva contraseña en los cuadros de texto **Nueva contraseña del administrador** y **Vuelva a escribir la nueva contraseña del administrador**.

6 Haga clic en **Cambiar contraseña**.

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

Activación o desactivación del inicio de sesión de administrador SSH en el dispositivo vRealize Orchestrator

Puede activar o desactivar la posibilidad de iniciar sesión como raíz en Orchestrator Appliance utilizando SSH.

Prerequisitos

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

Procedimiento

1 En un navegador web, vaya a https://*orchestrator_appliance_ip*:5480.

2 Inicie sesión como raíz.

3 En la pestaña **Administración**, seleccione **Servicio SSH habilitado** para activar el servicio SSH de Orchestrator.

4 (Opcional) Haga clic en **Inicio de sesión SSH de administrador habilitado** para poder iniciar sesión como raíz en Orchestrator Appliance utilizando SSH.

5 Haga clic en **Guardar configuración**.

Estado de SSH aparece como *En ejecución*.

Configuración de red para Orchestrator Appliance

Configure las opciones de red de Orchestrator Appliance para asignar una dirección IP estática y definir la configuración del proxy.

Prerequisitos

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

Procedimiento

1 En un navegador web, vaya a https://*orchestrator_appliance_ip*:5480.

2 Inicie sesión como raíz.

3 En la pestaña **Red**, haga clic en **Dirección**.

4 Seleccione el método que utiliza el dispositivo para obtener la configuración de la dirección IP.

Opción	Descripción
DHCP	Obtiene la configuración IP de un servidor DHCP. Es la configuración predeterminada.
Estático	Utiliza la configuración de IP estática. Escriba la dirección IP, la máscara de red y la puerta de enlace.

En función de la configuración de red, puede que tenga que seleccionar los tipos de dirección IPv4 e IPv6.

5 (Opcional) Escriba la información de configuración de red necesaria.

6 Haga clic en **Guardar configuración**.

7 (Opcional) Establezca la configuración del proxy y haga clic en **Guardar configuración**.

Actualizar Orchestrator Appliance 5.5.x y versiones posteriores a 7.x

vRealize Orchestrator 7.2 admite la actualización in situ de las versiones 5.5.x, 6.0.x, 7.0 y 7.1.

Puede actualizar su versión de Orchestrator Appliance a través de la interfaz de administración de dispositivos virtuales (VAMI).

Actualizar Orchestrator Appliance mediante el repositorio predeterminado de VMware

Puede configurar Orchestrator para que descargue el paquete de actualización desde el repositorio predeterminado de VMWare.

Prerequisitos

- Desmonte todos los sistemas de archivos de red. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente la memoria de Orchestrator Appliance hasta por lo menos 6 GB. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Tome una snapshot de la máquina virtual de Orchestrator. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Si utiliza una base de datos externa, cree una copia de seguridad de la misma.

- Si utiliza la base de datos preconfigurada en Orchestrator PostgreSQL, cree una copia de seguridad de la base de datos desde el menú **Exportar base de datos** del Centro de control.

Procedimiento

1 Acceda a la Interfaz de administración de dispositivos virtuales (VAMI) en https://*servidor_orchestrator*:5480 e inicie sesión como **`raíz`**.

2 En la pestaña **Actualizar**, haga clic en **Configuración**.

Se selecciona el botón de opción junto a **Usar repositorio predeterminado**.

3 En la página **Estado**, haga clic en **Buscar actualizaciones**.

4 Si hay actualizaciones disponibles, haga clic en **Instalar actualizaciones**.

5 Acepte el contrato de licencia del usuario final de VMware y confirme que desea instalar la actualización.

6 Para completar la actualización, reinicie Orchestrator Appliance.

a Inicie sesión de nuevo en la Interfaz de administración de dispositivos virtuales (VAMI) como **`raíz`**.

7 (Opcional) En la pestaña **Actualizar**, compruebe que se haya instalado correctamente la última versión del Orchestrator Appliance.

Ha actualizado correctamente Orchestrator Appliance.

Qué hacer a continuación

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

Actualizar Orchestrator Appliance con una imagen ISO

Puede configurar Orchestrator para que descargue el paquete de actualización desde un archivo de imagen ISO montado en la unidad de CD-ROM del dispositivo.

Prerequisitos

- Desmonte todos los sistemas de archivos de red. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente la memoria de Orchestrator Appliance hasta por lo menos 6 GB. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Tome una snapshot de la máquina virtual de Orchestrator. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Si utiliza una base de datos externa, cree una copia de seguridad de la misma.
- Si utiliza la base de datos preconfigurada en Orchestrator PostgreSQL, cree una copia de seguridad de la base de datos desde el menú **Exportar base de datos** del Centro de control.

Procedimiento

1 Descargue el archivo .iso de repositorio de actualizaciones de `VMware vRealize Orchestrator Appliance` *`versión`* del sitio oficial de descargas de VMware.

2 Conecte la unidad de CD-ROM de la máquina virtual de Orchestrator Appliance. Para obtener más información, consulte la documentación de *Administración de máquinas virtuales de vSphere*.

3 Monte el archivo de imagen ISO en la unidad de CD-ROM del dispositivo. Para obtener más información, consulte la documentación de *Administración de máquinas virtuales de vSphere*.

4 Acceda a la Interfaz de administración de dispositivos virtuales (VAMI) en https://*servidor_orchestrator*:5480 e inicie sesión como **raíz**.

5 En la pestaña **Actualizar**, haga clic en **Configuración**.

6 Seleccione el botón de opción junto a **Usar actualizaciones de CD-ROM**.

7 Vuelva a la página **Estado**.

Se mostrará la versión de la actualización disponible.

8 Haga clic en **Instalar actualizaciones**.

9 Acepte el contrato de licencia del usuario final de VMware y confirme que desea instalar la actualización.

10 Para completar la actualización, reinicie Orchestrator Appliance.

a Inicie sesión de nuevo en la Interfaz de administración de dispositivos virtuales (VAMI) como **raíz**.

11 (Opcional) En la pestaña **Actualizar**, compruebe que se haya instalado correctamente la última versión del Orchestrator Appliance.

Ha actualizado correctamente Orchestrator Appliance.

Qué hacer a continuación

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

Actualizar Orchestrator Appliance con un repositorio específico

Puede configurar Orchestrator para que utilice un repositorio local, en el que ha cargado el archivo de actualización.

Prerequisitos

- Desmonte todos los sistemas de archivos de red. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Aumente la memoria de Orchestrator Appliance hasta por lo menos 6 GB. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Tome una snapshot de la máquina virtual de Orchestrator. Para obtener más información, consulte la documentación correspondiente a la *administración de máquinas virtuales de vSphere*.
- Si utiliza una base de datos externa, cree una copia de seguridad de la misma.
- Si utiliza la base de datos preconfigurada en Orchestrator PostgreSQL, cree una copia de seguridad de la base de datos desde el menú **Exportar base de datos** del Centro de control.

Procedimiento

1 Prepare el repositorio local para las actualizaciones.

a Instale y configure un servidor web local.

b Descargue `VMware-vRO-Appliance-`*`versión-número_compilación`*`-updaterepo.zip` del sitio oficial de descargas de VMware.

c Extraiga el archivo `.ZIP` en el repositorio local.

2 Acceda a la Interfaz de administración de dispositivos virtuales (VAMI) en https://*servidor_orchestrator*:5480 e inicie sesión como **raíz**.

3 En la pestaña **Actualizar**, haga clic en **Configuración**.

4 Seleccione el botón de opción junto a **Usar repositorio especificado**.

5 Escriba la dirección URL del repositorio local que apunte al directorio `Update_Repo`.

`http://servidor_web_local:puerto/build/mts/release/bora-número_compilación/publish/exports/Update_Repo`

6 Si el repositorio local requiere autenticación, escriba el nombre de usuario y la contraseña.

7 Haga clic en **Guardar configuración**.

8 En la página **Estado**, haga clic en **Buscar actualizaciones**.

9 Si hay actualizaciones disponibles, haga clic en **Instalar actualizaciones**.

10 Acepte el contrato de licencia del usuario final de VMware y confirme que desea instalar la actualización.

11 Para completar la actualización, reinicie Orchestrator Appliance.

a Inicie sesión de nuevo en la Interfaz de administración de dispositivos virtuales (VAMI) como **`raíz`**.

12 (Opcional) En la pestaña **Actualizar**, compruebe que se haya instalado correctamente la última versión del Orchestrator Appliance.

Ha actualizado correctamente Orchestrator Appliance.

Qué hacer a continuación

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

Actualizar un clúster de Orchestrator 5.5.x y versiones posteriores a 7.x

Puede actualizar un clúster de Orchestrator a la versión 7.x actualizando una sola instancia y uniendo nodos que se instalan desde cero en la versión 7.x.

Prerequisitos

- Tome una instantánea de todos los nodos de servidor de vRealize Orchestrator.
- Realice una copia de seguridad de la base de datos compartida de Orchestrator.

Procedimiento

1 Detenga los servicios de Orchestrator `vco-server`, `vco-configurator` y `vco-proxy` en todos los nodos de clúster.

2 Actualice solo una de las instancias de servidor de Orchestrator en el clúster.

Consulte "Actualizar Orchestrator Appliance mediante el repositorio predeterminado de VMware," página 26.

3 Inicie el servicio de configuración del servidor de Orchestrator que ha actualizado e inicie sesión en el centro de control como **`raíz`**.

4 Vaya a la página **Validar configuración** para comprobar el estado de los componentes del sistema.

5 Implemente un dispositivo nuevo de Orchestrator en la versión actualizada.

6 Configure el nodo nuevo con los parámetros de red de una instancia existente.

7 En la página **Administración de clústeres de Orchestrator** del centro de control, una el nodo nuevo al nodo actualizado del clúster.

8 Reinicie los servidores de Orchestrator desde la página **Opciones de inicio** del centro de control para que coincidan las huellas digitales de configuración de los nodos.

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

10 (Opcional) Repita el procedimiento del Step 5 al Step 9 para cada nodo del clúster.

Ha actualizado correctamente el clúster de Orchestrator.

Actualizar un clúster de Orchestrator 7.0 a 7.x

En el clúster, varias instancias del servidor de Orchestrator funcionan a la vez. Si ya ha configurado un clúster de instancias de servidor de Orchestrator, puede actualizarlo a la última versión de Orchestrator actualizando sus nodos.

Procedimiento

1 Detenga los servicios de Orchestrator `vco-server`, `vco-configurator` y `vco-proxy` en todos los nodos de clúster.

2 Actualice una de las instancias de servidor de Orchestrator en el clúster.

Consulte "Actualizar Orchestrator Appliance mediante el repositorio predeterminado de VMware," página 26.

3 Inicie el servicio de configuración del servidor de Orchestrator que ha actualizado e inicie sesión en el centro de control como **`raíz`**.

4 Vaya a la página **Validar configuración** y compruebe el estado de los componentes del sistema.

5 Actualice todas las demás instancias del servidor de Orchestrator en el clúster.

6 Reinicie los servidores de Orchestrator desde la página **Opciones de inicio** del centro de control para que coincidan las huellas digitales de configuración de los nodos.

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

Ha actualizado correctamente el clúster de Orchestrator.

Configurar vRealize Orchestrator en Orchestrator Appliance 5

Aunque Orchestrator Appliance es una máquina virtual basada en Linux preconfigurada, debe configurar el complemento vCenter Server predeterminado y los demás complementos predeterminados de Orchestrator. También puede cambiar la configuración de Orchestrator.

Si desea utilizar Orchestrator Appliance en un entorno de media o gran escala, cambie el proveedor de autenticación para garantizar un rendimiento óptimo.

NOTA: La autenticación LDAP está en desuso y no se admitirá en futuras versiones.

Orchestrator Appliance contiene una base de datos PostgreSQL preconfigurada y un servidor LDAP de ApacheDS en curso. Solo es posible acceder a la base de datos PostgreSQL y el servidor LDAP de ApacheDS localmente desde la consola Linux del dispositivo virtual.

Software preconfigurado	Usuario o grupo de usuarios predeterminados	Contraseña
PostgreSQL preconfigurada	Usuario: vmware	vmware
LDAP de ApacheDS en curso	Grupo de usuarios: vcoadmins Usuario: vcoadmin De manera predeterminada, el usuario administrador está configurado como administrador de Orchestrator.	vcoadmin
LDAP de ApacheDS en curso	Grupo de usuarios: vcousers Usuario: vcouser	vcouser

La base de datos de PostgreSQL preconfigurada está lista para la producción. Para utilizar el dispositivo Orchestrator en un entorno de producción de alta carga, sustituya la base de datos de PostgreSQL preconfigurada por una instancia de base de datos externa. Para obtener más información sobre la configuración de una base de datos externa, consulte "Configurar la conexión de la base de datos de Orchestrator," página 41.

El servidor LDAP de ApacheDS en curso solo es adecuado para realizar pruebas. Para utilizar el dispositivo Orchestrator en un entorno de producción, configure un servicio de directorios con soporte externo o utilice autenticación de vRealize Automation, vSphere y vCenter Single Sign-On. Para obtener información sobre la configuración de un servicio de directorios externo o los proveedores de autenticación de vCenter Single Sign-On, vRealize Automation y vSphere, consulte "Seleccionar el tipo de autenticación," página 34.

Este capítulo cubre los siguientes temas:

Iniciar sesión en el centro de control

Para iniciar el proceso de configuración, debe acceder al centro de control.

Procedimiento

1 Acceda al centro de control desde https://*your_orchestrator_server_IP_or_DNS_name*:8281 en un navegador web y haga clic en **Centro de control de Orchestrator** o vaya directamente a https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter.

2 Inicie sesión con el nombre de usuario y contraseña predeterminados que configuró inicialmente.

- Nombre de usuario: **`raíz`**

  No es posible cambiar el nombre de usuario predeterminado.

- Contraseña: *your_password*

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`.

Ha iniciado sesión correctamente en el centro de control.

Puertos de red de Orchestrator

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

Puertos de configuración predeterminados

Para proporcionar el servicio de 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
Puerto de servidor HTTP	8280	TCP	Navegador web de usuario final	Servidor de 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 Orchestrator	El puerto de acceso para la página de inicio web de Orchestrator.
Puerto de acceso HTTPS de configuración web	8283	TCP	Navegador web de usuario final	Configuración de Orchestrator	El puerto de acceso SSL para la interfaz de usuario en Internet de configuración de Orchestrator.

Puertos de comunicación externos

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

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

Puerto	Número	Protocolo	Origen	Destino	Descripción
LDAP	389	TCP	Servidor de Orchestrator	Servidor LDAP	El puerto de búsqueda del servidor de autenticación LDAP. **NOTA:** La autenticación LDAP está en desuso y no se admitirá en futuras versiones.
LDAP con SSL	636	TCP	Servidor de Orchestrator	Servidor LDAP	El puerto de búsqueda del servidor de autenticación LDAP seguro.
LDAP con catálogo global	3268	TCP	Servidor de Orchestrator	Servidor de catálogo global	El puerto al que se dirigen las consultas del catálogo global de Microsoft.
Servidor de vCenter Single Sign-On	7444	TCP	Servidor de Orchestrator	Servidor de vCenter Single Sign-On	El puerto que se utiliza para comunicar con el servidor de vCenter Single Sign-On cuando se configura la **autenticación de vCenter Single Sign-On (heredada)** con vCenter Single Sign-On 5.5.
SQL Server	1433	TCP	Servidor de Orchestrator	Microsoft SQL Server	El puerto que se utiliza para comunicar con las instancias de Microsoft SQL Server que se configuran como base de datos de Orchestrator.
PostgreSQL	5432	TCP	Servidor de Orchestrator	Servidor de PostgreSQL	El puerto que se utiliza para comunicar con el servidor de PostgreSQL que se configura como base de datos de Orchestrator.
Oracle	1521	TCP	Servidor de Orchestrator	Servidor de base de datos de Oracle	El puerto que se utiliza para comunicar con el servidor de base de datos de Oracle que se configura como base de datos de Orchestrator.
Puerto de servidor SMTP	25	TCP	Servidor de Orchestrator	Servidor SMTP	El puerto que se utiliza para las notificaciones de correo electrónico.
Puerto API de vCenter Server	443	TCP	Servidor de Orchestrator	vCenter Server	El puerto de comunicación API de vCenter Server que utiliza Orchestrator para obtener la infraestructura virtual y la información de máquina virtual de las instancias orquestadas de vCenter Server.

Seleccionar el tipo de autenticación

Para trabajar correctamente y administrar los permisos de usuario, Orchestrator requiere un método de autenticación.

Orchestrator admite los tipos de autenticación siguientes.

Autenticación LDAP	Orchestrator se conecta a un servidor LDAP en funcionamiento. **NOTA:** La autenticación LDAP está en desuso y no se admitirá en futuras versiones.
Autenticación de vRealize Automation	Orchestrator se autentica a través del registro de componentes de vRealize Automation.
Autenticación de vSphere	Orchestrator se autentica a través de Platform Services Controller.
Autenticación de vCenter Single Sign-On (heredada)	Utilice este modo de autenticación solo si el proveedor de autenticación requerido es vCenter Single Sign-On 5.5.

Cuando descarga e implementa Orchestrator Appliance, el servidor de Orchestrator se configura previamente para funcionar con el servicio de directorios ApacheDS LDAP en curso integrado en el dispositivo. No obstante, si ya ha configurado Orchestrator para autenticarse a través de vRealize Automation, vSphere o SSO (heredada), la opción LDAP ya no aparece en el menú desplegable **Modo de autenticación**.

IMPORTANTE: Si desea utilizar Orchestrator a través de vSphere Web Client para administrar los objetos de inventario de vSphere, debe configurar Orchestrator para que funcione con el mismo Platform Service Controller al que están conectados vCenter Server y vSphere Web Client.

Configurar LDAP

Puede configurar Orchestrator para que se conecte a un servidor LDAP en funcionamiento en la infraestructura para autenticar usuarios y administrar los permisos de usuario.

NOTA: La autenticación LDAP está en desuso y no se admitirá en futuras versiones.

Si utiliza servidores LDAP seguros mediante SSL, Windows Server 2008 o 2012 y AD, compruebe que la política de grupo **Requisitos de firma de servidor LDAP** esté deshabilitada en el servidor LDAP.

IMPORTANTE: Varios dominios que no estén en el mismo árbol y tengan una confianza bidireccional son incompatibles y no funcionan con Orchestrator. El árbol de dominios es la única configuración compatible con Active Directory de varios dominios. La confianza externa y de bosque son incompatibles.

1 Importación del certificado SSL del servidor LDAP página 35

Si el servidor LDAP utiliza SSL, puede importar el archivo de certificado SSL al centro de control y permitir la conexión segura entre Orchestrator y LDAP.

2 Configurar la autenticación LDAP página 36

Para conectar Orchestrator a una instancia de servidor de directorios, debe proporcionar el host, el puerto y la base de búsqueda del servidor LDAP para generar la URL de conexión. Asimismo, debe proporcionar las credenciales de usuario, además de las rutas de búsqueda de usuarios y grupos, a fin de que los usuarios de LDAP se puedan autenticar en el cliente de Orchestrator.

3 Errores comunes de LDAP de Active Directory página 38

Si se produce el error `LDAP:código de error 49` y experimenta problemas para conectarse al servidor de autenticación LDAP, puede comprobar qué función LDAP está ocasionando el problema.

Importación del certificado SSL del servidor LDAP

Si el servidor LDAP utiliza SSL, puede importar el archivo de certificado SSL al centro de control y permitir la conexión segura entre Orchestrator y LDAP.

Puede importar el certificado SSL de LDAP de la página **Certificados** del centro de control.

Prerequisitos

- Si utiliza servidores LDAP, Windows Server 2008, Windows Server 2012 y Active Directory, compruebe que la política de grupo **Requisitos de firma del servidor LDAP** esté desactivada en el servidor LDAP.
- Obtenga un certificado de servidor autofirmado o un certificado firmado por una entidad de certificación.
- Configure el servidor LDAP para el acceso SSL. Consulte las instrucciones en la documentación del servidor LDAP.
- Especifique el certificado de confianza para llevar a cabo la sincronización SSL correctamente.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Certificados**.

3 En la pestaña **Certificados de confianza**, haga clic en **Importar**.

4 Cargue el certificado SSL de LDAP desde una URL o un archivo.

Opción	Acción
Importar de URL o URL de proxy	Escriba la URL del servidor LDAP: `https://dirección_IP_servidor_LDAP` o `dirección_IP_servidor_LDAP:puerto`
Importar desde archivo	Obtenga un archivo de certificado SSL de LDAP y vaya hasta él para importarlo.

5 Haga clic en **Importar**.

Aparece un mensaje que confirma que la importación se ha realizado correctamente.

El certificado importado aparecerá en la lista Certificados SSL de confianza. La conexión segura entre Orchestrator y el servidor LDAP se habrá activado.

Qué hacer a continuación

Cuando genera la URL de conexión LDAP, debe activar SSL en la página **Configurar proveedor de autenticación** del centro de control.

Configurar la autenticación LDAP

Para conectar Orchestrator a una instancia de servidor de directorios, debe proporcionar el host, el puerto y la base de búsqueda del servidor LDAP para generar la URL de conexión. Asimismo, debe proporcionar las credenciales de usuario, además de las rutas de búsqueda de usuarios y grupos, a fin de que los usuarios de LDAP se puedan autenticar en el cliente de Orchestrator.

Active Directory sobre LDAP y los servicios de directorios basados en OpenLDAP son los tipos de servicios de directorios admitidos.

NOTA: Si cambia el servidor LDAP o el tipo de servicios de directorios tras asignar permisos de acceso a flujos de trabajo o a acciones en objetos de Orchestrator, es preciso restablecer dichos permisos.

Si cambia la configuración de LDAP tras configurar aplicaciones personalizadas que recopilan y almacenan información de los usuarios, los registros de autenticación LDAP dejan de ser válidos cuando se utilizan en la nueva base de datos de LDAP.

Prerequisitos

Utilice la información de configuración detallada para configurar la autenticación LDAP. Consulte "Opciones de configuración de autenticación LDAP," página 36.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Configurar proveedor de autenticación**.

3 Seleccione **Autenticación LDAP** en el menú desplegable **Modo de autenticación**.

4 En el menú desplegable **Cliente LDAP**, seleccione el tipo de servidor de directorios que quiere utilizar.

5 Configure el servidor LDAP en su entorno.

6 Haga clic en **Guardar cambios**.

7 Indique las credenciales de un usuario de LDAP en **Probar inicio de sesión** para probar si este usuario tiene acceso al cliente de Orchestrator.

   Tras un inicio de sesión válido, el sistema comprueba si el usuario pertenece al grupo de administradores de Orchestrator.

Qué hacer a continuación

Configure la base de datos. Para obtener más información, consulte "Configurar la conexión de la base de datos de Orchestrator," página 41.

Opciones de configuración de autenticación LDAP

Para obtener una conexión correcta entre Orchestrator y el servidor de directorios, debe configurar las opciones de autenticación LDAP para que coincidan con las opciones de configuración del servidor LDAP.

Tabla 5-3. Opciones de autenticación LDAP

Opciones	Descripciones
Host de LDAP principal	Dirección IP o nombre de DNS del primer host en el que el centro de control verifica las credenciales de usuario.
Host de LDAP secundario	Dirección IP o nombre de DNS del host en el que el centro de control verifica las credenciales de usuario si el host de LDAP principal no está disponible.

Tabla 5-3. Opciones de autenticación LDAP (Continua)

Opciones	Descripciones
Puerto	Valor del puerto de búsqueda del servidor LDAP. **NOTA:** Orchestrator admite la estructura jerárquica de dominios de Active Directory. Si el controlador de dominio está configurado para usar el catálogo global, debe usar el puerto 3268. No se puede usar el puerto predeterminado 389 para conectarse al servidor del catálogo global.
Raíz	Contenedor de espacio de nombres raíz. Si el nombre de dominio es *empresa.org*, el contenedor raíz es **`dc=empresa,dc=org`**. **NOTA:** Para mejorar el rendimiento en directorios de servicios de tamaño grande, puede limitar la base de búsqueda definiendo un contenedor específico en la estructura de árbol. Por ejemplo, en lugar de buscar en todo el directorio, puede especificar **`ou=empleados,dc=empresa,dc=org`**. Este filtro de búsqueda devuelve todos los usuarios de la unidad organizativa Empleados. Los valores que se indican en los cuadros de texto pertinentes generan esta URL de conexión LDAP: `ldap://DomainController:389/ou=empleados,dc=empresa,dc=org`.
Utilizar SSL	Si esta opción está habilitada, Orchestrator y LDAP tienen una conexión cifrada. **NOTA:** Si LDAP utiliza SSL, primero se debe importar el certificado SSL y reiniciar el servicio del servidor de Orchestrator. Consulte "Importación del certificado SSL del servidor LDAP," página 35.
Nombre de usuario	Nombre de una cuenta de usuario que tiene permisos para acceder al árbol de directorios. El nombre de usuario de Active Directory se puede especificar en uno de estos formatos: ■ Nombre de usuario a secas, por ejemplo:**`usuario`** ■ Nombre distintivo, por ejemplo: **`cn=usuario,ou=empleados,dc=empresa,dc=org`** ■ Nombre principal, por ejemplo: **`usuario@empresa.org`**
Contraseña	Contraseña de la cuenta de usuario que tiene permisos para acceder al árbol de directorios.
Base de búsqueda de usuarios	Contenedor LDAP o unidad organizativa donde Orchestrator busca usuarios potenciales.
Grupo de administradores	Debe ser un grupo de LDAP al que desee otorgar privilegios administrativos para Orchestrator. Por ejemplo, **`Administradores de dominios`**.
Tiempo de espera de solicitud	Valor en milisegundos que determina el periodo en el que el servidor de Orchestrator envía una consulta al directorio de servicios y espera una respuesta. Si transcurre el periodo de tiempo de espera, modifique este valor para comprobar si el plazo expira en el servidor de Orchestrator.
Tiempo de espera de accesibilidad del host	Valor en milisegundos que determina el periodo de tiempo de espera para la comprobación de conectividad con el host de destino.

Tabla 5-3. Opciones de autenticación LDAP (Continua)

Opciones	Descripciones
Desreferenciar vínculos	Se esta opción está seleccionada, el servidor LDAP resuelve los alias de usuario con el objeto de usuario buscado.
Atributos de filtro	Filtra los atributos LDAP devueltos por la búsqueda LDAP. Si se selecciona esta casilla de verificación, la búsqueda en LDAP es más rápida, ya que no se devuelven determinados atributos. Ahora bien, puede suceder que más adelante necesite atributos LDAP adicionales para la automatización.

Errores comunes de LDAP de Active Directory

Si se produce el error `LDAP:código de error 49` y experimenta problemas para conectarse al servidor de autenticación LDAP, puede comprobar qué función LDAP está ocasionando el problema.

Tabla 5-4. Errores comunes de autenticación de Active Directory

Error	Descripción
525	El usuario no se encuentra.
52e	Las credenciales del usuario no son válidas.
530	El usuario no puede iniciar sesión en este momento.
531	El usuario no puede iniciar sesión en esta estación de trabajo.
532	La contraseña ha caducado.
533	Esta cuenta de usuario se ha desactivado.
701	Esta cuenta de usuario ha caducado.
773	El usuario debe restablecer su contraseña.
775	La cuenta de usuario se ha bloqueado.

Configurar la autenticación de vRealize Automation

Puede configurar Orchestrator para autenticar a través del registro de componentes de vRealize Automation.

Prerequisitos

Instale y configure vRealize Automation, y compruebe que el servidor de vRealize Automation se esté ejecutando.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Configurar proveedor de autenticación**.

3 Seleccione **vRealize Automation** en el menú desplegable **Modo de autenticación**.

4 En el cuadro de texto **Dirección del host**, indique la dirección de host de vRealize Automation y haga clic en **Conectar**.

5 Haga clic en **Aceptar certificado**.

6 En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de la cuenta de administrador de vRealize Automation.

   La cuenta se utiliza temporalmente solo para registrar o eliminar Orchestrator como solución.

7 (Opcional) Seleccione la casilla **Configurar licencias**.

8 Haga clic en **Registrar**.

9 En el cuadro de texto **Tenant predeterminado**, escriba el dominio predeterminado para autenticar a los usuarios que inician sesión sin un nombre de dominio. El valor predeterminado es **`vsphere.local`**.

10 En el cuadro de texto **Grupo de administradores**, escriba un grupo de administradores y haga clic en **Buscar**.

11 Seleccione un grupo de administradores.

12 Haga clic en **Guardar cambios**.

   Un mensaje indica que se ha guardado correctamente.

Qué hacer a continuación

Para que los cambios surtan efecto, reinicie el servidor de Orchestrator desde la página de opciones de inicio del centro de control.

Configuración de vCenter Single Sign-On

VMware vCenter Single Sign-On es un servicio de autenticación que implementa el patrón arquitectónico de autenticación asíncrona. Puede configurar Orchestrator para que se conecte a una instancia de vCenter Single Sign-On, mediante la ejecución de un servidor de Platform Services Controller.

El servidor vCenter Single Sign-On proporciona una interfaz de autenticación denominada Security Token Service (STS). Los clientes envían mensajes de autenticación a STS, que comprueba las credenciales del usuario frente a uno de los orígenes de identidad. Una vez efectuada correctamente la autenticación, STS genera un token.

Platform Services Controller contiene la interfaz administrativa de vCenter Single Sign-On, que es parte de vSphere Web Client. Para configurar vCenter Single Sign-On y administrar los usuarios y grupos de vCenter Single Sign-On, inicie sesión en vSphere Web Client como usuario con privilegios administrativos de vCenter Single Sign-On. Podría no ser el mismo usuario que el administrador de vCenter Server. Debe proporcionar las credenciales en la página de inicio de sesión de vSphere Web Client y, tras la autenticación, podrá acceder a la herramienta de administración de vCenter Single Sign-On para crear usuarios y asignar permisos administrativos a otros usuarios.

Con vSphere Web Client, se autentica en vCenter Single Sign-On proporcionando las credenciales en la página de inicio de sesión de vSphere Web Client. A continuación, puede ver todas las instancias de vCenter Server para las que tiene permiso. Después de conectarse a vCenter Server, no se requiere ninguna autenticación adicional. Las acciones que lleva a cabo con los objetos dependen de los permisos de vCenter Server que tiene el usuario sobre esos objetos.

Para más información sobre Platform Services Controller, consulte *Seguridad de vSphere*.

Después de configurar Orchestrator para que se autentique mediante vCenter Single Sign-On, asegúrese de configurarlo para que funcione con las instancias de vCenter Server registradas con vSphere Web Client utilizando la misma instancia de vCenter Single Sign-On.

Cuando inicia sesión en vSphere Web Client, el complemento web de Orchestrator se comunica con el servidor de Orchestrator en nombre del perfil de usuario que ha utilizado para iniciar sesión.

Configurar la autenticación a través de vSphere Platform Services Controller

Para registrar el servidor de Orchestrator con un servidor de vCenter Single Sign-On, utilice el modo de autenticación del centro de control. Utilice la autenticación de vCenter Single Sign-On con vCenter Server 6.0 y versiones posteriores.

Prerequisitos

Instale y configure VMware vCenter Single Sign-On, y compruebe que el servidor de vCenter Single Sign-On se esté ejecutando.

IMPORTANTE: Asegúrese de que los relojes del servidor de Orchestrator y vCenter Server Appliance estén sincronizados. De lo contrario, podría recibir errores de vCenter Single Sign-On crípticos.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Configurar proveedor de autenticación**.

3 Seleccione **vSphere** en el menú desplegable **Modo de autenticación**.

4 En el cuadro de texto **Dirección del host**, indique la dirección de host de Platform Services Controller y haga clic en **Conectar**.

5 Haga clic en **Aceptar certificado**.

6 En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de la cuenta de administrador de vCenter Single Sign-On.

La cuenta se utiliza temporalmente solo para registrar o eliminar Orchestrator como solución.

7 (Opcional) Seleccione la casilla **Configurar licencias**.

8 Haga clic en **Registrar**.

9 En el cuadro de texto **Tenant predeterminado**, escriba el dominio predeterminado para autenticar a los usuarios que inician sesión sin un nombre de dominio. El valor predeterminado es `vsphere.local`.

10 En el cuadro de texto **Grupo de administradores**, escriba un grupo de administradores y haga clic en **Buscar**.

11 Haga clic en **Guardar cambios**.

Un mensaje indica que se ha guardado correctamente.

Ha registrado satisfactoriamente Orchestrator con vCenter Single Sign-On.

Registrar Orchestrator como solución de vCenter Single Sign-On (heredada)

Para registrar el servidor de Orchestrator con un servidor de vCenter Single Sign-On, utilice el modo de autenticación heredado de Single Sign-On en el centro de control. Utilice la autenticación heredada de Single Sign-On solo con vCenter Server, versión 5.5 y sus versiones de actualización correspondientes a partir de la actualización 2.

Prerequisitos

Instale y configure VMware vCenter Single Sign-On, y compruebe que el servidor de vCenter Single Sign-On se esté ejecutando.

IMPORTANTE: Asegúrese de que los relojes del servidor de Orchestrator y vCenter Server Appliance estén sincronizados. De lo contrario, podría recibir errores de vCenter Single Sign-On crípticos.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Configurar proveedor de autenticación**.

3 Seleccione **SSO (heredada)** en el menú desplegable **Modo de autenticación**.

4 En el cuadro de texto **URL de STS**, escriba la URL para la interfaz de servicio de token de vCenter Single Sign-On.

```
https://su_servidor_vcenter_single_sign_on:7444/sts/STSService/vsphere.local
```

5 En el cuadro de texto **URL de administradores**, especifique la URL para la interfaz de servicio de administración de vCenter Single Sign-On.

```
https://su_servidor_vcenter_single_sign_on:7444/sso-adminserver/sdk/vsphere.local
```

6 Haga clic en **Conectar**.

7 Haga clic en **Aceptar certificado**.

8 En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador de vCenter Single Sign-On.

La cuenta se utiliza temporalmente solo para registrar o eliminar Orchestrator como solución.

9 Haga clic en **Registrar**.

10 En el cuadro de texto **Tenant predeterminado**, escriba el dominio predeterminado para autenticar a los usuarios que inician sesión sin un nombre de dominio. El valor predeterminado es `vsphere.local`.

11 En el cuadro de texto **Grupo de administradores**, escriba un grupo de administradores y haga clic en **Buscar**.

12 Haga clic en **Guardar cambios**.

Un mensaje indica que se ha guardado correctamente.

Ha registrado satisfactoriamente Orchestrator con vCenter Single Sign-On.

Configurar la conexión de la 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 PostgreSQL preinstalada en el dispositivo.

La base de datos Orchestrator PostgreSQL preconfigurada está lista para la producción. Para un mejor rendimiento en un entorno de alta carga de producción, instale un sistema de administración de bases de datos relacionales (RDBMS) independiente y cree una base de datos para Orchestrator. Para más información sobre cómo crear una base de datos para Orchestrator, consulte "Configurar la base de datos de Orchestrator," página 22. Para utilizar la base de datos externa con Orchestrator, configure la base de datos para la conexión remota.

Importación del certificado SSL de la base de datos

Si la base de datos utiliza SSL, debe importar el certificado SSL al centro de control y establecer una conexión segura entre Orchestrator y la base de datos.

Prerequisitos

- Configure la base de datos para el acceso SSL. Consulte las instrucciones correspondientes en la documentación de la base de datos.

- Obtenga un certificado de servidor autofirmado o un certificado firmado por una entidad de certificación.
- Especifique el certificado de confianza para llevar a cabo la sincronización SSL correctamente.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Certificados**.

3 En la pestaña **Certificados de confianza**, haga clic en **Importar**.

4 Cargue el certificado SSL de la base de datos desde una URL o un archivo.

Opción	Acción
Importar de URL o URL de proxy	Introduzca la dirección URL del servidor de base de datos: `https://dirección_IP_serviddor_base_datos` o `dirección_IP_servidor_base_datos:puerto`
Importar desde archivo	Obtenga el archivo de certificado SSL de la base de datos y vaya hasta él para importarlo.

El certificado importado aparecerá en la lista Certificados SSL de confianza. La conexión segura entre Orchestrator y su base de datos se habrá activado.

Qué hacer a continuación

Cuando configure la conexión de la base de datos, debe activar SSL en la página **Configurar base de datos** en el centro de control.

Configurar la conexión de la base de datos

Para establecer una conexión a la base de datos de Orchestrator, debe establecer los parámetros de la conexión.

Prerequisitos

- Configure una nueva base de datos para utilizar con el servidor de Orchestrator. Consulte "Configurar la base de datos de Orchestrator," página 22.
- Si utiliza una base de datos de SQL Server configurada para utilizar puertos dinámicos, compruebe que esté en ejecución el servicio SQL Server Browser.
- Para evitar interbloqueos transaccionales cuando utilice la base de datos de Microsoft SQL Server, debe activar las opciones de base de datos `ALLOW_SNAPSHOT_ISOLATION` y `READ_COMMITTED_SNAPSHOT`.
- Si la base de datos de Microsoft SQL Server utiliza puertos dinámicos, asegúrese de que SQL Server Browser esté ejecutándose.
- Para evitar un error `ORA-01450` durante el uso de una base de datos de Oracle, compruebe que haya configurado correctamente el tamaño del bloque de la base de datos. El tamaño mínimo necesario depende del tamaño del bloque utilizado por el índice de la base de datos de Oracle.
- Para almacenar caracteres en el formato correcto en una base de datos de Oracle, establezca el parámetro `NLS_CHARACTER_SET` en `AL32UTF8` antes de configurar la conexión de la base de datos y de crear una estructura de tabla para Orchestrator. Esta configuración es fundamental para un entorno internacionalizado.
- Para configurar Orchestrator a fin de que se comunique con la base de datos a través de una conexión segura, debe importar el certificado SSL de la base de datos. Para obtener más información, consulte "Importación del certificado SSL de la base de datos," página 41.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Configurar base de datos**.

3 En el menú desplegable **Tipo de la base de datos**, seleccione el tipo de la base de datos que debe utilizar el servidor de Orchestrator.

Opción	Descripción
Oracle	Configura Orchestrator para que funcione con una instancia de la base de datos de Oracle.
SQL Server	Configura Orchestrator para que funcione con una instancia de la base de datos de Microsoft SQL Server.
PostgreSQL	Configura Orchestrator para que funcione con una instancia de la base de datos de PostgreSQL.
DerbyDB en curso	Configura Orchestrator para que funcione con la base de datos de DerbyDB en curso. **NOTA:** No debe utilizar DerbyDB.

4 Introduzca los parámetros de conexión de la base de datos y haga clic en **Guardar cambios**.

Opción	Descripción
Dirección del servidor	La dirección IP o el nombre DNS del servidor de la base de datos. Esta opción se aplica a todas las bases de datos.
Puerto	El puerto del servidor de la base de datos se utiliza para la comunicación con la base de datos. Esta opción se aplica a todas las bases de datos.
Utilizar SSL	Seleccione **Utilizar SSL** para utilizar una conexión SSL con la base de datos. Para utilizar esta opción, debe importar el certificado SSL de la base de datos a Orchestrator. Esta opción se aplica a todas las bases de datos.
Nombre de la base de datos	El nombre único completo de la base de datos. El nombre de la base de datos se especifica en el parámetro `SERVICE_NAMES` en el archivo de parámetros de inicialización. Esta opción solo es válida para las bases de datos de SQL Server y PostgreSQL.
Nombre de usuario	El nombre de usuario que utiliza Orchestrator para conectarse a la base de datos seleccionada y utilizarla. El nombre que seleccione debe ser un usuario válido en la base de datos de destino con derechos de **db_owner**. Esta opción se aplica a todas las bases de datos.
Contraseña	La contraseña del nombre de usuario. Esta opción se aplica a todas las bases de datos.
Nombre de instancia (si la hay)	El nombre de la instancia de la base de datos que se puede identificar mediante el parámetro `INSTANCE_NAME` en el archivo de parámetros de inicialización de la base de datos. Esta opción solo es válida para las bases de datos de SQL Server y Oracle.

Opción	Descripción
Dominio	Para utilizar la autenticación de Windows, escriba el nombre de dominio de la máquina SQL Server, por ejemplo *empresa.org*. Para utilizar la autenticación SQL, deje en blanco este cuadro de texto. Esta opción solo es válida para SQL Server y especifica si se desea utilizar la autenticación de Windows o de SQL Server.
Utilizar modo de autenticación de Windows (NTLMv2)	Seleccione esta opción para enviar respuestas NTLMv2 cuando utilice la autenticación de Windows. Esta opción solo es válida para SQL Server.

Si los parámetros especificados son correctos, un mensaje indica que la conexión con la base de datos se ha establecido correctamente.

5 Actualice la estructura de tabla para Orchestrator, si es necesario.

6 Haga clic en **Guardar cambios**.

La conexión de base de datos se ha configurado correctamente.

Exportación de la base de datos de Orchestrator

Cree un archivo con una copia de seguridad completa de la base de datos del servidor. La base de datos solo se puede exportar si es PostgreSQL y se ejecuta en Linux.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Exportar base de datos**.

3 Seleccione si desea exportar los tokens de flujo de trabajo y los eventos de registro con la base de datos.

4 Haga clic en **Exportar base de datos**

El centro de control crea un archivo `vco-db-dump-`*`databaseName@hostname`*`.gz` en la máquina donde instaló el servidor de Orchestrator. Puede utilizar este archivo para clonar y restaurar el sistema.

Importación de una base de datos de Orchestrator

Puede importar una base de datos exportada previamente después de reinstalar Orchestrator o si se produce un error del sistema.

Prerequisitos

La nueva base de datos de Orchestrator debe estar vacía.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Importar base de datos**.

3 Vaya al archivo `.gz` que ha exportado en la instalación anterior y selecciónelo.

4 Haga clic en **Importar base de datos**

Un mensaje indica que la base de datos se ha importado correctamente. El nuevo sistema obtiene la base de datos del sistema antiguo.

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 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.

IMPORTANTE: No se puede cambiar el certificado del servidor si Orchestrator utiliza la base de datos Apache Derby en curso.

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.

Opciónpacteracontextmathced	Descripciónpacteracontextmathced
Importar de URL o URL de proxy	URL del servidor remoto: `https://dirección_IP_servidor` o `dirección_IP_servidor:puerto`
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," página 46.

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.

Opciónpacteracontextmathced	Descripciónpacteracontextmathced
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`.

Opciónpacteracontextmathced	Descripciónpacteracontextmathced
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.

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.

Prerequisitos

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:25 –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**.

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

Configuración de los complementos de Orchestrator

Los complementos predeterminados de Orchestrator se configuran únicamente mediante flujos de trabajo.

Si desea configurar cualquier complemento predeterminado de Orchestrator, debe utilizar los flujos de trabajo específicos del cliente de Orchestrator.

Administrar complementos de Orchestrator

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

Cambiar el nivel de registro de complementos

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

Instalar un nuevo complemento

Con los complementos de Orchestrator, el servidor de Orchestrator puede integrarse con otros productos de software. Orchestrator Appliance incluye una serie de complementos preinstalados; también se pueden instalar complementos personalizados.

Todos los complementos de Orchestrator se instalan desde el centro de control. Las extensiones de archivo que pueden usarse son `.vmoapp` y `.dar`. Un archivo `.vmoapp` puede contener varios archivos `.dar` y se puede instalar como una aplicación. Por su parte, un archivo `.dar` contiene todos los recursos asociados a un complemento.

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,” página 48.

Desinstalar un complemento

Puede utilizar el centro de control para deshabilitar un complemento; sin embargo, esta acción no quita el archivo del complemento del sistema de archivos de Orchestrator Appliance. Para quitar el archivo del complemento, debe iniciar sesión en Orchestrator Appliance y hacerlo manualmente.

Procedimiento

1 Elimine el complemento de Orchestrator Appliance.

   a Inicie sesión en Orchestrator Appliance sobre SSH como **raíz**.

   b Abra el archivo `/etc/vco/app-server/plugins/_VSOPluginInstallationVersion.xml` con un editor de texto.

   c Elimine la línea de código que se corresponde con el complemento que quiere quitar.

   d Vaya al directorio `/var/lib/vco/app-server/plugins`.

   e Elimine los archivos `.dar` que contienen el complemento que quiere quitar.

2 Reinicie los servicios de vRealize Orchestrator.

```
service vco-configurator restart && service vco-server restart
```

3 Inicie sesión en el centro de control como **raíz**.

4 En la página **Administrar complementos**, compruebe que se eliminó el complemento.

5 Mediante el cliente de Orchestrator, elimine los paquetes y las carpetas que están relacionadas con el complemento.

   a Inicie sesión en el cliente de Orchestrator.

   b Seleccione **Diseño** en el menú desplegable de la esquina superior izquierda.

   c Haga clic en la vista **Paquetes**.

   d Haga clic con el botón secundario en el paquete que quiere eliminar y seleccione **Eliminar elemento con contenido**.

   NOTA: No se eliminan los elementos de Orchestrator que están bloqueados en el estado de solo lectura, como los flujos de trabajo de la biblioteca estándar.

   e En el menú **Herramientas** de la esquina superior derecha, seleccione **Preferencias del usuario**.

   Se abrirá el menú contextual **Preferencias**.

   f En la página **General**, seleccione la casilla de verificación **Permitir la eliminación de una carpeta no vacía**.

   Ahora puede eliminar una carpeta completa, incluidos los flujos de trabajo y las subcarpetas, con un único clic.

   g Haga clic en la vista **Flujo de trabajo**.

   h Elimine la carpeta del complemento que quiere quitar.

   i Haga clic en la vista **Acciones**.

   j Elimine los módulos de acción del complemento que quiere quitar.

6 Reinicie los servicios de vRealize Orchestrator.

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

Opciones de inicio de Orchestrator

En la página **Opciones de inicio** del centro de control, puede iniciar, detener y reiniciar el servicio del servidor de Orchestrator.

El inicio de Orchestrator por primera vez podría requerir entre cinco y diez minutos porque el servidor instala el contenido de los complementos de Orchestrator en las tablas de bases de datos.

La página **Opciones de inicio** muestra el estado del servicio `vco-server`.

Estado	Descripción
`EN EJECUCIÓN`	El servicio del servidor de Orchestrator se ha iniciado y se ejecuta correctamente.
`SIN DEFINIR`	El servicio del servidor de Orchestrator se está iniciando.
`DETENIDO`	El servicio del servidor de Orchestrator no se está ejecutando.

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 está en ejecución, puede utilizar el servicio de comprobación del estado (incluido en la API de REST) accediendo a https://*nombre_DNS_o_servidor_IP_orchestrator*:8281/vco/api/healthstatus y comprobar el estado del nodo.

IMPORTANTE: No se admite el desarrollo de flujos de trabajo realizado por varios usuarios en un entorno agrupado. Cuando varios usuarios utilizan los distintos nodos de Orchestrator dentro del clúster para modificar el mismo recurso, se producen problemas de simultaneidad. Para tener más de un nodo de servidor de Orchestrator activo en un clúster, primero debe desarrollar los flujos de trabajo que necesita. A continuación, puede configurar Orchestrator para que funcione en un clúster.

Configurar un clúster de Orchestrator

Para aumentar la disponibilidad de los servicios de Orchestrator, puede crear un clúster de instancias de servidor de Orchestrator.

Un clúster de Orchestrator se compone de, como mínimo, dos instancias de servidor de Orchestrator que comparten una base de datos.

Prerequisitos

- Instale al menos dos instancias de servidor de Orchestrator.
- Configure la base de datos externa que tiene previsto utilizar como base de datos compartida, para que pueda aceptar conexiones de diferentes instancias de Orchestrator.

  Para evitar interbloqueos transaccionales cuando utilice la base de datos de Microsoft SQL Server, debe activar las opciones de base de datos `ALLOW_SNAPSHOT_ISOLATION` y `READ_COMMITTED_SNAPSHOT`.
- Si la base de datos de Microsoft SQL Server utiliza puertos dinámicos, asegúrese de que SQL Server Browser esté ejecutándose.
- Sincronice los relojes de las máquinas virtuales en las que estén instaladas las instancias del servidor de Orchestrator.

Procedimiento

1 Configure el primer nodo de Orchestrator.

  a Inicie sesión en el centro de control del primer servidor de Orchestrator como **`raíz`**.

  b Detenga el servicio del servidor de Orchestrator desde la página **Opciones de inicio**.

  c Configure la conexión a la base de datos compartida externa. Para obtener más información, consulte "Configurar la conexión de la base de datos," página 42.

  Los cambios en la configuración, por ejemplo de certificados, licencias o proveedores de autenticación, deben realizarse después de configurar las instancias de Orchestrator para que funcionen con la base de datos compartida.

  d Configure el proveedor de autenticación. Consulte "Seleccionar el tipo de autenticación," página 34.

  e (Opcional) Establezca cualquier otra propiedad del sistema. Consulte Capítulo 11, "Establecimiento de las propiedades del sistema," página 93 para obtener información.

  f (Opcional) Abra la página **Integración de registro** y configure Orchestrator para que utilice un servidor de registro remoto.

g (Opcional) En la pestaña **Configuración de los nodos de Orchestrator** de la página **Administración de clústeres de Orchestrator**, proporcione valores para la configuración del nodo de Orchestrator y haga clic en **Guardar**.

Opción	Descripciónpacteracontextmathced
Cantidad de nodos activos	El número máximo de instancias de servidor de Orchestrator activas en el clúster. Los nodos activos son las instancias de servidor de Orchestrator que ejecutan flujos de trabajo y responden a las solicitudes de los clientes. Si un nodo activo de Orchestrator deja de responder, lo sustituye una instancia inactiva de servidor de Orchestrator. El número predeterminado de nodos activos de Orchestrator en un clúster es de uno.
Intervalo de latidos (en milisegundos)	El intervalo de tiempo, en milisegundos, entre dos latidos de red que envía un nodo de Orchestrator para mostrar que está en ejecución. El valor predeterminado es de 12 segundos.
Cantidad de latidos de conmutación por error	El número de latidos ausentes antes de que un nodo de Orchestrator se considere fallido. El valor predeterminado es de 10 latidos.

El tiempo de espera predeterminado es de dos minutos y equivale al valor del intervalo de latidos predeterminado multiplicado por el número de latidos de conmutación por error predeterminados.

h Compruebe que el nodo esté configurado correctamente en la página **Validar configuración** en el centro de control.

i (Opcional) Instale los complementos externos.

j Inicie el servicio del servidor de Orchestrator en el primer nodo de Orchestrator.

k En la página **Opciones de inicio**, asegúrese de que las cadenas **Huella digital de configuración activa** y **Huella digital de configuración pendiente** coincidan.

NOTA: Puede que necesite actualizar la página **Opciones de inicio** varias veces hasta que coincidan ambas cadenas.

l (Opcional) Configure los complementos externos.

2 Configure el clúster de Orchestrator.

a Inicie sesión en el centro de control del segundo servidor de Orchestrator como `raíz`.

b Haga clic en la pestaña **Unir nodo a clúster** en la página **Administración de clústeres de Orchestrator**.

c En el cuadro de texto **Nombre del host**, escriba el nombre del host o la dirección IP de la primera instancia del servidor de Orchestrator.

d En los cuadros de texto **Nombre de usuario** y **Contraseña**, escriba sus credenciales del centro de control.

e Haga clic en **Unir**.

La instancia de Orchestrator clona la configuración del nodo, al cual se une.

Ha configurado correctamente un clúster de instancias de Orchestrator.

Qué hacer a continuación

Puede añadir más nodos activos del servidor de Orchestrator cambiando el valor del cuadro de texto **Cantidad de nodos activos** en la página **Administración de clústeres de Orchestrator**.

Supervisión y sincronización de un clúster de Orchestrator

Después de crear un clúster, puede supervisar el estado de los nodos del clúster y efectuar las acciones pertinentes para que los nodos estén sincronizados.

Puede comprobar los estados de sincronización de la configuración de las instancias de Orchestrator que se han unido a un clúster en la pestaña **Configuración de los nodos de Orchestrator** de la página **Administración de clústeres de Orchestrator**.

IMPORTANTE: El centro de control informa del estado del nodo local comparado con los otros nodos del clúster.

Estado de sincronización de la configuración	Nodo local	Nodo remoto
Sincronizado	La configuración del nodo local no cambió desde el último reinicio.	La configuración del nodo remoto es la misma que la del nodo local.
Es preciso reiniciar el nodo	La configuración del nodo local cambió o se replicó desde el nodo remoto. Reinicie el nodo local para aplicar la configuración pendiente.	La configuración del nodo remoto está sincronizada con el nodo local, pero no se ha aplicado. Reinicie el nodo remoto para aplicar la configuración.
Debe sincronizarse una configuración	N/D	La configuración activa del nodo remoto es la diferente a la configuración activa del nodo local.
El centro de control del nodo no está disponible	N/D	El servicio del centro de control (`vco-configurator`) del nodo remoto se ha detenido o no está disponible. El estado de sincronización no se puede recuperar.
No disponible. Falta nodo local	El nodo local no está en la lista de nodos del clúster. El estado de sincronización del nodo local no se puede recuperar.	N/D

Insertar configuración y reiniciar nodos

Al cambiar una configuración en el nodo local, utilice la opción de menú desplegable **Insertar configuración y reiniciar nodos** para copiar la configuración del nodo local en todos los demás nodos del clúster. Si desea copiar la configuración y reiniciar los nodos más adelante, utilice la opción **Insertar configuración**.

Eliminación de un nodo de un clúster de Orchestrator

Si desea eliminar un nodo de un clúster, debe configurar el nodo para que funcione con una base de datos que no esté en uso por parte de un clúster de Orchestrator.

NOTA: Cuando cambie la base de datos de un nodo, debe importar o volver a generar los certificados y la licencia.

Si el centro de control muestra nodos que ya no forman parte del clúster, acceda a la página **Administración de clústeres de Orchestrator**, en https://*nombre_DNS_o_servidor_IP_de_orchestrator*:8283/vco-controlcenter/#/control-app/ha?remove-nodes, para eliminar los nodos sobrantes.

Configurar un equilibrador de carga

Los equilibradores de carga distribuyen el trabajo entre los servidores en implementaciones de alta disponibilidad.

Tras configurar el clúster de Orchestrator, puede definir un equilibrador de carga que distribuya el tráfico entre diversas instancias de vRealize Orchestrator. Para obtener más información, consulte Equilibrio de carga de vRealize Orchestrator.

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. Si decide participar en el CEIP, VMware recopilará de forma periódica ciertos tipos de información técnica sobre el uso que hace de los productos y servicios de VMware en informes de CEIP.

Para conocer los tipos de información que VMware recopila y cómo utiliza esa información, visite el Portal de CEIP de VMware en http://www.vmware.com/trustvmware/ceip.html

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

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

Procedimiento

1. Inicie sesión en el centro de control como **raíz** y abra la página **Programa de mejora de la experiencia del cliente**.
2. Seleccione la casilla **Participe en el programa de mejora de la experiencia de cliente (CEIP)** para activar el CEIP o anule su selección para desactivar el programa; a continuación, haga clic en **Guardar**.
3. (Opcional) Anule la selección de la casilla **Detección automática del proxy** si desea añadir un host de 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.

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," página 45.

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 HTPS, el formato admitido es *dirección_IP_o_nombre_DNS:puerto*. 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 cubre los siguientes temas:

Crear un usuario nuevo en el centro de control

Para evitar posibles problemas de seguridad, en lugar de cambiar la contraseña raíz, puede crear una cuenta de usuario y asignarle una contraseña en cualquier momento. Al crear esta nueva cuenta de usuario, se deshabilita el acceso de la cuenta raíz al centro de control.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 En la página **Configuración**, haga clic en **Cambiar credenciales**.

3 En el cuadro de texto **Contraseña antigua**, indique la contraseña actual.

4 En el cuadro de texto **Nombre de usuario nuevo**, indique el nombre del nuevo usuario.

5 En el cuadro de texto **Contraseña nueva**, indique la nueva contraseña.

6 Vuelva a introducir la contraseña nueva para confirmarla.

7 Haga clic en **Cambiar credenciales**.

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 **administrador**.

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**.

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.

NOTA: Si decide clonar la instancia de Orchestrator, no debe importar la configuración de la base de datos a la instancia de Orchestrator clonada. En lugar de ello, debe configurar una conexión a otra base de datos externa.

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.

Prerequisitos

Detenga el servidor de Orchestrator desde la página **Opciones de inicio** en el centro de control.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

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.

4 Introduzca la contraseña que utilizó al exportar la configuración.

Este paso es innecesario si no exportó la configuración con una contraseña.

5 Haga clic en **Importar**.

6 Seleccione el tipo de archivos que desea importar.

IMPORTANTE: No utilice Forzar importación de complementos, a menos que desee que todos los complementos con versiones nuevas se sustituyan por versiones anteriores que podría contener el archivo exportado. Los complementos podrían dejar de funcionar debido a la incompatibilidad de versiones.

7 Haga clic en **Finalizar importación**.

Un mensaje indica que la configuración se ha importado correctamente. El nuevo sistema replica la configuración antigua por completo.

Qué hacer a continuación

- Compruebe que vRealize Orchestrator se haya configurado correctamente en la página **Validar configuración** del centro de control.
- Para que los cambios surtan efecto, reinicie el servidor de Orchestrator desde la página **Opciones de inicio** del centro de control.

Migrar la configuración de Orchestrator

La herramienta de migración de Orchestrator empaqueta las opciones de configuración, los complementos, las configuraciones de los complementos, los certificados y la información de la licencia en un archivo que puede importarse a vRealize Orchestrator 7.x.

Las opciones de línea de comandos siguientes se pueden utilizar con el comando `vro-migrate export`:

Opciónpacteracontextmathced	Descripciónpacteracontextmathced
`password`	Establezca una contraseña para proteger el archivo exportado. Si no se proporciona una contraseña, el archivo no está protegido.
`vroRootPath`	Especifique la ruta raíz del servidor de vRealize Orchestrator.

Migrar la configuración de Orchestrator desde Windows al dispositivo virtual

Migre la configuración independiente de 5.5.x y 6.x Orchestrator Windows a Orchestrator Appliance.

Prerequisitos

- Detenga los servidores de origen y destino de Orchestrator.
- Cree una copia de seguridad de la base de datos del servidor de origen de Orchestrator, incluido el esquema de la base de datos.

Procedimiento

1 Descargue la herramienta de migración desde el servidor de destino de Orchestrator.

   a Inicie sesión en el centro de control como **`raíz`**.

   b Abra la página **Exportar o importar configuración** y haga clic en la pestaña **Migrar configuración**.

   c Descargue la herramienta de migración como se especifica en la descripción de la página o directamente desde https://*nombre_DNS_o_IP_servidor_orchestrator*:8283/vco-controlcenter/api/server/migration-tool.

2 Exporte la configuración de Orchestrator desde el servidor de Orchestrator de origen.

   a Descomprima el archivo descargado y coloque la carpeta en la carpeta de instalación de Orchestrator.

     La ruta predeterminada de la carpeta de instalación de Orchestrator en una instalación basada en Windows es `C:\Archivos de programa\VMware\Orchestrator`.

   b Configure la variable de entorno `PATH` haciendo que apunte a la carpeta `bin` de la instancia de Java JRE que se instaló con Orchestrator.

   c Utilice el símbolo del sistema de Windows para ir hasta la carpeta `bin` en la carpeta de instalación de Orchestrator.

     De forma predeterminada, la ruta de la carpeta `bin` es `C:\Archivos de programa\VMware\Orchestrator\migration-cli\bin`.

   d Ejecute el comando `export` desde la línea de comandos.

     ```
     C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
     ```

     Este comando combina los archivos de configuración de VMware vRealize Orchestrator y los complementos en un archivo de exportación.

     El archivo se crea en la misma carpeta que la carpeta `migration-cli`.

3 Importe la configuración al servidor de destino de Orchestrator.

   a Abra **Exportar o importar configuración** en el centro de control y haga clic en la pestaña **Migrar configuración**.

   b Haga clic en **Importar**.

   c Seleccione el tipo de archivos que quiere importar.

     NOTA:

     Si los servidores de origen y de destino de Orchestrator están configurados para utilizar la misma base de datos externa, deje sin marcar la casilla **Migrar configuración de base de datos**. Así, el esquema de base de datos no se actualiza a la versión más reciente. De lo contrario, el entorno de origen de Orchestrator deja de funcionar.

   d Haga clic en **Finalizar migración**.

4 Si el vRealize Orchestrator de origen utiliza vRealize Automation como proveedor de autenticación, importe el certificado SSL del servidor de vRealize Automation al almacén de confianza de Orchestrator y cambie el proveedor de licencias en el servidor de destino de Orchestrator.

   a En la página **Certificados** del centro de control, haga clic en **Importar de URL**.

   b Proporcione la dirección URL del servidor de vRealize Automation.

   c Vaya a la página **Licencia** del centro de control.

   d En el menú desplegable **Seleccionar proveedor de licencias**, seleccione **Licencia de vRA**.

5 Si el vRealize Orchestrator de origen utiliza el modo de autenticación **vSphere** o **SSO (antiguo)**, cambie el proveedor de licencias a **Licencia manual** y proporcione la clave de licencia manual.

Un mensaje indica que la migración ha finalizado correctamente.

Qué hacer a continuación

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

- Para que los cambios surtan efecto, reinicie el servidor de Orchestrator desde la página **Opciones de inicio** del centro de control.

Migrar un clúster de instancias vRealize Orchestrator 6.x en Windows a un clúster de dispositivos virtuales vRealize Orchestrator 7.1 o 7.2

Puede migrar su clúster de instancias de vRealize Orchestrator 6.x instaladas en Windows a un clúster de dispositivos virtuales de vRealize Orchestrator, versión 7.1 o 7.2.

Prerequisitos

- Detenga el servicio del servidor de Orchestrator de las instancias de Orchestrator 6.x en el clúster.
- Haga una copia de seguridad de la base de datos, incluido el esquema de base de datos, del servidor externo de Orchestrator.
- Implemente un nodo de Orchestrator en la versión de destino. Para obtener más información, consulte "Descargar e implementar Orchestrator Appliance," página 23.

Procedimiento

1 Descargue la herramienta de migración desde el servidor de destino de Orchestrator.

   a Inicie sesión en el centro de control como **`raíz`**.

   b Abra la página **Exportar o importar configuración** y haga clic en la pestaña **Migrar configuración**.

   c Descargue la herramienta de migración como se especifica en la descripción o directamente desde https://*nombre_DNS_o_IP_servidor_orchestrator*:8283/vco-controlcenter/api/server/migration-tool.

2 Exporte la configuración de Orchestrator desde uno de los nodos del servidor de origen de Orchestrator.

   a Configure la variable de entorno `PATH` haciendo que apunte a la carpeta `bin` de la instancia de Java JRE que se instaló con Orchestrator.

   b Cargue la herramienta de migración en el servidor de Windows en el que está instalado el Orchestrator de origen.

   c Descomprima el archivo descargado y coloque la carpeta en la carpeta de instalación de Orchestrator.

   La ruta predeterminada de la carpeta de instalación de Orchestrator en una instalación basada en Windows es `C:\Archivos de programa\VMware\Orchestrator`.

   d Ejecute como administrador el símbolo del sistema de Windows y desplácese hasta la carpeta `bin` en la carpeta de instalación de Orchestrator.

   De forma predeterminada, la ruta de la carpeta `bin` es `C:\Archivos de programa\VMware\Orchestrator\migration-cli\bin`.

   e Ejecute el comando `export` desde la línea de comandos.

   ```
   C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
   ```

   Este comando combina los archivos de configuración de VMware vRealize Orchestrator y los complementos en un archivo de exportación.

   El archivo se crea en la misma carpeta que la carpeta `migration-cli`.

3 Importe la configuración al servidor de destino de Orchestrator.

   a Abra **Exportar o importar configuración** en el centro de control y haga clic en la pestaña **Migrar configuración**.

   b Desplácese hasta el archivo de configuración exportado y haga clic en **Importar**.

c Seleccione el tipo de archivos que quiere importar.

Opción	Descripción
Migrar configuración de base de datos	Utiliza la base de datos del clúster vRealize Orchestrator 6.x.
Migrar complementos	Migra todos los complementos que no están incluidos en la plataforma Orchestrator.
Migrar configuraciones de complementos antiguos	Migra la configuración de los complementos que se almacena en la carpeta *`carpeta_instalación_Orchestrator`*`\app-server\conf\plugins`.
Migrar certificados de confianza	Migra todos los certificados del almacén de confianza del clúster vRealize Orchestrator 6.x.

d Haga clic en **Finalizar migración**.

Un mensaje indica que la migración se completó correctamente.

4 Vuelva a configurar el clúster de Orchestrator.

a Abra la página avanzada **Administración de clústeres de Orchestrator** en https://*nombre_DNS_o_IP_servidor_orchestrator*:8283/vco-controlcenter/#/control-app/ha?remove-nodes.

b Seleccione las casillas de verificación junto a los nodos de Orchestrator 6.x y haga clic en **Quitar**.

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

Puede ignorar la advertencia `El clúster de Orchestrator se encuentra en estado inconsistente`, que desaparece cuando se inicia el servicio del servidor de Orchestrator.

d Si aparece un error de licencia, configure un proveedor de licencias adecuado en la página **Licencia** del centro de control.

5 En la página **Opciones de inicio** del centro de control, inicie el servicio del servidor de destino de Orchestrator.

a En la página **Opciones de inicio**, asegúrese de que las cadenas **Huella digital de configuración activa** y **Huella digital de configuración pendiente** coincidan.

NOTA: Puede que necesite actualizar la página **Opciones de inicio** varias veces hasta que coincidan ambas cadenas.

Ha migrado satisfactoriamente un clúster de vRealize Orchestrator 6.x a un clúster de dispositivos virtuales de Orchestrator de la versión 7.1 o 7.2.

Qué hacer a continuación

- Inicie sesión en el cliente de Orchestrator y compruebe que las configuraciones de todos los complementos instalados son correctas.
- Agregue más nodos al clúster de destino de Orchestrator. Para obtener más información, consulte "Configurar un clúster de Orchestrator," página 50.

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 registro	Cantidad de días que los eventos de registro del clúster se mantienen en la base de datos antes de purgarse.

Archivos de registro 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 registros 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 registro y de configuración de Orchestrator desde el menú **Exportar registros** del centro de control.

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

Nombre de archivo	Ubicación	Descripción
`scripting.log`	`/var/log/vco/app-server`	Proporciona mensajes de registro 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 registro cada 5 minutos.
`localhost_access_log.txt`	`/var/log/vco/app-server`	Registro de solicitudes HTTP del servidor.

Tabla 7-1. Lista de archivos de registro de Orchestrator (Continua)

Nombre de archivo	Ubicación	Descripción
`localhost_access_log.`*`fecha`*`.txt`	`/var/log/vco/configuration`	Registro de solicitudes HTTP del servicio del centro de control.
`controlcenter.log`	`/var/log/vco/configuration`	Archivo de registro 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.

ADVERTENCIA: 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

Puede utilizar el centro de control para generar un archivo ZIP de resolución de problemas con archivos de registro de configuración, servidor, contenedor e instalación.

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

Inspección de los registros del flujo de trabajo

Puede inspeccionar rápidamente y exportar los registros del sistema y del servidor de los flujos de trabajo finalizados en la página Inspeccionar flujos de trabajo del centro de control.

NOTA: Cuando utiliza Orchestrator como parte de un clúster, los registros del sistema se guardan solo en el nodo del servidor, desde el que se inicia el flujo de trabajo.

IMPORTANTE: La información de registro se guarda temporalmente.

- Los archivos del sistema se guardan en archivos de hasta 10 MB. El número máximo de archivos de registro es de 5 por nodo.
- Los registros de servidor se guardan durante 15 días en la base de datos.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Inspeccionar flujos de trabajo**.

3 Haga clic en la pestaña **Flujos de trabajo finalizados**.

4 (Opcional) Seleccione el tipo de tokens de flujo de trabajo que desee inspeccionar, seleccione el rango de fechas y haga clic en **Aplicar**.

5 (Opcional) Busque un flujo de trabajo por nombre, ID o ID de token.

6 Haga clic en el ID de token que desee inspeccionar.

La vista del registro de ejecución del flujo de trabajo aparece en la pantalla completa.

7 Inspeccione los registros del sistema y del servidor.

8 (Opcional) Haga clic en **Exportar registros de token** para exportar los registros de token del flujo de trabajo a un archivo `.zip`.

Filtrado de registros de Orchestrator

Puede filtrar los registros del servidor de Orchestrator para buscar una ejecución del flujo de trabajo específica y recopilar datos de diagnóstico sobre la ejecución del flujo de trabajo.

Los registros de Orchestrator contienen mucha información de utilidad que se 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 sobre cada ejecución del registro en directo de Orchestrator.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Secuencia de registro en directo**.

3 En la barra de búsqueda, introduzca los parámetros de búsqueda.

Por ejemplo, puede filtrar los registros por nombre de usuario, nombre de flujo de trabajo, ID de flujo de trabajo o ID de token.

4 (Opcional) Seleccione **Distinguir mayúsculas de minúsculas** y **Filtro (grep)** para filtrar aún más los resultados de la búsqueda.

Cuando se selecciona **Filtro (grep)**, el registro en directo solo muestra las líneas que coinciden con los parámetros de búsqueda.

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

Qué hacer a continuación

Si desea filtrar registros antiguos que no están accesibles a través de la página Secuencia de registro en directo del centro de control, puede utilizar herramientas de análisis de registro de terceros.

Migrar un servidor externo de Orchestrator a vRealize Automation 7.2

8

Puede migrar un servidor externo de Orchestrator a una instancia de vRealize Orchestrator integrada en vRealize Automation.

Puede implementar vRealize Orchestrator como instancia externa de servidor y configurar vRealize Automation para que funcione con esa instancia externa; también puede configurar y utilizar el servidor de vRealize Orchestrator que se incluye en vRealize Automation Appliance.

Con la versión de vRealize Automation 7.2, VMware le recomienda que migre su vRealize Orchestrator externo al servidor de Orchestrator que está integrado en vRealize Automation. La migración de una instancia externa al Orchestrator integrado proporciona las siguientes ventajas:

- Reduce el coste total de propiedad.
- Simplifica el modelo de implementación.
- Mejora la eficiencia operativa.

NOTA: Considere utilizar un vRealize Orchestrator externo en los casos siguientes:

- Varios arrendatarios en el entorno de vRealize Automation
- Entorno geográficamente disperso
- Manejo de la carga de trabajo
- Uso de complementos específicos, como el complemento Site Recovery Manager

Este capítulo cubre los siguientes temas:

Escenarios de migración

El procedimiento de migración de una instancia de vRealize Orchestrator externa a una de vRealize Orchestrator integrada en vRealize Automation varía según la configuración disponible. Existen diferentes escenarios de migración en función de si el servidor externo de Orchestrator está basado en Windows o es un dispositivo virtual, si utiliza una base de datos integrada o externa, entre otras condiciones. El proceso de migración se puede combinar con una actualización de vRealize Orchestrator, vRealize Automation o ambos. En este caso, el procedimiento de migración depende de las versiones de origen de los productos.

Matriz de escenario de migración

Puede elegir un escenario de migración en función de la implementación de origen.

Implementación de vRealize Orchestrator	Implementación de vRealize Automation	Escenario de migración
Dispositivo virtual de vRealize Orchestrator 6.0.3	vRealize Automation 6.2.3	"Migrar un dispositivo virtual vRealize Orchestrator 6.x externo a vRealize Automation 7.2," página 74
vRealize Orchestrator 6.0.4 en Windows	vRealize Automation 6.2.4	"Migrar un vRealize Orchestrator 6.x externo en Windows a vRealize Automation 7.2," página 72
Dispositivo virtual de vRealize Orchestrator 6.0.4	vRealize Automation 6.2.4	"Migrar un dispositivo virtual vRealize Orchestrator 6.x externo a vRealize Automation 7.2," página 74
Dispositivo virtual de vRealize Orchestrator 6.0.5	vRealize Automation 6.2.5	"Migrar un dispositivo virtual vRealize Orchestrator 6.x externo a vRealize Automation 7.2," página 74
Dispositivo virtual de vRealize Orchestrator 7.0 con una base de datos Oracle 12 c externa	vRealize Automation 7.0 o IaaS	"Migrar un vRealize Orchestrator 7.x externo a vRealize Automation 7.2," página 76
Dispositivo virtual de vRealize Orchestrator 7.0.1 con una base de datos PostgreSQL 9.3.9 externa	vRealize Automation 7.0.1 o IaaS	"Migrar un vRealize Orchestrator 7.x externo a vRealize Automation 7.2," página 76
Dispositivo virtual de vRealize Orchestrator 7.1	vRealize Automation 7.1	"Migrar un vRealize Orchestrator 7.x externo a vRealize Automation 7.2," página 76
Dispositivo virtual de vRealize Orchestrator 7.2	vRealize Automation 7.2	"Migrar un vRealize Orchestrator 7.x externo a vRealize Automation 7.2," página 76
vRealize Orchestrator 6.0.3 en Windows	vRealize Automation 6.2.3	"Migrar la configuración de Orchestrator desde Windows al dispositivo virtual," página 63

Migrar un vRealize Orchestrator 6.x externo en Windows a vRealize Automation 7.2

Después de actualizar vRealize Automation de la versión 6.x a la versión 7.2, puede migrar su Orchestrator 6.x externo existente instalado en Windows al servidor de Orchestrator que está integrado en vRealize Automation 7.2.

NOTA: Si tiene un entorno de vRealize Automation distribuido con varios nodos de vRealize Automation Appliance, realice el procedimiento de migración únicamente en el nodo principal de vRealize Automation.

Prerequisitos

- Actualice vRealize Automation de la versión 6.x a la versión 7.2.
- Detenga el servicio del servidor de Orchestrator del Orchestrator externo.
- Haga una copia de seguridad de la base de datos, incluido el esquema de base de datos, del servidor externo de Orchestrator.

NOTA: Si tiene pensado utilizar el entorno de Orchestrator de origen hasta el nuevo esté totalmente configurado, cree una copia de la base de datos de origen. De lo contrario, puede configurar el Orchestrator de destino para que utilice la misma base de datos, pero en tal caso, el entorno de Orchestrator de origen ya no funcionará debido a que el esquema de la base de datos se actualiza a la versión del Orchestrator de destino.

Procedimiento

1 Descargue la herramienta de migración desde el servidor de destino de Orchestrator.

   a Inicie sesión en vRealize Automation Appliance sobre SSH como **`raíz`**.

   b Descargue el archivo `migration-tool.zip` que se encuentra en el directorio `/var/lib/vco/downloads`.

2 Exporte la configuración de Orchestrator desde el servidor de Orchestrator de origen.

   a Configure la variable de entorno `PATH` haciendo que apunte a la carpeta `bin` de la instancia de Java JRE que se instaló con Orchestrator.

   b Cargue la herramienta de migración al servidor de Windows en el que está instalado el Orchestrator externo.

   c Descomprima el archivo descargado y coloque la carpeta en la carpeta de instalación de Orchestrator.

   La ruta predeterminada de la carpeta de instalación de Orchestrator en una instalación basada en Windows es `C:\Archivos de programa\VMware\Orchestrator`.

   d Ejecute como administrador el símbolo del sistema de Windows y desplácese hasta la carpeta `bin` en la carpeta de instalación de Orchestrator.

   De forma predeterminada, la ruta de la carpeta `bin` es `C:\Archivos de programa\VMware\Orchestrator\migration-cli\bin`.

   e Ejecute el comando `export` desde la línea de comandos.

   ```
   C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
   ```

   Este comando combina los archivos de configuración de VMware vRealize Orchestrator y los complementos en un archivo de exportación.

   El archivo se crea en la misma carpeta que la carpeta `migration-cli`.

3 Migre la configuración exportada al servidor de Orchestrator que está integrado en vRealize Automation 7.2.

   a Cargue el archivo de configuración exportado en el directorio `/usr/lib/vco/tools/configuration-cli/bin` de vRealize Automation Appliance.

   b En el directorio `/usr/lib/vco/tools/configuration-cli/bin`, cambie la propiedad del archivo de configuración del Orchestrator exportado.

   ```
   chown vco:vco orchestrator-config-export-dirección_IP_orchestrator-fecha_hora.zip
   ```

   c Importe el archivo de configuración de Orchestrator en el servidor integrado de vRealize Orchestrator; para ello, ejecute el script `vro-configure` con el comando `import`.

   ```
   ./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-IP_dispositivo_orchestrator-fecha_hora.zip
   ```

4 Migre la base de datos a la base de datos interna de PostgreSQL; para ello, ejecute el script `vro-configure` con el comando `db-migrate`.

   ```
   ./vro-configure.sh db-migrate --sourceJdbcUrl URL_conexión_JDBC --sourceDbUsername usuario_base_datos --sourceDbPassword contraseña_usuario_base_datos
   ```

   NOTA: Ponga las contraseñas que contienen caracteres especiales entre comillas.

   La *URL_conexión_JDBC* depende del tipo de base de datos que utiliza.

   ```
   PostgreSQL: jdbc:postgresql://host:puerto/nombre_base_datos
   ```

   ```
   MSSQL: jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\;domain=dominio
   ```

   ```
   Oracle: jdbc:oracle:thin:@host:puerto:base_datos
   ```

Se migró correctamente la vRealize Orchestrator 6.x externa instalada en Windows a una instancia de vRealize Orchestrator integrada en vRealize Automation 7.2.

Qué hacer a continuación

Configure el servidor integrado de vRealize Orchestrator. Consulte Capítulo 9, "Configure el servidor integrado de vRealize Orchestrator," página 79.

Migrar un dispositivo virtual vRealize Orchestrator 6.x externo a vRealize Automation 7.2

Después de actualizar el vRealize Automation desde la versión 6.x a la versión 7.2, puede migrar el dispositivo virtual Orchestrator 6.x externo al servidor de Orchestrator que está integrado en vRealize Automation 7.2.

NOTA: Si tiene un entorno de vRealize Automation distribuido con varios nodos de vRealize Automation Appliance, realice el procedimiento de migración únicamente en el nodo principal de vRealize Automation.

Prerequisitos

- Actualice vRealize Automation de la versión 6.x a la versión 7.2.
- Detenga el servicio del servidor de Orchestrator y el servicio del centro de control del Orchestrator externo.
- Haga una copia de seguridad de la base de datos, incluido el esquema de base de datos, del servidor externo de Orchestrator.

Procedimiento

1 Descargue la herramienta de migración desde el servidor de destino de Orchestrator al de origen.

   a Inicie sesión en el dispositivo virtual vRealize Orchestrator 6.x sobre SSH como **raíz**.

   b En el directorio `/var/lib/vco`, ejecute el comando `scp` para descargar el archivo `migration-tool.zip`.

   ```
   scp root@VRA-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
   ```

   c Ejecute el comando `unzip` para extraer el archivo de la herramienta de migración.

   ```
   unzip migration-tool.zip
   ```

2 Exporte la configuración de Orchestrator desde el servidor de Orchestrator de origen.

   a En el directorio `/var/lib/vco/migration-cli/bin`, ejecute el comando `export`.

   ```
   ./vro-migrate.sh export
   ```

   Este comando combina los archivos de configuración de VMware vRealize Orchestrator y los complementos en un archivo de exportación.

   Se crea un archivo con el nombre de archivo `orchestrator-config-export-`*`orchestrator_ip_address-date_hour`*`.zip` en la carpeta `/var/lib/vco`.

3 Migre la configuración exportada al servidor de Orchestrator que está integrado en vRealize Automation 7.2.

   a Inicie sesión en vRealize Automation Appliance sobre SSH como **raíz**.

   b En el directorio `/usr/lib/vco/tools/configuration-cli/bin`, ejecute el comando `scp` para descargar el archivo de configuración exportado.

   ```
   scp root@nombre_DNS_o_IP_orchestrator:/var/lib/vco/orchestrator-config-export-dirección_IP_orchestrator-fecha_hora.zip ./
   ```

   c Cambie la propiedad del archivo de configuración de Orchestrator exportado.

   ```
   chown vco:vco orchestrator-config-export-dirección_IP_orchestrator-fecha_hora.zip
   ```

   d Detenga el servicio del servidor de Orchestrator y el servicio del centro de control del servidor integrado de vRealize Orchestrator.

   ```
   service vco-server stop && service vco-configurator stop
   ```

   e Importe el archivo de configuración de Orchestrator en el servidor integrado de vRealize Orchestrator; para ello, ejecute el script `vro-configure` con el comando `import`.

   ```
   ./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-IP_dispositivo_orchestrator-fecha_hora.zip
   ```

4 Si el servidor externo de Orchestrator desde el que desea migrar utiliza la base de datos de PostgreSQL integrada, edite los archivos de configuración de la base de datos.

   a En el archivo `/storage/db/pgsql/data/postgresql.conf`, elimine la línea `listen_addresses`.

   b Establezca los valores de `listen_addresses` con un carácter comodín (*).

   ```
   listen_addresses ='*'
   ```

c Agregue una línea al archivo `/storage/db/pgsql/data/pg_hba.conf`.

```
host all all VRA-va-hostname.domain.name/32 md5
```

NOTA: El archivo `pg_hba.conf` requiere el uso de un formato de prefijo CIDR en lugar de una dirección IP y una máscara de subred.

d Reinicie el servicio del servidor de PostgreSQL.

```
service postgresql restart
```

5 Migre la base de datos a la base de datos interna de PostgreSQL; para ello, ejecute el script `vro-configure` con el comando `db-migrate`.

```
./vro-configure.sh db-migrate --sourceJdbcUrl URL_conexión_JDBC --sourceDbUsername
usuario_base_datos --sourceDbPassword contraseña_usuario_base_datos
```

NOTA: Ponga las contraseñas que contienen caracteres especiales entre comillas.

La *URL_conexión_JDBC* depende del tipo de base de datos que utiliza.

`PostgreSQL: jdbc:postgresql://host:puerto/nombre_base_datos`

`MSSQL: jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\;domain=dominio`

`Oracle: jdbc:oracle:thin:@host:puerto:base_datos`

6 Regrese a la configuración predeterminada de los archivos `postgresql.conf` y `pg_hba.conf`.

a Reinicie el servicio del servidor de PostgreSQL.

Se migró correctamente una instancia externa del dispositivo virtual vRealize Orchestrator 6.x a una instancia de vRealize Orchestrator integrada en vRealize Automation 7.2.

Qué hacer a continuación

Configure el servidor integrado de vRealize Orchestrator. Consulte Capítulo 9, "Configure el servidor integrado de vRealize Orchestrator," página 79.

Migrar un vRealize Orchestrator 7.x externo a vRealize Automation 7.2

Puede exportar la configuración de la instancia externa de Orchestrator e importarla al servidor de Orchestrator que está integrado en vRealize Automation.

NOTA: Si tiene varios nodos de vRealize Automation Appliance, realice el procedimiento de migración únicamente en el nodo principal de vRealize Automation.

Prerequisitos

- Actualice vRealize Automation de la versión 6.x a la versión 7.2.
- Detenga el servicio del servidor de Orchestrator del Orchestrator externo.
- Haga una copia de seguridad de la base de datos, incluido el esquema de base de datos, del servidor externo de Orchestrator.

Procedimiento

1 Exporte la configuración del servidor externo de Orchestrator.

a Inicie sesión en el centro del control del servidor externo de Orchestrator como **`raíz`**.

b Detenga el servicio del servidor de Orchestrator desde la página **Opciones de inicio** para prevenir cambios no deseados en la base de datos.

c Vaya a la página **Exportar o importar configuración**.

d En la página **Exportar configuración**, seleccione **Exportar configuración de servidor**, **Empaquetar complementos** y **Exportar configuraciones de complementos**.

2 Migre la configuración exportada a la instancia integrada de Orchestrator.

a Cargue el archivo de configuración de Orchestrator exportado en el directorio `/usr/lib/vco/tools/configuration-cli/bin` de vRealize Automation Appliance.

b Inicie sesión en vRealize Automation Appliance sobre SSH como **`raíz`**.

c Detenga el servicio del servidor de Orchestrator y el servicio del centro de control del servidor integrado de vRealize Orchestrator.

```
service vco-server stop && service vco-configurator stop
```

d Acceda al directorio `/usr/lib/vco/tools/configuration-cli/bin`.

e Cambie la propiedad del archivo de configuración de Orchestrator exportado.

```
chown vco:vco orchestrator-config-export-IP_dispositivo_orchestrator-fecha_hora.zip
```

f Importe el archivo de configuración de Orchestrator en el servidor integrado de vRealize Orchestrator; para ello, ejecute el script `vro-configure` con el comando `import`.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --
skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --
path orchestrator-config-export-IP_dispositivo_orchestrator-fecha_hora.zip
```

3 Migre la base de datos a la base de datos interna de PostgreSQL; para ello, ejecute el script `vro-configure` con el comando `db-migrate`.

```
./vro-configure.sh db-migrate --sourceJdbcUrl URL_conexión_JDBC --sourceDbUsername
usuario_base_datos --sourceDbPassword contraseña_usuario_base_datos
```

NOTA: Ponga las contraseñas que contienen caracteres especiales entre comillas.

La *URL_conexión_JDBC* depende del tipo de base de datos que utiliza.

```
PostgreSQL: jdbc:postgresql://host:puerto/nombre_base_datos
```

```
MSSQL: jdbc:jtds:sqlserver://host:puerto/nombre_base_datos\;domain=dominio
```

```
Oracle: jdbc:oracle:thin:@host:puerto:base_datos
```

Ha migrado correctamente una instancia externa del servidor de Orchestrator a una instancia de vRealize Orchestrator integrada en vRealize Automation.

Qué hacer a continuación

Configure el servidor integrado de vRealize Orchestrator. Consulte Capítulo 9, "Configure el servidor integrado de vRealize Orchestrator," página 79.

Configure el servidor integrado de vRealize Orchestrator 9

Después de exportar la configuración de un servidor externo de Orchestrator e importarla a vRealize Automation 7.2, debe configurar el servidor de Orchestrator integrado en vRealize Automation.

Prerequisitos

Migre la configuración del vRealize Orchestrator externo al interno.

Procedimiento

1 Inicie sesión en vRealize Automation Appliance sobre SSH como **raíz**.

2 Inicie el servicio del centro de control del servidor integrado de vRealize Orchestrator.

```
service vco-configurator start
```

3 Inicie sesión en el centro del control del servidor integrado de Orchestrator como **raíz**.

NOTA: Si migra desde una instancia externa de vRealize Orchestrator 7.2, vaya directamente al Step 8.

4 Vaya a la página avanzada Opciones de administración de Orchestrator en https://*vra-va-hostname.domain.name*:8283/vco-controlcenter/#/?advanced.

   a Actualice la página del navegador pulsando la tecla F5 del teclado.

5 En la página **Configurar base de datos**, haga clic en **Guardar**.

NOTA: Si el botón **Guardar** no está activo, haga clic en **Actualizar base de datos** y, a continuación, en **Guardar**.

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

7 En la página **Licencia**, seleccione **Licencia vRA** en el menú desplegable **Seleccionar proveedor de licencias**.

8 Si el Orchestrator externo se configuró para funcionar en modo de clúster, vuelva a configurar el clúster de Orchestrator en vRealize Automation.

   a Vaya a la página avanzada **Administración de clústeres de Orchestrator** en https://*vra-va-hostname.domain.name*:8283/vco-controlcenter/#/control-app/ha?advanced&remove-nodes.

   NOTA: Si no aparecen las casillas de verificación **Quitar** junto a los nodos existentes en el clúster, debe actualizar la página del navegador haciendo clic en el botón F5 del teclado.

   b En la página **Configuración de los nodos de Orchestrator**, cambie el valor de **Cantidad de nodos activos** a **10**.

c Si desea quitar algunos de los nodos externos de Orchestrator del clúster, seleccione las casillas de verificación junto a ellos y haga clic en **Quitar**.

d Para salir de la página avanzada de administración de clústeres, elimine la cadena `&remove-nodes` de la URL y actualice la página del navegador haciendo clic en el botón F5 del teclado.

e En la página **Validar configuración** del centro de control, compruebe que Orchestrator está configurado correctamente.

9 (Opcional) En la pestaña **Certificado de firma del paquete** de la página **Certificados**, genere un nuevo certificado de firma del paquete.

10 (Opcional) Cambie los valores del **Arrendatario predeterminado** y del **Grupo de administradores** en la página **Configurar proveedor de autenticación**.

11 En la página **Opciones de inicio**, inicie el servicio del servidor Orchestrator del servidor Orchestrator integrado en vRealize Automation.

12 Compruebe que el servicio de `vco-server` aparece como REGISTRADO en la pestaña **Servicios** de la consola de administración de vRealize Automation Appliance.

13 Seleccione los servicios de `vco` del servidor externo de Orchestrator y haga clic en **Eliminar del registro**.

Qué hacer a continuación

- Importe todos los certificados de confianza del servidor de Orchestrator externo al almacén de confianza del Orchestrator integrado. Para obtener más información, consulte "Administrar certificados de Orchestrator," página 45.
- Una los nodos de réplica de vRealize Automation al clúster de vRealize Automation para sincronizar la configuración de Orchestrator.
- Actualice el terminal de vRealize Orchestrator para que apunte al servidor de Orchestrator integrado que se migró.
- Agregue el host de vRealize Automation y de IaaS al inventario del complemento vRealize Automation mediante la ejecución de los flujos de trabajo Añadir un host de vRA y Añadir un host de IaaS.

Resolución de problemas y casos de uso de configuración 10

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 cubre los siguientes temas:

Registrar Orchestrator como extensión de vCenter Server

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

Procedimiento

1. Inicie sesión en el cliente de Orchestrator como administrador.
2. Haga clic en la vista **Flujos de trabajo**.
3. En la lista jerárquica de flujos de trabajo, expanda **Biblioteca > vCenter > Configuración**.
4. Haga clic con el botón derecho en el flujo de trabajo **Registro de vCenter Orchestrator como extensión de vCenter Server** y seleccione **Iniciar flujo de trabajo**.
5. Seleccione la instancia de vCenter Server con la que registrar Orchestrator.
6. Introduzca https://*dirección_IP_o_nombre_DNS_servidor_orchestrator*:8281 o la URL de servicio del equilibrador de carga que redirige las solicitudes a los nodos del servidor de Orchestrator.
7. Haga clic en **Enviar**.

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 **administrador**.

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**.

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.

Prerequisitos

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-lighttp restart
```

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

Cancelación de flujos de trabajo en ejecución

Cancele los flujos de trabajo cuando el servidor de Orchestrator esté detenido; de lo contrario, la operación podría no efectuarse correctamente.

Prerequisitos

Detenga el servidor de Orchestrator desde la página **Opciones de inicio** en el centro de control.

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Solución de problemas**.

3 Cancele los flujos de trabajo en ejecución.

Opción	Descripción
Cancelar todas las ejecuciones de flujos de trabajo	Escriba un ID de flujo de trabajo para cancelar todos los tokens de dicho flujo de trabajo. Si el servidor no se ha detenido, es posible que los tokens de flujo de trabajo no se cancelen.
Cancelar ejecuciones de flujos de trabajo por ID	Indique todos los ID de token que desee cancelar. Sepárelos con comas. Si el servidor no se ha detenido, es posible que los tokens de flujo de trabajo no se cancelen.
Cancelar todos los tokens	Cancele todos los flujos de trabajo en ejecución en el servidor. Es necesario detener el servidor para utilizar esta opción.

En el próximo inicio del servidor, los flujos de trabajo adoptarán el estado cancelado.

Qué hacer a continuación

Compruebe que los flujos de trabajo estén cancelados en la página **Inspeccionar flujos de trabajo** del 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 **administrador**.

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**.

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

Copia de seguridad de la configuración y los elementos de Orchestrator

Puede tomar un snapshot de su configuración de Orchestrator e importar dicha configuración a una nueva instancia de Orchestrator para realizar una copia de seguridad de la configuración de Orchestrator. También puede realizar una copia de seguridad de los elementos de Orchestrator que ha modificado.

Si edita los flujos de trabajo, las acciones, las políticas o los elementos de configuración estándar, y luego importa un paquete que contiene los mismos elementos con un número de versión de Orchestrator superior, se perderán los cambios en los elementos. Para que los elementos modificados y personalizados estén disponibles tras la actualización, debe exportarlos en un paquete antes de iniciar el procedimiento.

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

Procedimiento

1 Inicie sesión en el Centro de control como **administrador**.

2 Haga clic en **Exportar o importar configuración**.

3 Seleccione el tipo de archivos que quiere exportar.

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

  Utilice la misma contraseña cuando importe la configuración.

5 Haga clic en **Exportar**.

6 Inicie sesión en la aplicación de cliente de Orchestrator.

7 Cree un paquete que contenga todos los elementos de Orchestrator que haya creado o editado.

  a Haga clic en la vista **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 nuevo paquete y haga clic en **Aceptar**.

    La sintaxis de los nombres de paquetes es *`dominio.su_compañía.carpeta.nombre_paquete`*..

    Por ejemplo, `com.vmware.micarpeta.mipaquete`.

  d Haga clic con el botón derecho 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) Añada plantillas de políticas, acciones, elementos de configuración, elementos de recursos y complementos al paquete.

8 Exporte el paquete.

  a Haga clic con el botón derecho en el paquete que quiera exportar y seleccione **Exportar paquete**.

  b Busque y seleccione la ubicación donde vaya a guardar el paquete y haga clic en **Abrir**.

  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.

f Haga clic en **Guardar**.

9 Importe la configuración de Orchestrator a la nueva instancia de servidor de Orchestrator.

a Inicie sesión en Control Center de la nueva instancia de Orchestrator como **administrador**.

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 Haga clic en **Importar**.

10 Importe el paquete que ha exportado a la nueva instancia de Orchestrator.

a Inicie sesión en la aplicación de 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 vista **Paquetes**.

d Haga clic con el botón derecho en el panel izquierdo y seleccione **Importar paquete**.

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

Aparecerá información de certificado sobre el exportador.

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

Se abrirá la vista Importar paquete. Si la versión del elemento de paquete importado es posterior a la versión en el servidor, el sistema selecciona el elemento para importar.

g Anule la selección de los elementos que no desee importar.

Por ejemplo, anule la selección de los elementos personalizados para los que existan versiones posteriores.

h (Opcional) Anule la selección de la casilla **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, elija 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 sus valores.
No importar etiquetas	No importa las etiquetas del paquete.

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

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.

Antes de efectuar la copia de seguridad de toda la máquina virtual, puede exportar la base de datos. Para obtener información sobre cómo exportar la base de datos, consulte "Exportación de la base de datos de Orchestrator," página 44. Si vRealize Orchestrator y la base de datos externa están en equipos diferentes, la copia de seguridad de la base de datos debe efectuarse por separado.

NOTA: 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.

Prerequisitos

- 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**.

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

Qué hacer a continuación

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.

Si vRealize Orchestrator y la base de datos externa se ejecutan en máquinas diferentes, primero debe restaurar la base de datos y después la máquina virtual de vRealize Orchestrator.

Prerequisitos

- 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 *Administración de vSphere Data Protection*.
- Cree una copia de seguridad de la instancia de vRealize Orchestrator. Consulte "Copia de seguridad de vRealize Orchestrator," página 87.
- 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.

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

Qué hacer a continuación

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.

Prerequisitos

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**.

- 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 11

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

Este capítulo cubre los siguientes temas:

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 **administrador**.

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.

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 acceso de escritura al sistema Orchestrator

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

Contenido obligatorio del archivo js-io-rights.conf

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

- Un signo más (+) o un signo menos (–) para indicar si los derechos están permitidos o denegados
- Los niveles de derechos de lectura (`r`), escritura (`w`) y ejecución (`x`)
- La ruta en la que aplicar los derechos

Contenido predeterminado del archivo js-io-rights.conf

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

```
-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 `js-io-rights.conf` permiten los derechos de acceso siguientes:

`-rwx /`	Se deniega cualquier 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 del archivo js-io-rights.conf

Orchestrator resuelve los derechos de acceso en el orden en que aparecen en el archivo `js-io-rights.conf`. Cada línea reemplaza 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`. Ahora bien, esto comporta un riesgo elevado de seguridad.

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 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 Orchestrator.

Procedimiento

1 Inicie sesión en la consola de Linux de Orchestrator Appliance como **`raíz`**.

2 Vaya a `/etc/vco/app-server`.

3 Abra el archivo de configuración `js-io-rights.conf` en un editor de texto.

4 Añada las líneas pertinentes al archivo `js-io-rights.conf` para permitir o denegar el acceso a áreas del sistema de archivos.

Por ejemplo, la 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.

Ha modificado los derechos de acceso al sistema de archivos para flujos de trabajo y para la API de 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 **administrador**.

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**.

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.

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 **administrador**.

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.

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 **administrador**.

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.

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

Procedimiento a partir de aquí 12

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.

Inicie sesión en el cliente 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 de Orchestrator.

La interfaz del cliente 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 de Orchestrator están sincronizados.

Prerequisitos

- 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 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 de Orchestrator.

Si está utilizando la autenticación de vRealize Automation, vCenter Single Sign-On u otro servicio de directorio como método de autenticación, escriba las credenciales respectivas para iniciar sesión en el cliente de Orchestrator.

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

El cliente 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 el tema *Instalar y configurar VMware vRealize Orchestrator*.

Qué hacer a continuación

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

Índice

R

S

T

V