

Configuración de vRealize Automation

28 de diciembre de 2020

vRealize Automation 7.4

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

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

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

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

Copyright © 2015-2020 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Configurar vRealize Automation 6

Información actualizada 7

1 Preparaciones externas para el aprovisionamiento de blueprint 8

Preparar el entorno para la administración de vRealize Automation 8

Lista de comprobación para preparar la configuración de red y seguridad de NSX 10

Lista de comprobación para proporcionar soporte técnico del proveedor de IPAM de terceros 15

Lista de comprobación para la configuración de Contenedores para vRealize Automation 19

Preparar el entorno de vCloud Director para vRealize Automation 20

Preparar el entorno de vCloud Air para vRealize Automation 21

Preparar el entorno de Amazon AWS 21

Preparar funciones de red y seguridad de Red Hat OpenStack 29

Preparar el entorno de SCVMM 29

Configurar la conectividad VPC de red a Azure 30

Preparar el aprovisionamiento de máquinas 32

Elegir el método de aprovisionamiento de máquinas que se preparará 32

Lista de comprobación para ejecutar scripts de Visual Basic durante el aprovisionamiento 36

Usar el agente invitado de vRealize Automation durante el aprovisionamiento 38

Lista de comprobación para preparar el aprovisionamiento mediante clonación 46

Preparar el aprovisionamiento de vCloud Air y vCloud Director 60

Preparar el aprovisionamiento de Kickstart de Linux 62

Preparar el aprovisionamiento de SCCM 65

Preparar el aprovisionamiento de WIM 66

Preparar el aprovisionamiento de imágenes de máquina virtual 75

Preparar el aprovisionamiento de imágenes de máquina de Amazon 75

Escenario: Preparar recursos de vSphere para el aprovisionamiento de máquinas en Rainpole 78

Preparar el aprovisionamiento de Software 81

Preparar el aprovisionamiento de máquinas con Software 82

Escenario: Preparar una plantilla de CentOS de vSphere para los blueprints de componente de software y de máquina clonada 86

Escenario: Preparar la importación del blueprint de la aplicación de muestra Dukes Bank de vSphere 90

2 Preparación de tenants y recursos para el aprovisionamiento de blueprints 96

Configurar las opciones de tenant 96

Elegir opciones de configuración de Administración de directorios	97
Actualizar conectores externos para Administración de directorios	169
Escenario: Configurar un vínculo de Active Directory para vRealize Automation de alta disponibilidad	178
Configurar conectores externos para la autenticación del proveedor de identidades de terceros y la tarjeta inteligente en vRealize Automation	180
Crear un vínculo de Active Directory con varios dominios o bosques	189
Configurar funciones de usuarios y grupos	191
Crear tenants adicionales	198
Eliminar un tenant	201
Configurar los ajustes de seguridad para varios tenants	201
Configurar la personalización de marca	202
Lista de comprobación para la configuración de notificaciones	205
Crear un archivo RDP personalizado para admitir conexiones RDP para máquinas aprovisionadas	217
Escenario: Añadir ubicaciones de centros de datos para implementaciones en varias regiones	218
Configurar vRealize Orchestrator	219
Configurar recursos	225
Lista de comprobación para la configuración de recursos de IaaS	225
Configurar recursos de XaaS	361
Crear y configurar contenedores	375
Instalar complementos adicionales en el servidor predeterminado de vRealize Orchestrator	396
Trabajar con políticas de Active Directory	396
Preferencias del usuario para notificaciones y delegados	400

3 Proporcionar blueprints de servicio a los usuarios 401

Diseñar blueprints	401
Crear la biblioteca de diseño	404
Diseñar blueprints de máquinas	407
Diseñar componentes de Software	507
Diseñar acciones personalizadas y blueprints XaaS	522
Publicar un blueprint	589
Trabajar con blueprints de desarrollador	590
Exportar e importar blueprints y contenido	590
Descargar y configurar el blueprint independiente proporcionado	598
Crear blueprints y otros contenidos de IaaS en un entorno de varios desarrolladores	598
Ensamblar blueprints compuestos	599
Información sobre el comportamiento de blueprint anidado	601
Usar componentes de máquina y componentes de Software al ensamblar un blueprint	604
Crear enlaces de propiedad entre componentes de blueprint	606
Crear dependencias y controlar el orden de aprovisionamiento	607

Personalizar formularios de solicitud de blueprint	608
Crear un formulario de solicitud personalizado con opciones de Active Directory	611
Propiedades de campos del diseñador de formularios personalizados	622
Usar acciones de vRealize Orchestrator en el diseñador de formularios personalizados	628
Usar el elemento de cuadrícula de datos en el diseñador de formularios personalizados	630
Uso de la validación externa en el diseñador de formularios personalizados	633
Administrar el catálogo de servicios	637
Lista de comprobación para configurar el catálogo de servicios	638
Crear un servicio	639
Trabajar con elementos del catálogo y acciones	642
Crear autorizaciones	645
Trabajar con políticas de aprobación	654
Solicitar el aprovisionamiento de máquinas a través de un blueprint parametrizado	683
Escenario: Hacer que el blueprint de aplicación CentOS con MySQL esté disponible en el catálogo de servicios	685
Administrar los elementos de catálogo implementados	689
Ejecutar acciones en recursos aprovisionados	690
Especificar los ajustes de reconfiguración de máquinas y consideraciones de reconfiguración	716
Reconfigurar un equilibrador de carga en una implementación	723
Cambiar las reglas NAT en una implementación	725
Agregar o quitar elementos de seguridad en una implementación	727
Mostrar todas las reglas NAT de una instancia de NSX Edge existente	728

Configurar vRealize Automation

Configuración de vRealize Automation proporciona información sobre la configuración de vRealize Automation y sus entornos externos para preparar el aprovisionamiento de vRealize Automation y la administración de catálogos.

Público objetivo

Esta información está destinada a los profesionales informáticos responsables de la configuración del entorno de vRealize Automation y a los administradores de infraestructuras responsables de preparar elementos en su infraestructura existente para su uso en el aprovisionamiento de vRealize Automation. La información se ha escrito para los administradores de sistemas Windows y Linux con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Glosario de publicaciones técnicas de VMware

El departamento de Publicaciones técnicas de VMware ofrece un glosario con términos que quizá usted desconozca. Para consultar las definiciones de términos tal como se utilizan en la documentación técnica de VMware, visite <http://www.vmware.com/es/support/pubs>.

Información actualizada

Configuración de vRealize Automation se actualiza con cada versión del producto o cuando sea necesario.

Esta tabla muestra el historial de actualizaciones de *Configuración de vRealize Automation*.

Revisión	Descripción
16 de noviembre de 2018	Modificaciones menores.
5 de octubre de 2018	Modificaciones menores.
15 de junio de 2018	<ul style="list-style-type: none">■ Se ha actualizado Configurar una conexión del directorio OpenLDAP■ Se ha actualizado Configurar Administración de directorios para alta disponibilidad y se ha añadido Habilitar la sincronización de directorios en un conector secundario para proporcionar más información sobre cómo trabajar con conectores en una configuración de alta disponibilidad.■ Se ha actualizado Crear un endpoint de Puppet.■ Modificaciones menores.
3 DE MAYO DE 2018	<ul style="list-style-type: none">■ Modificaciones menores.■ Se añadió información sobre Regiones admitidas de Azure.
12 DE ABRIL DE 2018	Versión inicial.

Preparaciones externas para el aprovisionamiento de blueprint

1

Puede que necesite crear o preparar algunos elementos fuera de vRealize Automation para admitir el aprovisionamiento de elementos de catálogo. Por ejemplo, si desea proporcionar un elemento de catálogo para aprovisionar una máquina clonada, debe crear una plantilla en el hipervisor a partir de la cual se realizará la clonación.

Este capítulo incluye los siguientes temas:

- [Preparar el entorno para la administración de vRealize Automation](#)
- [Configurar la conectividad VPC de red a Azure](#)
- [Preparar el aprovisionamiento de máquinas](#)
- [Preparar el aprovisionamiento de Software](#)

Preparar el entorno para la administración de vRealize Automation

En función de la plataforma de integración, es posible que deba realizar algunos cambios de configuración para preparar el entorno para la administración de vRealize Automation o para aprovechar ciertas características.

Tabla 1-1. Preparar el entorno para la integración de vRealize Automation







Entorno	Preparativos
	<p>Si desea aprovechar NSX para administrar las características de redes y seguridad de las máquinas aprovisionadas con vRealize Automation, prepare la instancia de NSX para la integración. Consulte Lista de comprobación para preparar la configuración de red y seguridad de NSX.</p>
 vCloud Director	<p>Instale y configure la instancia de vCloud Director, establezca los recursos de vSphere y de nube, e identifique o cree las credenciales apropiadas para que vRealize Automation pueda acceder al entorno de vCloud Director. Consulte Preparar el entorno de vCloud Director para vRealize Automation.</p>
 vCloud Air	<p>Registre la cuenta de vCloud Air, configure el entorno de vCloud Air, e identifique o cree las credenciales apropiadas para que vRealize Automation pueda acceder al entorno. Consulte Preparar el aprovisionamiento de vCloud Air y vCloud Director.</p>
 Amazon AWS	<p>Prepare los elementos y las funciones de usuario en su entorno de Amazon AWS para usarlos en vRealize Automation y comprender cómo se asignan las características de Amazon AWS a las características de vRealize Automation. Consulte Preparar el entorno de Amazon AWS.</p>
Microsoft Azure	<p>Configure redes para utilizar los túneles VPN y admitir componentes de software en los blueprints de Azure. Consulte Configurar la conectividad VPC de red a Azure.</p>
 Red Hat OpenStack	<p>Si desea aprovechar Red Hat OpenStack para administrar las características de redes y seguridad de las máquinas aprovisionadas con vRealize Automation, prepare la instancia de Red Hat OpenStack para la integración. Consulte Preparar funciones de red y seguridad de Red Hat OpenStack.</p>
 SCVMM	<p>Configure el almacenamiento y las redes, y familiarícese con las restricciones de asignación de nombres de plantillas y perfiles de hardware. Consulte Preparar el entorno de SCVMM.</p>

Tabla 1-1. Preparar el entorno para la integración de vRealize Automation (continuación)

Entorno	Preparativos
Proveedores de IPAM externos	Registre un complemento o paquete de proveedores de IPAM externos, ejecute los flujos de trabajo de configuración y registre la solución de IPAM como un nuevo endpoint de vRealize Automation. Consulte Lista de comprobación para proporcionar soporte técnico del proveedor de IPAM de terceros .
Todos los demás entornos	No es necesario realizar cambios en el entorno. Para preparar el aprovisionamiento de máquinas, cree plantillas, entornos de arranque o imágenes de máquina. Consulte Preparar el aprovisionamiento de máquinas .

Lista de comprobación para preparar la configuración de red y seguridad de NSX

Antes de poder usar las opciones de red y seguridad de NSX en vRealize Automation, debe configurar el entorno de red y seguridad de NSX que pretende utilizar.

A partir de vRealize Automation 7.3, ya no se necesita instalar el complemento de NSX para obtener la funcionalidad integrada de NSX. Toda la funcionalidad integrada de NSX se obtiene directamente desde las instancias de NSX API, en lugar de obtenerla desde el complemento de NSX. Sin embargo, si desea utilizar XaaS para ampliar su integración de vRealize Automation y NSX, debe instalar el complemento de vRealize Orchestrator en NSX tal como se describe aquí.

Para usar las capacidades del equilibrador de carga, la seguridad y la red de NSX en vRealize Automation, cuando se utilizan las credenciales de NSX Manager debe utilizar la cuenta de administrador de NSX Manager.

Para obtener información relacionada sobre NSX, consulte la documentación de NSX en https://www.vmware.com/support/pubs/nsx_pubs.html y los blogs públicos y artículos, como [Integrar NSX con vRealize Automation](#).

La mayor parte del soporte de la configuración de red y seguridad de vRealize Automation que se especifica en los blueprints y las reservas se configura de forma externa y se pone a disposición de vRealize Automation tras ejecutar la recopilación de datos en los recursos del equipo.

Para obtener más información sobre la configuración de NSX que puede establecer para los blueprints de vRealize Automation, consulte [Configurar opciones del componente de red y seguridad](#).

Tabla 1-2. Preparación de la lista de comprobación de red y seguridad de NSX

Tarea	Ubicación	Detalles
<input type="checkbox"/> Establecer la configuración de red de NSX, incluida la configuración de puerta de enlace y zona de transporte.	Configure los ajustes de red en NSX.	Consulte la <i>Guía de administración de NSX</i> .
<input type="checkbox"/> Crear políticas de seguridad, etiquetas y grupos de NSX.	Configure los ajustes de seguridad en NSX.	Consulte la <i>Guía de administración de NSX</i> .
<input type="checkbox"/> Establecer la configuración de equilibrador de carga de NSX.	Configure un equilibrador de carga de NSX para que funcione con vRealize Automation.	Consulte la <i>Guía de administración de NSX</i> . Consulte también Propiedades personalizadas de redes en <i>Referencia de propiedades personalizadas</i> .
<input type="checkbox"/> Para implementaciones de centros virtuales cruzados, compruebe que el administrador de equipos de NSX tiene la función de administrador principal de NSX.	El aprovisionamiento de vRealize Automation requiere que el administrador de equipos de NSX para la región en la que residen las máquinas tenga la función de administrador principal de NSX.	Consulte Requisitos del administrador para el aprovisionamiento de objetos universales de NSX . Consulte las guías <i>NSX Installation Guide</i> y <i>NSX Administration Guide</i> para obtener información sobre la implementación de centros virtuales cruzados, objetos universales y la función de administrador principal de NSX.

Instalar el complemento de NSX en vRealize Orchestrator

Para instalar el complemento de NSX, hay que descargar el archivo del instalador de vRealize Orchestrator, usar la interfaz de configuración de vRealize Orchestrator para cargar el archivo de complemento y, por último, instalar dicho complemento en un servidor de vRealize Orchestrator.

Para obtener información general sobre cómo solucionar problemas de complementos o cómo actualizarlos, consulte la documentación sobre vRealize Orchestrator https://www.vmware.com/support/pubs/orchestrator_pubs.html.

Requisitos previos

A partir de vRealize Automation 7.3, ya no se necesita instalar el complemento de NSX para obtener la funcionalidad integrada de NSX. Toda la funcionalidad integrada de NSX se obtiene directamente desde las instancias de NSX API, en lugar de obtenerla desde el complemento de NSX. Sin embargo, si desea utilizar XaaS para ampliar su integración de vRealize Automation y NSX, debe instalar el complemento de vRealize Orchestrator en NSX tal como se describe aquí.

Si utiliza una instancia integrada de vRealize Orchestrator que ya contiene un complemento de NSX instalado, puede omitir este procedimiento.

- Confirme que ejecuta una instancia de vRealize Orchestrator compatible.
Para obtener información sobre cómo configurar vRealize Orchestrator, consulte el tema de *instalación y configuración de VMware vRealize Orchestrator*.
- Compruebe que posee credenciales de una cuenta con permiso para instalar complementos de vRealize Orchestrator y para autenticarse mediante vCenter Single Sign-On.
- Compruebe que ha instalado el cliente de vRealize Orchestrator y que puede iniciar sesión con credenciales de administrador.
- Confirme cuál es la versión correcta del complemento de NSX en la [matriz de compatibilidad](#) de vRealize Automation.

Procedimiento

- 1 Descargue el archivo de complemento en una ubicación a la que se pueda acceder desde el servidor de vRealize Orchestrator.

El formato de nombre de archivo del instalador del complemento es, con los valores de versión correspondientes, `o11nplugin-nsx-1.n.n.vmoapp`. Los archivos de instalación del complemento para la conexión de red y la seguridad de NSX están disponibles en el sitio de descargas del producto de VMware en <http://vmware.com/web/vmware/downloads>.
- 2 Abra un navegador e inicie la interfaz de configuración de vRealize Orchestrator.

Un ejemplo de formato de URL es `https://orchestrator_server.com:8283`.
- 3 Haga clic en **Complementos** en el panel izquierdo y desplácese a la sección Instalar nuevo complemento.
- 4 En el cuadro de texto **Archivo de complemento**, vaya al archivo del instalador de complemento y haga clic en **Cargar e instalar**.

El archivo debe tener el formato `.vmoapp`.
- 5 Cuando se le solicite, acepte el acuerdo de licencia en el panel Instalar un complemento.
- 6 En la sección Estado de instalación de complementos habilitados, confirme que se especifica el nombre de complemento de NSX correcto.

Consulte *Matriz de soporte de vRealize Automation* para obtener información de la versión.

Se muestra el estado El complemento se instalará en el siguiente inicio de servidor.
- 7 Reinicie el servicio de servidor de vRealize Orchestrator.
- 8 Reinicie la interfaz de configuración de vRealize Orchestrator.
- 9 Haga clic en **Complementos** y confirme que el estado ha cambiado a **Instalación correcta**.

- 10 Abra la aplicación de cliente de vRealize Orchestrator, inicie sesión y use la pestaña **Flujo de trabajo** para desplazarse por la biblioteca hasta llegar a la carpeta NSX.

Puede desplazarse por los flujos de trabajo que el complemento de NSX proporciona.

Pasos siguientes

Cree un endpoint de vRealize Orchestrator en vRealize Automation para usarlo para ejecutar flujos de trabajo. Consulte [Crear un endpoint de vRealize Orchestrator](#).

Ejecutar un flujo de trabajo de seguridad de vRealize Orchestrator y NSX

Para poder usar las funciones de política de seguridad de NSX desde vRealize Automation, un administrador debe ejecutar el flujo de trabajo **Enable security policy support for overlapping subnets** en vRealize Orchestrator.

La compatibilidad de políticas de seguridad en el flujo de trabajo de subredes superpuestas es válida en endpoints de NSX 6.1 en adelante. Ejecute este flujo de trabajo una sola vez para permitir esta compatibilidad.

Requisitos previos

- Confirme que hay un endpoint de vSphere registrado con un endpoint de NSX. Consulte [Crear un endpoint de vSphere](#).
- Inicie sesión en el cliente de vRealize Orchestrator como administrador.
- Compruebe que ha ejecutado el flujo de trabajo de vRO **Create NSX endpoint**.

Procedimiento

- 1 Haga clic en la pestaña **Flujo de trabajo** y seleccione **NSX > Flujos de trabajo de NSX para VCAC**.
- 2 Ejecute el flujo de trabajo **Crear extremo de NSX** y responda los mensajes.
- 3 Ejecute el flujo de trabajo **Permitir compatibilidad de política de seguridad en subredes superpuestas**.
- 4 Seleccione el endpoint de NSX como parámetro de entrada del flujo de trabajo.

Use la dirección IP que especificó al crear el endpoint de vSphere para registrar una instancia de NSX.

Resultados

Tras ejecutar este flujo de trabajo, las reglas de cortafuegos distribuido definidas en la política de seguridad se aplicarán únicamente en las vNIC de los miembros del grupo de seguridad que esta política de seguridad rige.

Pasos siguientes

Aplicar las funciones de seguridad correspondientes al blueprint.

Requisitos del administrador para el aprovisionamiento de objetos universales de NSX

Para aprovisionar máquinas en un entorno de Cross-vCenter NSX al utilizar objetos universales de NSX, debe aprovisionar una instancia de vCenter en la que el administrador informático de NSX tenga la función principal.

En un entorno de Cross-vCenter NSX, puede haber varias instancias de vCenter Server, cada una emparejada con su propia instancia de NSX Manager. A una instancia de NSX Manager se le asigna la función de instancia principal de NSX Manager y a las otras se les asigna la función de instancia secundaria de NSX Manager.

La instancia principal de NSX Manager puede crear objetos universales, como conmutadores lógicos universales. Estos objetos se sincronizan con las instancias secundarias de NSX Manager. Puede ver los objetos desde las instancias secundarias de NSX Manager, pero no puede editarlos allí. Debe utilizar la instancia principal de NSX Manager para administrar objetos universales. La instancia principal de NSX Manager puede utilizarse para configurar cualquiera de las instancias secundarias de NSX Manager en el entorno.

Para obtener más información sobre el entorno de Cross-vCenter NSX, consulte *Descripción general de Cross-vCenter Networking and Security* en la *guía de administración de NSX* de la [documentación del producto de NSX](#).

Para un endpoint de vSphere (vCenter) que está asociado al endpoint de NSX de una instancia principal de NSX Manager, vRealize Automation es compatible con los objetos locales de NSX, como conmutadores lógicos locales y puertas de enlace de Edge locales, así como grupos de seguridad, etiquetas de seguridad y equilibradores de carga locales. También es compatible con redes NAT uno a uno y uno a muchos con zona de transporte universal, redes enrutadas con zona de transporte universal y enrutadores lógicos distribuidos (Distributed Logical Router, DLR) universales y un equilibrador de carga con cualquier tipo de red.

vRealize Automation no admite etiquetas ni grupos de seguridad universales de NSX existentes y a petición.

Para aprovisionar redes a petición locales como la instancia principal de NSX Manager, utilice una zona de transporte local específica de vCenter. Puede configurar reservas de vRealize Automation para usar la zona de transporte local y los cables virtuales para las implementaciones en esa instancia local de vCenter.

Si se conecta un endpoint de vSphere (vCenter) a un endpoint secundario de NSX Manager correspondiente, solo puede aprovisionar y usar los objetos locales.

Un endpoint de NSX solo puede asociarse con un endpoint de vSphere. Esta restricción de asociación significa que no se puede aprovisionar una red a petición universal y asociarla a máquinas vSphere que se aprovisionan en diferentes instancias de vCenter.

vRealize Automation puede consumir un conmutador lógico universal de NSX como una red externa. Si existe un conmutador universal, se recopilan sus datos y, a continuación, se conecta a cada máquina de la implementación, o bien cada una de estas lo consume.

- El aprovisionamiento de una red a petición a una zona de transporte universal puede crear un nuevo conmutador lógico universal.
- El aprovisionamiento de una red a petición a una zona de transporte universal en la instancia principal de NSX Manager crea un conmutador lógico universal.
- El aprovisionamiento de una red a petición a una zona de transporte universal en una instancia secundaria de NSX Manager genera un error, ya que NSX no puede crear un conmutador lógico universal en una instancia secundaria de NSX Manager.

Consulte el artículo de la base de conocimientos de VMware en el que se discute el *error en la implementación de blueprints de vRealize Automation con objetos de NSX (2147240)* en <http://kb.vmware.com/kb/2147240> para obtener más información sobre los objetos universales de NSX.

Lista de comprobación para proporcionar soporte técnico del proveedor de IPAM de terceros

Puede obtener direcciones IP y rangos para usarlos en la definición de perfil de red de un proveedor de IPAM de terceros compatible, como Infoblox.

Para crear y usar un endpoint de proveedor de IPAM externo en un perfil de red de vRealize Automation, debe descargar u obtener de otro modo un complemento o un paquete de proveedor de IPAM de vRealize Orchestrator, importar el complemento o el paquete, y ejecutar los flujos de trabajo necesarios en vRealize Orchestrator; a continuación, debe registrar la solución de IPAM como un endpoint de vRealize Automation.

Para ver una descripción general del proceso de aprovisionamiento para usar un proveedor de IPAM externo con el fin de suministrar un rango de posibles direcciones IP, consulte [Aprovisionamiento de una implementación de vRealize Automation con un proveedor de IPAM de terceros](#).

Tabla 1-3. Lista de comprobación para preparar la compatibilidad con proveedores de IPAM externos

Tarea	Descripción	Detalles
<input type="checkbox"/> Obtenga e importe el complemento de vRealize Orchestrator del proveedor de IPAM externo compatible.	<p>Descargue el complemento o el paquete del proveedor de IPAM, por ejemplo la documentación de soporte y del complemento Infoblox IPAM para vRealize Orchestrator, en VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_groups/cloud-management), e importe el complemento o el paquete en vRealize Orchestrator.</p> <p>Si VMware Solution Exchange no contiene el paquete del proveedor de IPAM que usted necesita, podrá crear uno propio con el SDK del proveedor de la solución IPAM de terceros y con la documentación de soporte.</p> <p>En https://code.vmware.com/sdks o https://code.vmware.com/samples, encontrará un SDK del proveedor de la solución IPAM de terceros específico para la versión de vRealize Automation, documentación de soporte y el paquete de inicio asociado de vRealize Orchestrator y vRealize Automation.</p>	<p>Consulte Obtención e importación de un paquete de proveedores de IPAM de terceros en vRealize Orchestrator.</p>
<input type="checkbox"/> Ejecute los flujos de trabajo de configuración necesarios y registre la solución de IPAM externa como un endpoint de vRealize Automation.	<p>Ejecute los flujos de trabajo de configuración de vRealize Orchestrator y registre el tipo de endpoint de proveedor de IPAM en vRealize Orchestrator.</p>	<p>Consulte Ejecutar el flujo de trabajo para registrar un tipo de endpoint de IPAM de terceros en vRealize Orchestrator.</p>

Obtención e importación de un paquete de proveedores de IPAM de terceros en vRealize Orchestrator

Para poder definir y usar un endpoint de proveedor de IPAM de terceros, primero debe obtener el paquete de proveedores de IPAM de terceros e importar el paquete en vRealize Orchestrator.

Puede descargar y usar un complemento existente de proveedores de administración de direcciones IP de terceros, como Infoblox IPAM. También puede crear su propio complemento o paquete de IPAM de terceros utilizando el paquete de inicio suministrado por VMware y la documentación de SDK complementaria para utilizarlo con otro proveedor de soluciones IPAM de terceros, como BlueCat.

- Obtenga el complemento [Infoblox IPAM para vRealize Orchestrator](#) existente y documentación complementaria en marketplace.vmware.com. La descarga también contiene documentación para instalar y utilizar el complemento.

- Cree su propia solución IPAM de terceros mediante la obtención y el uso de un SDK de proveedor de soluciones IPAM de terceros, la documentación de soporte y un paquete de inicio asociado para vRealize Orchestrator y vRealize Automation. Consulte la página [Paquete de IPAM de terceros de ejemplo de vRealize Automation](#) en code.vmware.com/web/sdk.

Después de importar el complemento o el paquete del proveedor de IPAM de terceros en vRealize Orchestrator, ejecute los flujos de trabajo necesarios y registre el tipo de endpoint de IPAM en vRealize Orchestrator.

Para obtener más información sobre la importación de complementos y paquetes y la ejecución de flujos de trabajo de vRealize Orchestrator, consulte el tema sobre el *uso del cliente de VMware vRealize Orchestrator*. Para obtener más información sobre cómo ampliar vRealize Automation con flujos de trabajo, complementos y paquetes de vRealize Orchestrator, consulte *Extensibilidad del ciclo de vida*.

Esta secuencia de pasos utiliza el complemento Infoblox IPAM como un ejemplo. La secuencia de pasos puede variar según la versión de vRealize Automation o del complemento.

Requisitos previos

- Descargue el paquete o el complemento desde marketplace.vmware.com.
- Inicie sesión en vRealize Orchestrator con privilegios de administrador para importar, configurar y registrar un complemento o un paquete de vRealize Orchestrator.

Procedimiento

- 1 Abra el sitio marketplace.vmware.com.
- 2 Busque y descargue el complemento o paquete.

Por ejemplo, importe el complemento de Infoblox que admite el endpoint de IPAM de terceros de Infoblox en vRealize Orchestrator y vRealize Automation 7.1 o versiones posteriores.

- a En la categoría **Publicador**, seleccione **Infoblox** y haga clic en **Aplicar**.
- b Seleccione [el complemento de Infoblox para vRealize Orchestrator](#).
- c Haga clic en las **Especificaciones técnicas** y revise los requisitos previos.
- d Haga clic en **Probar** para obtener información adicional y recibir un correo electrónico que contiene un vínculo de descarga.
- e Descargue el archivo ZIP tal como se especifica en las instrucciones del correo electrónico.

La versión 4.0 y las versiones posteriores del complemento son compatibles con vRealize Automation 7.1 y versiones posteriores. El archivo zip también contiene documentación sobre el complemento.

- 3 En vRealize Orchestrator, haga clic en la pestaña **Administrador** y luego haga clic en **Importar paquete**.

- 4 Seleccione el paquete que se importará.
- 5 Seleccione todos los flujos de trabajo y artefactos y haga clic en **Importar elementos seleccionados**.

Pasos siguientes

[Ejecutar el flujo de trabajo para registrar un tipo de endpoint de IPAM de terceros en vRealize Orchestrator](#).

Ejecutar el flujo de trabajo para registrar un tipo de endpoint de IPAM de terceros en vRealize Orchestrator

Ejecute el flujo de trabajo de registro en vRealize Orchestrator para permitir que vRealize Automation use el proveedor de IPAM de terceros y registre el tipo de endpoint de IPAM para usarlo en vRealize Automation.

Requisitos previos

- [Obtención e importación de un paquete de proveedores de IPAM de terceros en vRealize Orchestrator](#)
- Compruebe que ha iniciado sesión en vRealize Orchestrator con permiso para ejecutar flujos de trabajo de registro.
- Prepárese para introducir las credenciales de administrador de vRealize Automation cuando se lo solicite el flujo de trabajo de registro. Cuando registre los tipos de endpoint de IPAM en vRealize Orchestrator, se le pedirá que introduzca las credenciales de administrador de vRealize Automation.

Procedimiento

- 1 En vRealize Orchestrator, haga clic en la pestaña **Diseño**, seleccione **Administrador > Biblioteca** y seleccione **IPAM Service Package SDK**.

Cada paquete de proveedor de IPAM tiene un nombre exclusivo y contiene flujos de trabajo únicos. Cada proveedor suministra su propio flujo de trabajo de registro. Aunque los nombre del flujo de trabajo pueden ser similares entre paquetes de proveedores, la ubicación de los flujos de trabajo en vRealize Orchestrator puede ser diferente y es específica de cada proveedor.

- 2 Por ejemplo, ejecute el flujo de trabajo de registro de **Register IPAM Endpoint** y especifique el tipo de endpoint de Infoblox IPAM.

- 3 En la solicitud de credenciales de vRealize Automation, introduzca las credenciales de administrador de vRealize Automation (por ejemplo, las credenciales de administrador de tejido).

Debe proporcionar al flujo de trabajo de registro las credenciales de administrador del sistema de vRealize Automation. Aunque un usuario que no sea administrador del sistema haya iniciado sesión en el cliente de vRealize Orchestrator, si se proporcionan las credenciales de administrador del sistema de vRealize Automation al flujo de trabajo, el registro se realizará correctamente.

Resultados

En este ejemplo, el paquete registra Infoblox como un nuevo tipo de endpoint de IPAM en el servicio de endpoints de vRealize Automation y hace que el tipo de endpoint esté disponible al crear o editar endpoints en vRealize Automation.

Nota Puede que la conexión de Infoblox IPAM desaparezca de la pestaña **Inventario** de vRealize Orchestrator después de reiniciar el servidor vRealize Orchestrator en el centro de control de vRealize Orchestrator. Para resolver este problema, ejecute el flujo de trabajo **Create IPAM Connection** desde la secuencia de menú **vRO admin > Biblioteca > Infoblox > vRA > Asistentes**. Luego, en la pestaña **Inventario** de vRealize Orchestrator, seleccione **Infoblox IPAM** y actualice la página para que muestre la conexión de Infoblox IPAM.

Pasos siguientes

Ahora, en vRealize Automation, puede crear un endpoint de tipo Infoblox IPAM o un endpoint para cualquier paquete o complemento de terceros que haya registrado. Consulte [Crear un endpoint de proveedor de IPAM de terceros](#).

Lista de comprobación para la configuración de Contenedores para vRealize Automation

Para empezar a usar la característica Contenedores, debe configurarla de manera que admita funciones de usuario de vRealize Automation.

Después de configurar las definiciones del contenedor en Contenedores, puede añadir y configurar componentes de contenedor en un blueprint.

Tabla 1-4. Lista de comprobación para la configuración de Contenedores para vRealize Automation

Tarea	Detalles
Asigne las funciones de administrador de contenedores y de arquitecto de contenedores.	Consulte información sobre las funciones de contenedor en <i>Fundamentos y conceptos</i> .
Indique las definiciones de contenedor en la pestaña Contenedores de vRealize Automation.	Consulte <i>Configuración de vRealize Automation</i> .
Añada componentes de contenedor y componentes de red de contenedor a blueprints en la pestaña Diseño de vRealize Automation.	Consulte <i>Configuración de vRealize Automation</i> .

Configurar Contenedores usando el dispositivo de vRealize Automation

Se puede acceder a la información de servicio Xenon en el dispositivo de vRealize Automation (Configuración de vRA > Xenon).

Contiene información acerca de la máquina virtual, el puerto de escucha y el estado del servicio del host Xenon. También muestra información sobre los nodos Xenon en clúster.

Puede administrar el servicio Xenon Linux mediante los siguientes comandos de la CLI en el dispositivo de vRealize Automation.

Comando	Descripción
<code>service xenon-service status</code>	Muestra el estado del servicio (en ejecución o detenido).
<code>service xenon-service start</code>	Inicia el servicio.
<code>service xenon-service stop</code>	Detiene el servicio.
<code>service xenon-service restart</code>	Reinicia el servicio.
<code>service xenon-service get_host</code>	Muestra el nombre de host en el que se está ejecutando el servicio.
<code>service xenon-service get_port</code>	Muestra el puerto del servicio.
<code>service xenon-service status_cluster</code>	Muestra información sobre todos los nodos en clúster en formato JSON.
<code>service xenon-service reset</code>	Elimina el directorio en el que Xenon mantiene todos los archivos de configuración y reinicia el servicio.

Agrupar contenedores en clústeres

Puede usar el servicio Xenon con Contenedores para vRealize Automation para unir nodos a un clúster. Si los nodos están agrupados en clústeres, el servicio Xenon conecta otros nodos de manera automática cuando arranca.

Puede supervisar el estado del clúster en la pestaña **Xenon** del dispositivo de vRealize Automation o mediante la ejecución del comando siguiente en una CLI:

```
service xenon-service status_cluster
```

Xenon funciona mediante una agrupación en clústeres basada en cuórum. El cuórum se calcula con la fórmula $(\text{number of nodes} / 2) + 1$.

Preparar el entorno de vCloud Director para vRealize Automation

Antes de integrar vCloud Director con vRealize Automation, debe instalar y configurar la instancia de vCloud Director, establecer los recursos de vSphere y de nube e identificar o crear las credenciales apropiadas para que vRealize Automation pueda acceder al entorno de vCloud Director.

Configurar el entorno

Configure los recursos de vSphere y de nube, incluidos los centros de datos virtuales y las redes. Para obtener más información, consulte la documentación de vCloud Director.

Credenciales necesarias para la integración

Cree o identifique las credenciales de administrador de la organización o de administrador del sistema que los administradores de IaaS de vRealize Automation usarán para establecer el entorno de vCloud Director bajo la administración de vRealize Automation como un endpoint.

Consideraciones sobre las funciones de usuario

Las funciones de usuario de vCloud Director de una organización no necesitan coincidir con las funciones de los grupos empresariales de vRealize Automation. Si la cuenta de usuario no existe en vCloud Director, vCloud Director realizará una búsqueda en el LDAP o Active Directory asociado y creará la cuenta de usuario si el usuario existe en el almacén de identidades. Si no puede crear la cuenta de usuario, se registra una advertencia pero no se genera un error en el proceso de aprovisionamiento. La máquina aprovisionada se asigna a la cuenta que se usó para configurar el extremo de vCloud Director.

Para obtener información relacionada con la administración de usuarios de vCloud Director, consulte la documentación de vCloud Director.

Preparar el entorno de vCloud Air para vRealize Automation

Antes de integrar vCloud Air con vRealize Automation, debe registrar la cuenta de vCloud Air, establecer el entorno de vCloud Air e identificar o crear las credenciales apropiadas para que vRealize Automation pueda acceder al entorno.

Configurar el entorno

Configure el entorno tal como se indica en la documentación de vCloud Air.

Credenciales necesarias para la integración

Cree o identifique las credenciales de administrador de la infraestructura virtual o de administrador de la cuenta que los administradores de IaaS de vRealize Automation usarán para establecer el entorno de vCloud Air bajo la administración de vRealize Automation como un endpoint.

Consideraciones sobre las funciones de usuario

Las funciones de usuario de vCloud Air de una organización no necesitan coincidir con las funciones de los grupos empresariales de vRealize Automation. Para obtener información relacionada con la administración de usuarios de vCloud Air, consulte la documentación de vCloud Air.

Preparar el entorno de Amazon AWS

Prepare los elementos y las funciones de usuario en su entorno de Amazon AWS, prepare la comunicación de Amazon AWS con el agente invitado y el agente de arranque de Software, y familiarícese con la asignación de las características de Amazon AWS a las características de vRealize Automation.

Funciones de usuario de Amazon AWS y credenciales necesarias para vRealize Automation

Debe configurar credenciales en Amazon AWS con los permisos necesarios para que vRealize Automation administre el entorno.

vRealize Automation requiere claves de acceso para credenciales de endpoint y no admite nombres de usuario ni contraseñas.

■ Autorización de funciones y permisos en Amazon Web Services

Si bien la función Usuario avanzado de AWS proporciona a un usuario o un grupo del servicio de directorio de AWS acceso completo a los servicios y los recursos de AWS, no es obligatoria. También se admiten las funciones de usuario con privilegios más bajos. La política de seguridad de AWS que cumple las necesidades de las funcionalidades de vRealize Automation es:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVolumes",

      "ec2:DescribeVpcAttribute",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImageAttribute",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeVolumeStatus",
      "ec2:DescribeVpnConnections",
      "ec2:DescribeRegions",
      "ec2:DescribeTags",
      "ec2:DescribeVolumeAttribute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeNetworkInterfaceAttribute",

      "ec2:DisassociateAddress",
      "ec2:GetPasswordData",

      "ec2:ImportKeyPair",
      "ec2:ImportVolume",

      "ec2:CreateVolume",
      "ec2>DeleteVolume",
      "ec2:AttachVolume",
      "ec2:ModifyVolumeAttribute",
      "ec2:DetachVolume",
```

```

        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses",

        "ec2:CreateKeyPair",
        "ec2:DeleteKeyPair",

        "ec2:CreateTags",
        "ec2:AssociateAddress",
        "ec2:ReportInstanceState",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:MonitorInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ec2:TerminateInstances",

        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth"
    ],
    "Resource": "*"
}
}]

```

■ Credenciales de autenticación en Amazon Web Services

Para administrar los usuarios y los grupos de Identity and Access Management (IAM) de Amazon, su usuario debe estar configurado con credenciales de Administrador de acceso completo de AWS.

Cuando se crea un endpoint de AWS en vRA, se le pedirá que introduzca una clave y una clave secreta. Para obtener la clave de acceso necesaria para crear el endpoint de Amazon, el administrador debe solicitar una clave de un usuario que tenga credenciales de Administrador de acceso completo de AWS o tener también configurada la política Administrador de acceso completo de AWS. Consulte [Crear un endpoint de Amazon](#).

Para obtener información sobre cómo activar políticas y funciones, consulte la sección *AWS Identity and Access Management (IAM)* de la documentación del producto de Amazon Web Services.

Permitir a Amazon AWS comunicarse con el agente de arranque y el agente invitado de Software

Si desea aprovisionar blueprints de aplicación que contengan Software o si desea seguir personalizando las máquinas aprovisionadas mediante el agente invitado, debe habilitar la conectividad entre el entorno Amazon AWS, en el que se aprovisionan las máquinas, y el entorno vRealize Automation, en el que los agentes descargan los paquetes y reciben instrucciones.

Cuando se utiliza vRealize Automation para aprovisionar las máquinas Amazon AWS con el agente invitado de vRealize Automation y el agente de arranque de Software, debe configurar la conectividad VPC de red a Amazon para que las máquinas aprovisionadas se vuelvan a comunicar con vRealize Automation para personalizar las máquinas.

Para obtener más información acerca de las opciones de conectividad de VPC de Amazon AWS, consulte la documentación de Amazon AWS.

Usar funciones de Amazon opcionales

vRealize Automation admite varias funciones de Amazon, tales como Amazon Virtual Private Cloud, equilibradores de carga flexibles, direcciones IP flexibles y almacenamiento en bloque flexible.

Usar grupos de seguridad de Amazon

Especifique al menos un grupo de seguridad cuando cree una reserva de Amazon. Todas las regiones disponibles requieren al menos un grupo de seguridad especificado.

Un grupo de seguridad actúa como un firewall para controlar el acceso a una máquina. Cada región incluye, como mínimo, el grupo de seguridad predeterminado. Los administradores pueden usar la Amazon Web Services Management Console para crear grupos de seguridad adicionales, configurar puertos para Microsoft Remote Desktop Protocol o SSH, y configurar una red privada virtual para una Amazon VPN.

Cuando cree una reserva de Amazon o configure un componente de máquina en el blueprint, puede elegir en la lista de grupos de seguridad que están disponibles en la región de la cuenta de Amazon especificada. Los grupos de seguridad se importan durante la recopilación de datos.

Para obtener información sobre la creación y el uso de grupos de seguridad en Amazon Web Services, consulte la documentación de Amazon.

Información sobre las regiones de Amazon Web Services

Cada cuenta de Amazon Web Services se representa mediante un endpoint de la nube. Cuando se crea un endpoint de Amazon Elastic Cloud Computing en vRealize Automation, las regiones se recopilan como recursos informáticos. Después de que el administrador de IaaS seleccione los recursos informáticos de un grupo empresarial, se realizan automáticamente recopilaciones de datos de inventario y estado.

En la recopilación de datos de inventario, que se realiza automáticamente una vez al día, se recopilan datos sobre lo que se incluye en un recurso informático. Por ejemplo:

- Direcciones IP flexibles
- Equilibradores de carga flexibles
- Volúmenes de almacenamiento en bloque flexibles

La recopilación de datos de estado se realiza automáticamente cada 15 minutos de forma predeterminada. Se recopila información sobre el estado de las instancias administradas, que son instancias que crea vRealize Automation. A continuación se muestran algunos ejemplos de datos de estado:

- Contraseñas de Windows
- Estado de las máquinas en los equilibradores de carga
- Direcciones IP flexibles

Un administrador de tejido puede iniciar la recopilación de datos de estado e inventario, así como desactivar o cambiar la frecuencia de esta recopilación.

Usar Amazon Virtual Private Cloud

Amazon Virtual Private Cloud permite aprovisionar instancias de máquinas de Amazon en una sección privada de la nube de Amazon Web Services.

Los usuarios de Amazon Web Services pueden utilizar Amazon VPC para designar una topología de red virtual según las especificaciones que haya definido. Puede asignar una Amazon VPC en vRealize Automation. Sin embargo, vRealize Automation no realiza un seguimiento del coste que supone usar la Amazon VPC.

Cuando se aprovisiona mediante Amazon VPC, vRealize Automation espera que haya una subred de VPC de la que Amazon obtenga una dirección IP principal. Esta dirección es estática hasta que finaliza la instancia. También puede usar el grupo de direcciones IP flexibles para adjuntar una dirección IP flexible a una instancia en vRealize Automation. Esto permitiría al usuario mantener la misma dirección IP en caso de que se aprovisione y se desmonte una instancia de forma continua en Amazon Web Services.

Utilice la AWS Management Console para crear los siguientes elementos:

- Una Amazon VPC, que incluye puertas de enlace de Internet, una tabla de enrutamiento, grupos de seguridad y subredes, y direcciones IP disponibles.
- Una Amazon Virtual Private Network si los usuarios necesitan iniciar sesión en instancias de máquinas de Amazon fuera de la AWS Management Console.

Los usuarios de vRealize Automation pueden realizar las siguientes tareas cuando trabajen con una Amazon VPC:

- Un administrador de tejido puede asignar una Amazon VPC a una reserva de nube. Consulte [Crear una reserva de Amazon EC2](#).
- Un propietario de una máquina puede asignar una instancia de máquina de Amazon a una Amazon VPC.

Para obtener más información sobre la creación de una Amazon VPC, consulte la documentación de Amazon Web Services.

Usar equilibradores de carga flexibles en Amazon Web Services

Los equilibradores de carga flexibles distribuyen el tráfico de aplicaciones entrante entre las instancias de Amazon Web Services. El equilibrio de carga de Amazon permite mejorar el rendimiento y la tolerancia a errores.

Amazon pone el equilibrio de carga flexible a disposición de las máquinas aprovisionadas mediante blueprints de Amazon EC2.

El equilibrador de carga flexible debe estar disponible en Amazon Web Services, Amazon Virtual Private Network y en la ubicación de aprovisionamiento. Por ejemplo, si un equilibrador de carga está disponible en us-east1c y la ubicación de una máquina es us-east1b, la máquina no puede usar el equilibrador de carga disponible.

vRealize Automation no crea, administra ni supervisa los equilibradores de carga flexibles.

Para obtener más información sobre la creación de equilibradores de carga flexibles de Amazon mediante Amazon Web Services Management Console, consulte la documentación de Amazon Web Services.

Usar direcciones IP flexibles en Amazon Web Services

El uso de una dirección IP flexible permite realizar rápidamente una conmutación por error en otra máquina en un entorno dinámico de nube de Amazon Web Services. En vRealize Automation, la dirección IP flexible está disponible para todos los grupos empresariales que tengan derechos en la región.

Un administrador puede asignar direcciones IP flexibles a su cuenta de Amazon Web Services mediante AWS Management Console. Hay dos grupos de direcciones IP flexibles en cualquier región: un rango para instancias que no son de Amazon VPC y otro rango para Amazon VPC. Si asigna direcciones únicamente en una región que no sea de Amazon VPC, las direcciones no estarán disponibles en una instancia de Amazon VPC. Lo contrario también es cierto. Si asigna direcciones únicamente en una instancia de Amazon VPC, las direcciones no estarán disponibles en una región que no sea de Amazon VPC.

La dirección IP elástica está asociada con su cuenta de Amazon Web Services, no una máquina específica, pero solo una máquina puede usar la dirección al mismo tiempo. La dirección permanece asociada a su cuenta de Amazon Web Services hasta que decide liberarla. Puede liberarla para asignarla a una instancia de máquina específica.

Un arquitecto de IaaS puede añadir una propiedad personalizada a un blueprint para asignar una dirección IP elástica a máquinas durante el aprovisionamiento. Los propietarios y administradores de máquinas pueden ver las direcciones IP elásticas asignadas a máquinas y los propietarios o administradores de máquinas con derechos para editar máquinas pueden asignar direcciones IP elásticas tras el aprovisionamiento. Sin embargo, si la dirección ya está asociada a una instancia de máquina, y la instancia forma parte de la implementación de Amazon Virtual Private Cloud, Amazon no asigna la dirección.

Para obtener más información sobre la creación y el uso de direcciones IP flexibles de Amazon, consulte la documentación de Amazon Web Services.

Usar almacenamiento en bloque flexible en Amazon Web Services

El almacenamiento en bloque flexible de Amazon proporciona volúmenes de almacenamiento en bloque que se pueden utilizar con una instancia de máquina de Amazon y Amazon Virtual Private Cloud. El volumen de almacenamiento puede continuar más allá del tiempo en el que su instancia de máquina de Amazon asociada permanezca en el entorno de nube de Amazon Web Services.

Cuando utilice un volumen de almacenamiento en bloque flexible de Amazon junto con vRealize Automation, debe tener en cuenta las siguientes advertencias:

- No puede adjuntar un volumen de almacenamiento en bloque flexible existente cuando aprovisiona una instancia de máquina. Sin embargo, si crea un nuevo volumen y solicita más de una máquina simultáneamente, el volumen se creará y adjuntará a cada instancia. Por ejemplo, si crea un volumen denominado volumen_1 y solicita tres máquinas, se creará un volumen para cada máquina. Se crearán tres volúmenes denominados volumen_1 y se adjuntarán a cada una de las máquinas. Cada volumen tendrá un ID de volumen único. Todos los volúmenes tendrán el mismo tamaño y estarán en la misma ubicación.
- El volumen debe tener el mismo sistema operativo y estar en la misma ubicación que la máquina a la que se adjunta.
- vRealize Automation no administra el volumen principal de una instancia con almacenamiento en bloque flexible.

Para obtener más información sobre el almacenamiento en bloque flexible de Amazon y para ver detalles sobre cómo habilitarlo mediante Amazon Web Services Management Console, consulte la documentación de Amazon Web Services.

Configurar la conectividad de red a VPC de Amazon para un entorno de prueba de concepto

Como el profesional de TI que configura un entorno para evaluar vRealize Automation, desea configurar temporalmente la conectividad de red a VPC de Amazon para admitir la función Software de vRealize Automation.

La conectividad entre la red y el VPC de Amazon solamente es necesaria si desea usar el agente invitado para personalizar máquinas aprovisionadas, o bien si desea incluir componentes de Software en sus blueprints. En un entorno de producción, configuraría la conectividad oficialmente a través de Amazon Web Services. Sin embargo, como trabaja en un entorno de prueba de concepto, desea crear una conectividad temporal de red a VPC de Amazon. Primero establezca el túnel SSH y después configure una reserva de Amazon en vRealize Automation para enrutar por el túnel.

Requisitos previos

- Cree un grupo de seguridad de Amazon AWS denominado TunnelGroup y configúrelo para que permita el acceso en el puerto 22.

- Cree o identifique una máquina CentOS en el grupo de seguridad TunnelGroup de Amazon AWS y anote las siguientes configuraciones:
 - Credenciales de usuario administrador, por ejemplo *root*.
 - Dirección IP pública.
 - Dirección IP privada.
- Cree o identifique una máquina CentOS en la misma red local donde se encuentra la instalación de vRealize Automation.
- Instale el servidor OpenSSH SSHD en ambas máquinas de túnel.

Procedimiento

- 1 Inicie sesión en su máquina de túnel de Amazon AWS como el usuario raíz o similar.
- 2 Desactive iptables.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

- 3 Edite `/etc/ssh/sshd_config` para habilitar `AllowTCPForwarding` y `GatewayPorts`.
- 4 Reinicie el servicio.

```
/etc/init.d/sshd restart
```

- 5 Inicie sesión en la máquina CentOS en la misma red local donde se encuentra la instalación de vRealize Automation como el usuario raíz.
- 6 Invoque el túnel SSH de la máquina de red local a la máquina de túnel de Amazon AWS.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \

-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
User of Amazon tunnel machine@Public IP Address of Amazon tunnel machine
```

Ha configurado el reenvío de puerto para permitir que la máquina de túnel de Amazon AWS pueda acceder a los recursos de vRealize Automation, pero el túnel SSH no funcionará hasta que configure una reserva de Amazon para enrutar por el túnel.

Pasos siguientes

- 1 Instale el agente de arranque del software y el agente invitado en una máquina Windows o Linux de referencia para crear una imagen de máquina de Amazon que los arquitectos de IaaS puedan usar para crear blueprints. Consulte [Preparar el aprovisionamiento de Software](#).
- 2 Configure la reserva de Amazon en vRealize Automation para enrutar por el túnel SSH. Consulte [Escenario: Crear una reserva de Amazon para un entorno de prueba de concepto](#).

Preparar funciones de red y seguridad de Red Hat OpenStack

vRealize Automation admite varias funciones en OpenStack, como los grupos de seguridad y las direcciones IP flotantes. Familiarícese con el funcionamiento de estas funciones con vRealize Automation y configúrelas en su entorno.

Usar grupos de seguridad de OpenStack

Los grupos de seguridad permiten especificar reglas para controlar el tráfico de red a través de puertos específicos.

Puede especificar grupos de seguridad en una reserva al solicitar una máquina. También puede especificar un grupo de seguridad de NSX existente o a petición en el lienzo de diseño.

Los grupos de seguridad se importan durante la recopilación de datos.

Todas las regiones disponibles requieren al menos un grupo de seguridad especificado. Al crear una reserva, se muestran los grupos de seguridad disponibles para el usuario en esa región. Cada región incluye, como mínimo, el grupo de seguridad predeterminado.

Los grupos de seguridad adicionales deben administrarse en el recurso de origen. Para obtener más información sobre la administración de grupos de seguridad para las diversas máquinas, consulte la documentación de OpenStack.

Usar direcciones IP flotantes con OpenStack

Se pueden asignar direcciones IP flotantes a una instancia virtual en funcionamiento en OpenStack.

Para poder asignar direcciones IP flotantes, hay que configurar el reenvío de IP y crear un grupo de direcciones IP flotantes en Red Hat OpenStack. Para obtener más información, consulte la documentación de Red Hat OpenStack.

Es necesario autorizar las acciones Asociar IP flotante y Desasociar IP flotante a los propietarios de máquina. De este modo, los usuarios autorizados podrán asociar una dirección IP flotante a una máquina aprovisionada desde redes externas conectadas a la máquina (seleccionando para ello una dirección disponible del grupo de direcciones IP flotantes). Una vez que una dirección IP flotante se ha asociado a una máquina, un usuario de vRealize Automation puede seleccionar la opción Desasociar IP flotante para ver las direcciones IP flotantes que hay asignadas actualmente y desasociar una dirección de una máquina.

Preparar el entorno de SCVMM

Antes de empezar a crear plantillas y perfiles de hardware de SCVMM para usarlos en el aprovisionamiento de máquinas de vRealize Automation, debe comprender las restricciones de asignación de nombres de plantillas y perfiles de hardware, y configurar las opciones de red y almacenamiento de SCVMM.

Para obtener información relacionada con la preparación de su entorno, consulte la información de requisitos de SCVMM en *Instalación de vRealize Automation*.

Para obtener información relacionada con el aprovisionamiento de máquinas, consulte [Crear un endpoint de Hyper-V \(SCVMM\)](#).

vRealize Automation no admite un entorno de implementación en el que se use una configuración de nube privada de SCVMM. Actualmente, vRealize Automation no puede realizar tareas de recopilación, asignación o aprovisionamiento que estén basadas en nubes privadas de SCVMM.

Asignación de nombres de plantillas y perfiles de hardware

Siguiendo las convenciones de asignación de nombres que SCVMM y vRealize Automation usan en las plantillas y perfiles de hardware, no inicie los nombres de plantillas y perfiles de hardware con las palabras "temporary" o "profile". Por ejemplo, los siguientes términos se ignoran durante la recopilación de datos:

- TemporaryTemplate
- Temporary Template
- TemporaryProfile
- Temporary Profile
- Profile

Configuración de red requerida para clústeres de SCVMM

Los clústeres de SCVMM solo exponen redes virtuales a vRealize Automation, de forma que debe existir una relación 1:1 entre las redes virtual y lógica. Con la consola de SCVMM, asigne cada red lógica a una red virtual y configure el clúster de SCVMM para acceder a las máquinas a través de la red virtual.

Configuración de almacenamiento requerida para clústeres de SCVMM

En los clústeres de Hyper-V de SCVMM, vRealize Automation recopila datos y aprovisionamientos únicamente en volúmenes compartidos. Con la consola de SCVMM, configure los clústeres para utilizar volúmenes de recursos compartidos para almacenamiento.

Configuración de almacenamiento requerida para hosts de SCVMM independientes

Para los hosts de SCVMM independientes, vRealize Automation recopila datos y aprovisionamientos en la ruta de máquina virtual predeterminada. Con la consola de SCVMM, configure rutas de máquinas virtuales predeterminadas para los hosts independientes.

Configurar la conectividad VPC de red a Azure

Debe configurar la conectividad de red a Azure si quiere usar componentes de software en los blueprints de Azure.

Requisitos previos

- Cree un grupo de seguridad de Azure denominado TunnelGroup y configúrelo para que permita el acceso en el puerto 22.
- Cree o identifique una máquina, como una máquina CentOS, en el grupo de seguridad TunnelGroup de Azure y anote las siguientes configuraciones:
 - Credenciales de usuario administrador, por ejemplo *root*.
 - Dirección IP pública.
 - Dirección IP privada.
- Cree o identifique una máquina CentOS en la misma red local donde se encuentra la instalación de vRealize Automation.
- Instale el servidor OpenSSH SSHD en ambas máquinas de túnel.

Procedimiento

- 1 Inicie sesión en la máquina de túnel de Azure como el usuario raíz o similar.
- 2 Desactive iptables.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

- 3 Edite `/etc/ssh/sshd_config` para habilitar `AllowTCPForwarding` y `GatewayPorts`.
- 4 Reinicie el servicio.

```
/etc/init.d/sshd restart
```

- 5 Inicie sesión en la máquina CentOS en la misma red local donde se encuentra la instalación de vRealize Automation como el usuario raíz.
- 6 Invoque el túnel SSH de la máquina de red local a la máquina de túnel de Azure.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \
-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
User of Azure tunnel machine@Public IP Address of Azure tunnel machine
```

Ha configurado el enrutamiento de puerto para permitir que la máquina de túnel de Azure acceda a los recursos de vRealize Automation, pero el túnel SSH no funcionará hasta que configure una reserva de Azure para enrutar por el túnel.

Pasos siguientes

- 1 Instale el agente de arranque del software y el agente invitado en una máquina Windows o Linux de referencia para crear una imagen de máquina de Azure que los arquitectos de IaaS puedan usar para crear blueprints. Consulte [Preparar el aprovisionamiento de Software](#).
- 2 Configure la reserva de Azure en vRealize Automation para enrutar por el túnel SSH. Consulte [Crear una reserva de Microsoft Azure](#).

Preparar el aprovisionamiento de máquinas

En función del entorno y del método de aprovisionamiento de máquinas, es posible que necesite configurar elementos fuera de vRealize Automation.

Por ejemplo, puede que deba configurar plantillas de máquina o imágenes de máquina. También es posible que deba configurar los ajustes de NSX o ejecutar flujos de trabajo de vRealize Orchestrator.

Para obtener información relacionada con la especificación de los puertos durante la preparación del aprovisionamiento de las máquinas, consulte *Guía de configuración segura* y *Arquitectura de referencia* en la [información sobre VMware vRealize Automation](#).

Elegir el método de aprovisionamiento de máquinas que se preparará

Para la mayor parte de los métodos de aprovisionamiento de máquinas, debe preparar elementos fuera de vRealize Automation.

Tabla 1-5. Elegir el método de aprovisionamiento de máquinas que se preparará

Escenario	Endpoint compatible	Compatibilidad con agentes	Método de aprovisionamiento	Preparativos anteriores al aprovisionamiento
Configure vRealize Automation para que ejecute scripts de Visual Basic personalizados como pasos extra dentro del ciclo de vida de la máquina, ya sea antes o después del aprovisionamiento de la máquina. Por ejemplo, podría usar un script anterior al aprovisionamiento para generar certificados o tokens de seguridad antes de realizar el aprovisionamiento y después ejecutar un script posterior al aprovisionamiento para usar esos certificados y tokens después del aprovisionamiento de la máquina.	Puede ejecutar scripts de Visual Basic con cualquier endpoint admitido excepto Amazon AWS.	Depende del método de aprovisionamiento que elija.	Admitido como paso adicional en cualquier método de aprovisionamiento, pero no puede usar scripts de Visual Basic con máquinas de Amazon AWS.	Lista de comprobación para ejecutar scripts de Visual Basic durante el aprovisionamiento
Aprovisione blueprints de aplicación que automaticen la instalación, la configuración y la administración del ciclo de vida de middleware y componentes de implementaciones de aplicaciones como Oracle, MySQL, WAR y esquemas de base de datos.	<ul style="list-style-type: none"> ■ vSphere ■ vCloud Air ■ vCloud Director ■ Amazon AWS 	<ul style="list-style-type: none"> ■ (Requerido) Agente invitado ■ (Requerido) Agente de arranque de software y agente invitado 	<ul style="list-style-type: none"> ■ Clonar ■ Clon (para vCloud Air o vCloud Director) ■ Clon vinculado ■ Imagen de máquina de Amazon 	Si desea poder usar componentes de Software en sus blueprints, prepare un método de aprovisionamiento que admita el agente invitado y el agente de arranque de Software. Para obtener más información sobre cómo prepararse para Software, consulte Preparar el aprovisionamiento de Software .
Siga personalizando máquinas después de aprovisionar con el agente invitado.	Todos los endpoints virtuales y Amazon AWS.	<ul style="list-style-type: none"> ■ (Requerido) Agente invitado ■ (Opcional) Agente de arranque de software y agente invitado 	Admitido para todos los métodos de aprovisionamiento, excepto Imagen de máquina virtual.	Si desea poder personalizar máquinas después del aprovisionamiento, seleccione un método de aprovisionamiento que admita el agente invitado. .

Tabla 1-5. Elegir el método de aprovisionamiento de máquinas que se preparará (continuación)

Escenario	Endpoint compatible	Compatibilidad con agentes	Método de aprovisionamiento	Preparativos anteriores al aprovisionamiento
Aprovisionar máquinas sin sistema operativo invitado. Puede instalar un sistema operativo tras el aprovisionamiento.	Todos los endpoints de máquinas virtuales.	No se admite	Básico	Ningún preparativo anterior al aprovisionamiento fuera de vRealize Automation.
Aprovisionar una copia con espacio eficiente de una máquina virtual llamada clon vinculado. Los clones vinculados se basan en el snapshot de una máquina virtual y usan una cadena de discos delta para realizar un seguimiento de las diferencias con respecto a una máquina principal.	vSphere	<ul style="list-style-type: none"> ■ (Opcional) Agente invitado ■ (Opcional) Agente de arranque de software y agente invitado 	Clon vinculado	<p>Debe tener ya una máquina virtual de vSphere.</p> <p>Para admitir Software, debe instalar el agente invitado y el agente de arranque de software en la máquina que vaya a clonar.</p> <p>El snapshot de máquina virtual identificado en el blueprint debe apagarse antes de aprovisionar las máquinas virtuales de clon vinculado.</p>
Aprovisionar una copia con espacio eficiente de una máquina virtual mediante la tecnología Net App FlexClone.	vSphere	(Opcional) Agente invitado	NetApp FlexClone	Consulte Lista de comprobación para preparar el aprovisionamiento mediante clonación .
Aprovisionar máquinas mediante la clonación de un objeto de plantilla creado a partir de una máquina Windows o Linux existente, llamada máquina de referencia, y un objeto de personalización.	<ul style="list-style-type: none"> ■ vSphere ■ KVM (RHEV) ■ SCVMM 	<ul style="list-style-type: none"> ■ (Opcional) Agente invitado ■ (Opcional solo para vSphere) Agente de arranque de software y agente invitado 	Clonar	<p>Consulte Lista de comprobación para preparar el aprovisionamiento mediante clonación.</p> <p>Para admitir Software, debe instalar el agente invitado y el agente de arranque de software en la máquina de vSphere que vaya a clonar.</p>
Aprovisionar máquinas de vCloud Air o vCloud Director clonado a partir de una plantilla y un objeto de personalización.	<ul style="list-style-type: none"> ■ vCloud Air ■ vCloud Director 	<ul style="list-style-type: none"> ■ (Opcional) Agente invitado ■ (Opcional) Agente de arranque de software y agente invitado 	Clonado de vCloud Air o vCloud Director	<p>Consulte Preparar el aprovisionamiento de vCloud Air y vCloud Director.</p> <p>Para admitir Software, cree una plantilla que contenga el agente invitado y el agente de arranque de software. Para vCloud Air, configure la conectividad de red entre su entorno de vRealize Automation y el de vCloud Air.</p>

Tabla 1-5. Elegir el método de aprovisionamiento de máquinas que se preparará (continuación)

Escenario	Endpoint compatible	Compatibilidad con agentes	Método de aprovisionamiento	Preparativos anteriores al aprovisionamiento
Aprovisionar una máquina mediante el arranque desde una imagen ISO usando un archivo de configuración Kickstart o autoYaST y una imagen de distribución Linux para instalar el sistema operativo en la máquina.	<ul style="list-style-type: none"> ■ Todos los endpoints virtuales ■ Red Hat OpenStack 	El agente invitado se instala como parte de las instrucciones de preparación.	Kickstart de Linux	Preparar el aprovisionamiento de Kickstart de Linux
Aprovisionar una máquina y transferir el control a una secuencia de tareas de SCCM para arrancar desde una imagen ISO, implementar un sistema operativo Windows e instalar el agente invitado de vRealize Automation.	Todos los endpoints de máquinas virtuales.	El agente invitado se instala como parte de las instrucciones de preparación.	SCCM	Preparar el aprovisionamiento de SCCM
Aprovisionar una máquina mediante el arranque en un entorno WinPE y la instalación de un sistema operativo usando una imagen Windows Imaging File Format (WIM) de una máquina de referencia Windows existente.	<ul style="list-style-type: none"> ■ Todos los endpoints virtuales ■ Red Hat OpenStack 	Se necesita el agente invitado. Al crear la imagen de WinPE, debe insertar manualmente el agente invitado.	WIM	Preparar el aprovisionamiento de WIM
Iniciar una instancia desde una imagen de máquina virtual.	Red Hat OpenStack	No se admite	Imagen de máquina virtual	Consulte Preparar el aprovisionamiento de imágenes de máquina virtual .
Iniciar una instancia desde una imagen de máquina de Amazon.	Amazon AWS	<ul style="list-style-type: none"> ■ (Opcional) Agente invitado ■ (Opcional) Agente de arranque de software y agente invitado 	Imagen de máquina de Amazon	Asocie los tipos de instancia y las imágenes de máquina de Amazon con su cuenta de Amazon AWS. Para admitir Software, cree una imagen de máquina de Amazon que contenga el agente invitado y el agente de arranque de software, y configure la conectividad entre la red y la VPC entre su entorno de Amazon AWS y el de vRealize Automation.

Lista de comprobación para ejecutar scripts de Visual Basic durante el aprovisionamiento

vRealize Automation se puede configurar para que ejecute sus scripts de Visual Basic personalizados como pasos extra dentro del ciclo de vida de la máquina, ya sea antes o después del aprovisionamiento de máquina. Así, por ejemplo, podría usar un script anterior al aprovisionamiento para generar certificados o tokens de seguridad antes de realizar el aprovisionamiento y, luego, ejecutar un script posterior al aprovisionamiento para usar esos certificados y tokens después del aprovisionamiento de máquinas. Los scripts de Visual Basic se pueden utilizar con cualquier método de aprovisionamiento, pero no con máquinas de Amazon AWS.

Tabla 1-6. Lista de comprobación para ejecutar scripts de Visual Basic durante el aprovisionamiento

Tarea	Ubicación	Detalles
❑ Instalar y configurar el agente de EPI de scripts de Visual Basic.	Normalmente, el host de Manager Service.	Consulte <i>Instalación de vRealize Automation</i> .
❑ Crear los scripts de Visual Basic.	Máquina en la que está instalado el agente de EPI.	<p>vRealize Automation incluye un script de Visual Basic de ejemplo (PrePostProvisioningExample.vbs) en el subdirectorio Scripts del directorio de instalación del agente de EPI. Este script contiene un encabezado para cargar todos los argumentos en un diccionario, un cuerpo en el que se pueden incluir funciones y un pie de página para devolver propiedades personalizadas actualizadas a vRealize Automation.</p> <p>Cuando se ejecuta un script de Visual Basic, el agente de EPI pasa todas las propiedades personalizadas de máquina como argumentos a ese script. Para devolver propiedades personalizadas actualizadas a vRealize Automation, coloque esas propiedades en un diccionario y llame a la función proporcionada por vRealize Automation.</p>
❑ Reunir la información necesaria para incluir sus scripts en los blueprints.	<p>La información se captura y transfiere a los arquitectos de la infraestructura.</p> <p>Nota Un administrador de tejido puede crear un grupo de propiedades mediante los conjuntos de propiedades ExternalPreProvisioningVbScript y ExternalPostProvisioningVbScript para proporcionar la información necesaria. De este modo, será más fácil que los arquitectos de blueprints incluyan esta información correctamente en sus blueprints.</p>	<ul style="list-style-type: none"> ■ La ruta completa del script de Visual Basic, incluidos el nombre de archivo y la extensión. Por ejemplo: <i>%Unidad del sistema%Archivos de programa (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs</i>. ■ Para ejecutar un script antes del aprovisionamiento, indique a los arquitectos de la infraestructura que especifiquen la ruta completa al script como valor de la propiedad personalizada ExternalPreProvisioningVbScript. Para ejecutar un script después del aprovisionamiento, es necesario usar la propiedad personalizada ExternalPostProvisioningVbScript.

Usar el agente invitado de vRealize Automation durante el aprovisionamiento

Puede instalar el agente invitado en máquinas de referencia para personalizar más una máquina tras la implementación. Puede utilizar las propiedades personalizadas reservadas para el agente de invitado para realizar personalizaciones básicas, como añadir y formatear discos, o bien puede crear sus propios scripts personalizados para que el agente invitado se ejecute en el sistema operativo invitado de una máquina aprovisionada.

Después de finalizar la implementación y de ejecutar la especificación de personalización (en caso de que se haya proporcionado una), el agente invitado crea un archivo XML que contiene todas las propiedades personalizadas de la máquina implementada `c:\VRMGuestAgent\site\workitem.xml`, completa las tareas que tiene asignadas con las propiedades personalizadas del agente invitado y luego se elimina a sí mismo de la máquina aprovisionada.

Puede escribir sus propios scripts personalizados para que el agente invitado los ejecute en las máquinas implementadas y utilizar propiedades personalizadas en el blueprint de máquina para especificar la ubicación de dichos scripts y el orden en que deben ejecutarse. También puede usar propiedades personalizadas en el blueprint de máquina para pasar valores de propiedad personalizados a sus scripts como parámetros.

Por ejemplo, podría usar el agente invitado para realizar las siguientes personalizaciones en las máquinas implementadas:

- Cambiar la dirección IP
- Añadir o formatear unidades
- Ejecutar scripts de seguridad
- Inicializar otro agente, por ejemplo, Puppet o Chef

También puede proporcionar una cadena cifrada como propiedad personalizada en un argumento de línea de comandos. Eso permite almacenar información cifrada que el agente invitado puede descifrar y comprender como argumento de línea de comandos válido.

Nota El agente invitado de Linux asigna direcciones IP estáticas durante las acciones de creación y clonación para el aprovisionamiento de PXE y Kickstart de Linux en relación con las propiedades personalizadas de vRealize Automation en elementos de trabajo. El agente invitado no puede alojar el esquema de asignación de nombres de red coherente más reciente, como en Ubuntu 16.x, cuando asigna direcciones IP estáticas.

Sus scripts personalizados no tienen que estar instalados localmente en la máquina. Siempre que la máquina aprovisionada tenga acceso de red a la ubicación del script, el agente invitado podrá acceder a los scripts y ejecutarlos. Esto reduce los costes de mantenimiento, ya que es posible actualizar los scripts sin tener que volver a construir todas las plantillas.

Puede configurar opciones de seguridad para las máquinas virtuales que se van a aprovisionar mediante la especificación de información en el script de una reserva, un blueprint o un agente invitado. Si las máquinas que se aprovisionarán requieren un agente invitado, debe añadir una regla de seguridad que contenga ese requisito a la reserva o el blueprint. Por ejemplo, si usa una política de seguridad predeterminada que deniegue la comunicación entre todas las máquinas y dependa de una política de seguridad independiente para permitir la comunicación entre máquinas específicas, es posible que el agente invitado no pueda comunicarse con vRealize Automation durante la fase de personalización. Para evitar este problema durante el aprovisionamiento de máquinas, use una política de seguridad predeterminada que permita la comunicación durante la fase de personalización.

Si opta por instalar el agente invitado para ejecutar scripts personalizados en máquinas aprovisionadas, los blueprints deben incluir las propiedades personalizadas del agente invitado adecuadas. Por ejemplo, si instala el agente invitado en una plantilla de clonación, crea un script personalizado que cambie la dirección IP de la máquina aprovisionada y coloca el script en una ubicación compartida, necesitará incluir varias propiedades personalizadas en el blueprint.

Tabla 1-7. Propiedades personalizadas para cambiar la dirección IP de una máquina aprovisionada con un agente invitado

Propiedad personalizada	Descripción
VirtualMachine.Admin.UseGuestAgent	Establézcala en true para inicializar el agente invitado cuando se inicie la máquina aprovisionada.
VirtualMachine.Customize.WaitComplete	Establézcala en True para impedir que el flujo de trabajo de aprovisionamiento envíe elementos de trabajo al agente invitado hasta que todas las personalizaciones se hayan completado.

Tabla 1-7. Propiedades personalizadas para cambiar la dirección IP de una máquina aprovisionada con un agente invitado (continuación)

Propiedad personalizada	Descripción
VirtualMachine.SoftwareN.ScriptPath	<p>Especifica la ruta completa de un script de instalación de una aplicación. La ruta debe ser una ruta absoluta válida según el sistema operativo invitado y debe incluir el nombre del archivo de script.</p> <p>Puede transferir valores de propiedad personalizada como parámetros al script si inserta <code>{CustomPropertyName}</code> en la cadena de la ruta. Por ejemplo, si tiene una propiedad personalizada denominada <code>ActivationKey</code> cuyo valor es 1234, la ruta de script es <code>D:\InstallApp.bat -key {ActivationKey}</code>. El agente invitado ejecuta el comando <code>D:\InstallApp.bat -key 1234</code>. Posteriormente, el archivo de script se puede programar para aceptar y usar este valor.</p> <p>Inserte <code>{Owner}</code> para pasar el nombre de propietario de la máquina al script.</p> <p>Para pasar valores de propiedad personalizados como parámetros al script, inserte <code>{YourCustomProperty}</code> en la cadena de ruta. Por ejemplo, al introducir el valor <code>\\vra-scripts.mycompany.com\scripts\changeIP.bat</code> se ejecuta el script <code>changeIP.bat</code> desde una ubicación compartida, pero al introducir el valor <code>\\vra-scripts.mycompany.com\scripts\changeIP.bat {VirtualMachine.Network0.Address}</code> se ejecuta el script <code>changeIP</code> y, además, se pasa el valor de la propiedad <code>VirtualMachine.Network0.Address</code> al script como un parámetro.</p>
VirtualMachine.ScriptPath.Decrypt	<p>Permite que vRealize Automation obtenga una cadena cifrada que pase como declaración de propiedad personalizada <code>VirtualMachine.SoftwareN.ScriptPath</code> correctamente formateada hasta la línea de comandos <code>gugent</code>.</p> <p>Puede proporcionar una cadena cifrada (p. ej., su contraseña) como propiedad personalizada en un argumento de línea de comandos. Eso le permite almacenar información cifrada que el agente invitado puede descifrar y comprender como argumento de línea de comandos válido. Por ejemplo, la cadena de propiedad personalizada <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat password</code> no es segura, ya que contiene una contraseña real.</p>

Tabla 1-7. Propiedades personalizadas para cambiar la dirección IP de una máquina aprovisionada con un agente invitado (continuación)

Propiedad personalizada	Descripción
	<p>Para cifrar la contraseña, puede crear una propiedad personalizada de vRealize Automation (p. ej., <code>MyPassword = password</code>) y habilitar el cifrado seleccionando la casilla de verificación disponible. El agente invitado descifra la entrada [MyPassword] hasta obtener el valor de la propiedad personalizada <code>MyPassword</code> y ejecuta el script como <code>c:\dosomething.bat password</code>.</p> <ul style="list-style-type: none"> ■ Cree una propiedad personalizada <code>MyPassword = password</code>, donde <code>password</code> es el valor de la contraseña real. Habilite el cifrado seleccionando la casilla de verificación disponible. ■ Establezca la propiedad personalizada <code>VirtualMachine.ScriptPath.Decrypt</code> en <code>VirtualMachine.ScriptPath.Decrypt = true</code>. ■ Establezca la propiedad personalizada <code>VirtualMachine.Software0.ScriptPath</code> en <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat [MyPassword]</code>. <p>Si establece <code>VirtualMachine.ScriptPath.Decrypt</code> como <code>false</code> o no crea la propiedad personalizada <code>VirtualMachine.ScriptPath.Decrypt</code>, no se descifrá la cadena que está entre corchetes ([y]).</p>

Para obtener más información sobre las propiedades personalizadas que puede usar con el agente invitado, consulte *Referencia de propiedades personalizadas*.

Configurar el agente invitado para confiar en un servidor

El método más seguro para configurar el agente invitado de modo que confíe en un servidor consiste en la instalación del archivo PEM de clave pública para el host de Manager Service de vRealize Automation en la carpeta de agente invitado adecuada.

Busque la carpeta del agente invitado en cada plantilla del archivo PEM `cert.pem` para que el host de Manager Service confíe en un servidor:

- Carpeta del agente invitado de Windows en cada plantilla que utilice gagent

```
C:\VRMGuestAgent\cert.pem
```

- Carpeta del agente invitado de Linux en cada plantilla que utilice gagent

```
/usr/share/gagent/cert.pem
```

Si no coloca el archivo `cert.pem` en esta ubicación, la máquina de referencia de plantilla no podrá utilizar el agente invitado. Por ejemplo, si intenta recopilar la información de la clave pública después de que la máquina virtual se inicie mediante la alteración de scripts, interrumpirá la condición de seguridad.

En función del entorno configurado, se deben tener en cuenta consideraciones adicionales:

- Para las instalaciones WIM, debe añadir el contenido del archivo PEM de clave pública a la interfaz de usuario y al ejecutable de la consola. El indicador de la consola es **/cert filename**.
- Para las instalaciones Kickstart de RedHat, debe cortar la clave pública y pegarlo en el archivo de muestra, ya que, de lo contrario, el agente invitado no podrá ejecutarse.
- Para la instalación de SCCM, el archivo `cert.pem` debe estar en la carpeta `VRMGuestAgent`.
- Para las instalaciones de vSphere en Linux, el archivo `cert.pem` debe estar en la carpeta `/usr/share/gugent`.

Nota Opcionalmente, puede instalar software y agentes invitados a la vez descargando el siguiente script de <https://APPLIANCE/software/index.html>. El script le permite gestionar la aceptación de huellas digitales de certificado SSL mientras crea las plantillas.

- Linux
`prepare_vra_template.sh`
- Windows
`prepare_vra_template.ps1`

Si instala el software y el agente invitado a la vez, no es necesario que siga las instrucciones indicadas en [Instalar el agente invitado en una máquina de referencia de Linux](#) o [Instalar el agente invitado en una máquina de referencia de Windows](#).

Instalar el agente invitado en una máquina de referencia de Linux

Instale el agente invitado de Linux en las máquinas de referencia para seguir personalizando las máquinas tras la implementación.

Requisitos previos

- Identifique o cree la máquina de referencia.
- Los archivos de agente invitado que descargue contienen los formatos de paquete `tar.gz` y `RPM`. Si su sistema operativo no puede instalar archivos `tar.gz` o `RPM`, use una herramienta de conversión para convertirlos al formato de paquete que le convenga.
- Establezca confianza segura entre el agente invitado y la máquina de Manager Service. Consulte [Configurar el agente invitado para confiar en un servidor](#).

Procedimiento

- 1 Desplácese hasta la página de la consola de administración del dispositivo de vRealize Automation.

Por ejemplo: `https://va-hostname.domain.com`.

- 2 Haga clic en la **página del agente invitado y el agente de software** en la sección de instalación de componentes de vRealize Automation de la página.
Por ejemplo: `https://va-hostname.domain.com/software/index.html`.
Se abre la página de los **instaladores del agente invitado y del agente de software**, donde se proporcionan vínculos a descargas disponibles.
- 3 Haga clic en los **paquetes de agentes invitados de Linux** en la sección de los instaladores de agentes invitados de la página para descargar y guarde el archivo `LinuxGuestAgentPkgs.zip`.
- 4 Descomprima el archivo `LinuxGuestAgentPkgs.zip` descargado para crear la carpeta `VraLinuxGuestAgent`.

- 5 Instale el paquete de agente invitado correspondiente al sistema operativo invitado que vaya a implementar durante el aprovisionamiento.

- a Desplácese hasta el subdirectorio `VraLinuxGuestAgent` que corresponde al sistema operativo invitado que se implementará durante el aprovisionamiento, por ejemplo `rhel32`.
- b Busque el formato de paquete de su elección o convierta un paquete al formato de paquete deseado.
- c Instale el paquete de agente invitado en la máquina de referencia.

Por ejemplo, para instalar los archivos del paquete RPM, ejecute `rpm -i gurent-gurent-7.1.0-4201531.i386.rpm`.

- 6 Configure el agente invitado para que se comuniquen con Manager Service. Para ello, ejecute `installgurent.sh Manager_Service_Hostname_fdqn:portnumber ssl platform`.

El número de puerto predeterminado de Manager Service es 443. Los valores de plataforma aceptados son `ec2`, `vcd`, `vca` y `vsphere`.

Opción	Descripción
Si usa un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga de Manager Service. Por ejemplo:</p> <pre>cd /usr/share/gurent ./installgurent.sh load_balancer_manager_service.mycompany.com:443 ssl ec2</pre>
Si no usa un equilibrador de carga	<p>Escriba el nombre de dominio completo y el número de puerto de la máquina de Manager Service. Por ejemplo:</p> <pre>cd /usr/share/gurent ./installgurent.sh manager_service_machine.mycompany.com:443 ssl vsphere</pre>

- 7 Si aún no hay máquinas implementadas configuradas para confiar en el certificado SSL de Manager Service, deberá instalar el archivo `cert.pem` en la máquina de referencia para definir la confianza.

- El método más seguro consiste en obtener `cert.pem` e instalar manualmente el archivo en la máquina de referencia.
- El método más cómodo consiste en conectarse al equilibrador de carga o a la máquina de Manager Service y descargar el certificado `cert.pem`.

Opción	Descripción
Si usa un equilibrador de carga	<p>En tanto que usuario raíz en la máquina de referencia, ejecute el siguiente comando:</p> <pre>echo openssl s_client -connect manager_service_load_balancer.mycompany.com:443 sed -ne '/- BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>
Si no usa un equilibrador de carga	<p>En tanto que usuario raíz en la máquina de referencia, ejecute el siguiente comando:</p> <pre>echo openssl s_client -connect manager_service_machine.mycompany.com:443 sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>

- 8 Si instala el agente invitado en un sistema operativo Ubuntu, cree vínculos simbólicos para objetos compartidos ejecutando uno de los siguientes conjuntos de comandos.

Opción	Descripción
Sistemas de 64 bits	<pre>cd /lib/x86_64-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>
Sistemas de 32 bits	<pre>cd /lib/i386-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>

Pasos siguientes

Convierta la máquina de referencia en una plantilla para clonar un snapshot o una imagen de máquina de Amazon que los arquitectos de IaaS podrán usar cuando creen blueprints.

Instalar el agente invitado en una máquina de referencia de Windows

Instale el agente invitado de Windows vRealize Automation en una máquina de referencia de Windows para ejecutarlo como un servicio de Windows y permitir una mayor personalización de las máquinas.

Requisitos previos

- Identifique o cree la máquina de referencia.

- Establezca confianza segura entre el agente invitado y la máquina de Manager Service. Consulte [Configurar el agente invitado para confiar en un servidor](#).

Procedimiento

- 1 Desplácese hasta la página de **instaladores de agentes invitados y de software** del dispositivo vRealize Automation:

`https://vrealize-automation-appliance-FQDN/software`
- 2 En **Instaladores de agentes invitados**, descargue y guarde el archivo ejecutable de 32 o 64 bits en la raíz de la unidad C:.

Nota Hay una alternativa con la línea de comandos a este procedimiento para la instalación del agente invitado. En lugar de descargar los archivos ejecutables, puede ir a **Instaladores de software de Windows** en la página de instaladores de agentes invitados y de software. Allí podrá descargar y ejecutar el script de PowerShell `prepare_vra_template.ps1`:

```
PowerShell -NoProfile -ExecutionPolicy Bypass -Command prepare_vra_template.ps1
```

- 3 Extraiga los archivos del agente invitado de Windows mediante el archivo ejecutable. La extracción crea `C:\VRMGuestAgent` y agrega los archivos. No cambie el nombre de `C:\VRMGuestAgent`.
- 4 Configure el agente invitado para que se comuniquen con Manager Service.
 - a Abra una ventana de símbolo del sistema con privilegios elevados.
 - b Vaya a `C:\VRMGuestAgent`.
 - c Coloque el archivo PEM de Manager Service de confianza en el directorio `C:\VRMGuestAgent\` a fin de configurar el agente invitado para que confíe en su máquina de Manager Service.
 - d Ejecute `win service -i -h Manager_Service_Hostname_fdqn:portnumber -p ssl`.

El número de puerto predeterminado de Manager Service es 443.

Opción	Descripción
Si usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto del equilibrador de carga de Manager Service. Por ejemplo, <code>win service -i -h load_balancer_manager_service.mycompany.com:443 -p ssl</code> .
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el número de puerto de la máquina de Manager Service. Por ejemplo, <code>win service -i -h manager_service_machine.mycompany.com:443 -p ssl</code> .
Si prepara una imagen de máquina de Amazon	Necesita especificar que está usando Amazon. Por ejemplo, <code>win service -i -h manager_service_machine.mycompany.com:443:443 -p ssl -c ec2</code>

Resultados

El nombre del servicio de Windows es VCACGuestAgentService. Puede buscar el log de instalación VCAC-GuestAgentService.log en C:\VRMGuestAgent.

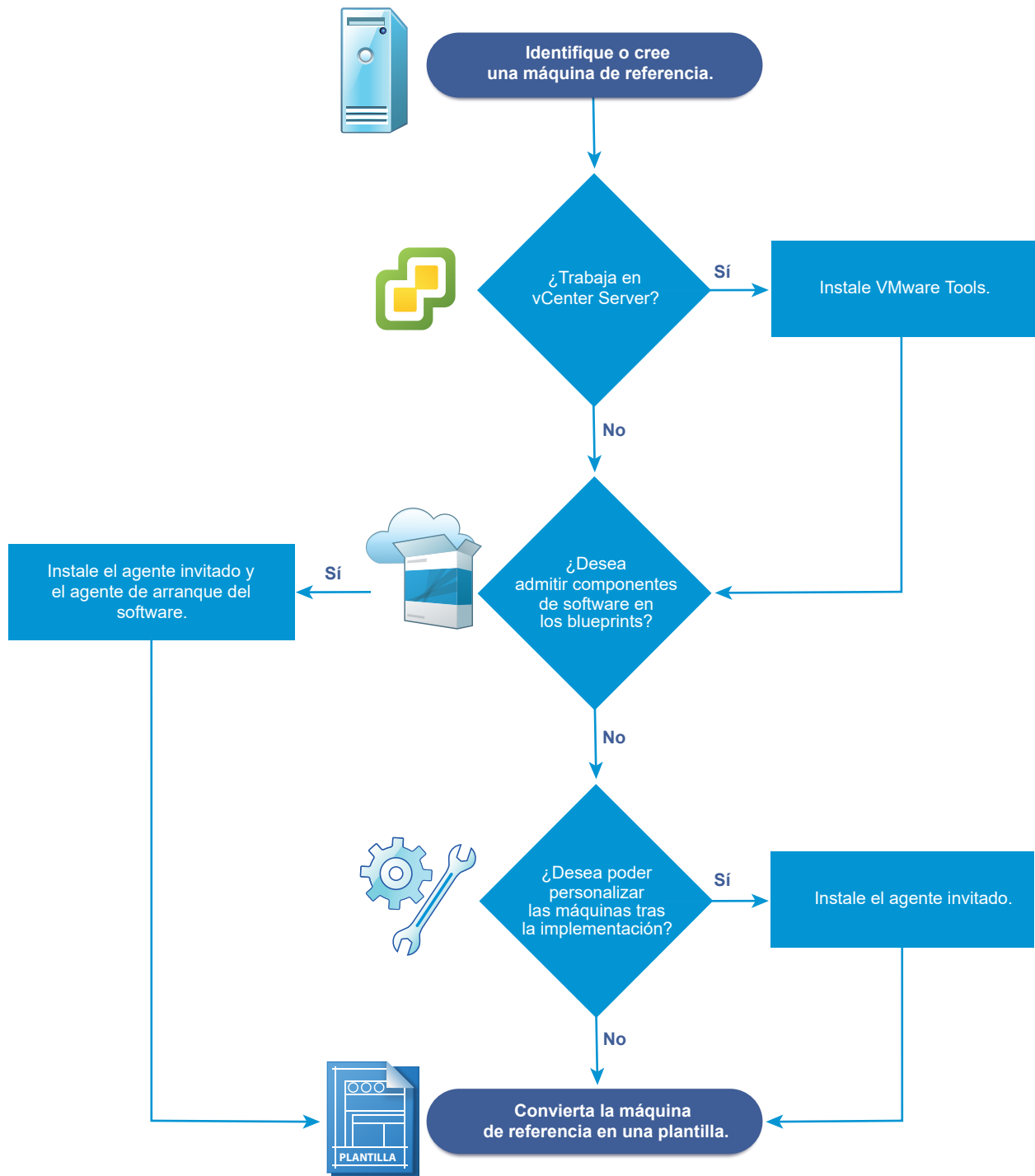
Pasos siguientes

Convierta la máquina de referencia en una plantilla para clonar un snapshot o una imagen de máquina de Amazon para que los arquitectos de IaaS puedan usarla cuando creen blueprints.

Lista de comprobación para preparar el aprovisionamiento mediante clonación

Es necesario realizar algunos preparativos fuera de vRealize Automation para crear la plantilla y los objetos de personalización que se usan para clonar las máquinas virtuales Linux y Windows.

La clonación requiere una plantilla de la cual se clonará, que debe crearse a partir de una máquina de referencia.



Si piensa aprovisionar una máquina Windows mediante clonación, el único modo de unir la máquina aprovisionada a un dominio de Active Directory es a través de la especificación de personalización de vCenter Server o la inclusión de un perfil de sistema operativo invitado en la plantilla de SCVMM. Las máquinas aprovisionadas mediante clonación no se pueden ubicar en el contenedor de Active Directory durante el aprovisionamiento. Debe hacerlo manualmente después del aprovisionamiento.

Tabla 1-8. Lista de comprobación para preparar el aprovisionamiento mediante clonación

Tarea	Ubicación	Detalles
<input type="checkbox"/> Identificar o crear la máquina de referencia.	Hipervisor	Consulte la documentación que le ha proporcionado el hipervisor.
<input type="checkbox"/> (Opcional) Si desea que su plantilla de clonación admita componentes de Software, instale el agente invitado y el agente de arranque del software de vRealize Automation en su máquina de referencia.	Máquina de referencia	<p>Para máquinas Windows de referencia, consulte Preparar una máquina Windows de referencia para que sea compatible con el Software.</p> <p>Para máquinas Linux de referencia, consulte Preparar una máquina Linux de referencia para que sea compatible con Software.</p>
<input type="checkbox"/> (Opcional) Si no desea que la plantilla de clonación admita componentes de Software, pero desea poder personalizar las máquinas implementadas, instale el agente invitado de vRealize Automation en su máquina de referencia.	Máquina de referencia	Consulte Usar el agente invitado de vRealize Automation durante el aprovisionamiento .
<input type="checkbox"/> Si trabaja en un entorno de vCenter Server, instale VMware Tools en la máquina de referencia.	vCenter Server	Consulte la documentación de VMware Tools.
<input type="checkbox"/> Usar la máquina de referencia para crear una plantilla para la clonación.	Hipervisor	<p>La máquina de referencia puede estar encendida o apagada. Si va a clonar en vCenter Server, puede usar una máquina de referencia directamente sin crear una plantilla.</p> <p>Consulte la documentación que le ha proporcionado el hipervisor.</p>
<input type="checkbox"/> Crear el objeto de personalización para configurar las máquinas clonadas mediante la aplicación de la información de la utilidad de preparación del sistema o una personalización de Linux.	Hipervisor	<p>Si va a clonar para Linux, puede instalar el agente invitado de Linux y proporcionar scripts de personalización externos en vez de crear un objeto de personalización. Si va a clonar con vCenter Server, debe proporcionar la especificación de personalización como el objeto de personalización.</p> <p>Consulte la documentación que le ha proporcionado el hipervisor.</p>
<input type="checkbox"/> Recopilar la información necesaria para crear blueprints que clonen la plantilla.	La información se captura y transfiere a los arquitectos de IaaS.	Consulte Hoja de trabajo para el aprovisionamiento virtual mediante clonación .

Hoja de trabajo para el aprovisionamiento virtual mediante clonación

Rellene la hoja de trabajo de transferencia de conocimientos para capturar información sobre la plantilla, personalizaciones y propiedades personalizadas para crear blueprints de clon para las plantillas que ha preparado en su entorno. No se requiere la totalidad de esta información para cada implementación. Utilice esta hoja de trabajo como guía o bien copie y pegue las tablas de la hoja de trabajo en una herramienta de procesamiento de texto para su edición.

Información de reserva y plantilla necesaria

Tabla 1-9. Hoja de trabajo de información de reserva y plantilla necesaria

Información necesaria	Mi valor	Detalles
Nombre de la plantilla		
Reservas en las que la plantilla está disponible o política de reserva que se aplicará		Para evitar errores durante el aprovisionamiento, asegúrese de que la plantilla esté disponible en todas las reservas, o cree políticas de reserva que los arquitectos puedan usar para restringir las reservas de blueprints a las ubicaciones donde la plantilla esté disponible.
(Solo vSphere) Tipo de clonación solicitada para esta plantilla		<ul style="list-style-type: none"> ■ Clonar ■ Clon vinculado ■ NetApp FlexClone
Nombre de especificación de la personalización (necesario para clonar con direcciones IP estáticas)		No es posible realizar personalizaciones de máquinas Windows sin un objeto de especificación de personalización.
(Solo SCVMM) Nombre ISO		
(Solo SCVMM) Disco duro virtual		
(Solo SCVMM) Perfil de hardware para adjuntar a las máquinas aprovisionadas		

Grupos de propiedades necesarias

Puede completar las secciones de información de propiedad personalizada de la hoja de trabajo o bien puede crear grupos de propiedades y solicitar a los arquitectos que añadan sus grupos de propiedades a sus blueprints en lugar de varias propiedades personalizadas individuales.

Sistema operativo de vCenter Server necesario

Debe proporcionar la propiedad personalizada del sistema operativo invitado para el aprovisionamiento de vCenter Server.

Tabla 1-10. Sistema operativo de vCenter Server

Propiedad personalizada	Mi valor	Descripción
VMware.VirtualCenter.OperatingSystem		Especifica la versión del sistema operativo invitado de vCenter Server (VirtualMachineGuestOsIdentifier) con el que vCenter Server crea la máquina. Esta versión de sistema operativo debe ser la misma que la versión de sistema operativo que se va a instalar en la máquina aprovisionada. Los administradores pueden crear grupos de propiedades utilizando uno de los diferentes conjuntos de propiedades (por ejemplo, VMware[OS_Version]Properties) que hay predefinidos para incluir los valores de VMware.VirtualCenter.OperatingSystem correctos. Esta propiedad está pensada para el aprovisionamiento virtual.

Información de script de Visual Basic

Si ha configurado vRealize Automation para ejecutar sus scripts de Visual Basic personalizados como pasos adicionales en el ciclo de vida de la máquina, debe incluir información acerca de los scripts en el blueprint.

Nota Un administrador de tejido puede crear un grupo de propiedades mediante los conjuntos de propiedades ExternalPreProvisioningVbScript y ExternalPostProvisioningVbScript para proporcionar la información necesaria. De este modo, será más fácil que los arquitectos de blueprints incluyan esta información correctamente en sus blueprints.

Tabla 1-11. Información de script de Visual Basic

Propiedad personalizada	Mi valor	Descripción
ExternalPreProvisioningVbScript		Ejecute un script antes del aprovisionamiento. Introduzca la ruta completa al script, incluido el nombre de archivo y la extensión. <i>%Unidad del sistema%Archivos de programa (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs.</i>
ExternalPostProvisioningVbScript		Ejecute un script después del aprovisionamiento. Introduzca la ruta completa al script, incluido el nombre de archivo y la extensión. <i>%Unidad del sistema%Archivos de programa (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs</i>

Información de script de personalización del agente invitado de Linux

Si ha configurado su plantilla de Linux para usar el agente invitado para ejecutar scripts de personalización, debe incluir información acerca de los scripts en el blueprint.

Tabla 1-12. Hoja de trabajo de información de script de personalización del agente invitado de Linux

Propiedad personalizada	Mi valor	Descripción
Linux.ExternalScript.Name		<p>Especifica el nombre de un script de personalización opcional (por ejemplo <code>config.sh</code>), que el agente invitado de Linux ejecuta después de que el sistema operativo se haya instalado. Esta propiedad está disponible para las máquinas de Linux clonadas a partir de plantillas en las que el agente de Linux está instalado.</p> <p>Si especifica un script externo, deberá definir también dónde se ubica utilizando las propiedades <code>Linux.ExternalScript.LocationType</code> y <code>Linux.ExternalScript.Path</code>.</p>
Linux.ExternalScript.LocationType		<p>Especifica el tipo de ubicación del script de personalización nombrado en la propiedad <code>Linux.ExternalScript.Name</code>. Puede ser local o NFS.</p> <p>También hay que especificar la ubicación del script mediante la propiedad <code>Linux.ExternalScript.Path</code>. Si el tipo de ubicación es NFS, use también la propiedad <code>Linux.ExternalScript.Server</code>.</p>
Linux.ExternalScript.Server		<p>Especifica el nombre del servidor NFS (por ejemplo, <code>lab-ad.lab.local</code>) en el que se encuentra el script de personalización externo de Linux nombrado en <code>Linux.ExternalScript.Name</code>.</p>
Linux.ExternalScript.Path		<p>Especifica la ruta local al script de personalización de Linux o la ruta externa al script de personalización de Linux en el servidor NFS. El valor debe empezar por una barra diagonal y no incluir el nombre de archivo (por ejemplo, <code>/scripts/linux/config.sh</code>).</p>

Otras propiedades personalizadas del agente invitado

Si ha instalado el agente invitado en su máquina de referencia, puede usar las propiedades personalizadas para personalizar las máquinas aún más tras la implementación.

Tabla 1-13. Hoja de trabajo de propiedades personalizadas para personalizar máquinas clonadas con un agente invitado

Propiedad personalizada	Mi valor	Descripción
<code>VirtualMachine.Admin.AddOwnerToAdmins</code>		Establézcala en True (valor predeterminado) para añadir el propietario de la máquina (según está especificado en la propiedad <code>VirtualMachine.Admin.Owner</code>) al grupo de administradores locales de la máquina.
<code>VirtualMachine.Admin.AllowLogin</code>		Establézcala en True (valor predeterminado) para añadir el propietario de la máquina (según está especificado en la propiedad <code>VirtualMachine.Admin.Owner</code>) al grupo de usuarios de escritorio remoto.
<code>VirtualMachine.Admin.UseGuestAgent</code>		Si el agente invitado se instala como un servicio en una plantilla para la clonación, establézcala en True en el blueprint de máquina para habilitar el servicio de agente invitado en máquinas clonadas a partir de esa plantilla. Cuando la máquina se inicie, lo hará también el servicio de agente invitado. Establézcala en False para desactivar el agente invitado. Si se establece en False, el flujo de trabajo de clon mejorado no utilizará el agente invitado en las tareas de sistema operativo invitado, lo que reduce su funcionalidad a <code>VMwareCloneWorkflow</code> . Si no se especifica ni establece en otra opción distinta de False, el flujo de trabajo de clon mejorado envía elementos de trabajo al agente invitado.
<code>VirtualMachine.DiskN.Active</code>		Establézcala en True (valor predeterminado) para especificar que el disco <i>N</i> de la máquina está activo. Establézcala en False para especificar que el disco <i>N</i> de la máquina no está activo.
<code>VirtualMachine.DiskN.Label</code>		Especifica la etiqueta del disco <i>N</i> de una máquina. El número máximo de caracteres de la etiqueta de disco es 32. La numeración de discos debe ser secuencial. Cuando se usa con un agente invitado, especifica la etiqueta del disco <i>N</i> de una máquina dentro del sistema operativo invitado.

Tabla 1-13. Hoja de trabajo de propiedades personalizadas para personalizar máquinas clonadas con un agente invitado (continuación)

Propiedad personalizada	Mi valor	Descripción
<code>VirtualMachine.DiskN.Letter</code>		Especifica la letra de unidad o el punto de montaje del disco <i>N</i> de una máquina. El valor predeterminado es C. Por ejemplo, para especificar la letra D para Disco 1, defina la propiedad personalizada como <code>VirtualMachine.Disk1.Letter</code> y escriba el valor D. La numeración de discos debe ser secuencial. Cuando se usa junto con un agente invitado, este valor especifica la letra de unidad o el punto de montaje donde el agente invitado va a montar un disco <i>N</i> adicional en el sistema operativo invitado.
<code>VirtualMachine.Admin.CustomizeGuestOSDelay</code>		Especifica el tiempo que debe transcurrir entre que una personalización se completa y que la personalización de sistema operativo invitado se inicia. Este valor debe tener el formato HH:MM:SS. Si no se establece ningún valor, el valor predeterminado es un minuto (00:01:00). Si decide no incluir esta propiedad personalizada, se puede producir un error de aprovisionamiento en caso de que la máquina virtual se reinicie antes que los elementos de trabajo del agente invitado finalicen.
<code>VirtualMachine.Customize.WaitCompletion</code>		Establézcala en True para impedir que el flujo de trabajo de aprovisionamiento envíe elementos de trabajo al agente invitado hasta que todas las personalizaciones se hayan completado.
<code>VirtualMachine.SoftwareN.Name</code>		Especifica el nombre descriptivo de una aplicación de software <i>N</i> o script que se va a instalar o ejecutar durante el aprovisionamiento. Esta propiedad es opcional y tiene un carácter meramente informativo. No realiza ninguna función real para el flujo de trabajo de clon mejorado o el agente invitado, pero sí resulta útil en una selección de software personalizada en una interfaz de usuario o en la elaboración de informes de uso de software.

Tabla 1-13. Hoja de trabajo de propiedades personalizadas para personalizar máquinas clonadas con un agente invitado (continuación)

Propiedad personalizada	Mi valor	Descripción
VirtualMachine.SoftwareN.ScriptPath		<p>Especifica la ruta completa de un script de instalación de una aplicación. La ruta debe ser una ruta absoluta válida según el sistema operativo invitado y debe incluir el nombre del archivo de script.</p> <p>Puede transferir valores de propiedad personalizada como parámetros al script si inserta {CustomPropertyName} en la cadena de la ruta. Por ejemplo, si tiene una propiedad personalizada denominada ActivationKey cuyo valor es 1234, la ruta de script es D:\InstallApp.bat -key {ActivationKey}. El agente invitado ejecuta el comando D:\InstallApp.bat -key 1234. Posteriormente, el archivo de script se puede programar para aceptar y usar este valor.</p>
VirtualMachine.SoftwareN.ISOName		<p>Especifica la ruta y el nombre de archivo del archivo ISO relativo a la raíz de almacén de datos. El formato es <i>folder_name/subfolder_name/file_name.iso</i>. Si no se especifica ningún valor, la imagen ISO no se montará.</p>
VirtualMachine.SoftwareN.ISOLocation		<p>Especifica la ruta de almacenamiento que contiene el archivo de imagen ISO que la aplicación o el script va a usar. Use un formato en la ruta según aparece en la reserva de host, por ejemplo, <i>netapp-1:it_nfs_1</i>. Si no se especifica ningún valor, la imagen ISO no se montará.</p>

Propiedades personalizadas de red

Puede utilizar propiedades personalizadas para especificar la configuración de dispositivos de red específicos en una máquina.

Las propiedades personalizadas comunes relacionadas con redes se enumeran en la tabla siguiente. Para conocer propiedades personalizadas adicionales y relacionadas, consulte las *propiedades personalizadas de los blueprints de clon* y *propiedades personalizadas de redes* en *Referencia de propiedades personalizadas*.

Tabla 1-14. Propiedades personalizadas de configuración de redes

Propiedad personalizada	Mi valor	Descripción
<code>VirtualMachine.NetworkN.Address</code>		Especifica la dirección IP del dispositivo de red <i>N</i> en una máquina aprovisionada con una dirección IP estática.
<code>VirtualMachine.NetworkN.MacAddressType</code>		<p>Indica si la dirección MAC del dispositivo de red <i>N</i> se genera, o bien está definida por el usuario (es estática). Esta propiedad está disponible para la clonación.</p> <p>El valor predeterminado se genera. Si el valor es estático, también se debe usar</p> <p><code>VirtualMachine.NetworkN.MacAddress</code> para especificar la dirección MAC.</p> <p>Las propiedades personalizadas <code>VirtualMachine.NetworkN</code> son específicas de blueprints y máquinas individuales. Cuando se solicita una máquina, la asignación de direcciones IP y de red se realiza antes de que dicha máquina se asigne a una reserva. No utilice esta propiedad en una reserva, dado que no es seguro que los blueprints vayan a estar asignados a una reserva concreta. No se admite esta propiedad para redes enrutadas a petición o NAT a petición.</p>

Tabla 1-14. Propiedades personalizadas de configuración de redes (continuación)

Propiedad personalizada	Mi valor	Descripción
VirtualMachine.NetworkN.MacAddress		<p>Especifica la dirección MAC de un dispositivo de red <i>N</i>. Esta propiedad está disponible para la clonación.</p> <p>Si el valor de VirtualMachine.NetworkN.MacAddressType se genera, esta propiedad contiene la dirección generada.</p> <p>Si el valor de VirtualMachine.NetworkN.MacAddressType es, por contra, estático, esta propiedad especifica la dirección MAC. En el caso de las máquinas virtuales aprovisionadas en hosts de ESX Server, la dirección debe estar dentro del rango especificado por VMware. Para ver más detalles, consulte la documentación de vSphere.</p> <p>Las propiedades personalizadas VirtualMachine.NetworkN son específicas de blueprints y máquinas individuales. Cuando se solicita una máquina, la asignación de direcciones IP y de red se realiza antes de que dicha máquina se asigne a una reserva. No utilice esta propiedad en una reserva, dado que no es seguro que los blueprints vayan a estar asignados a una reserva concreta. No se admite esta propiedad para redes enrutadas a petición o NAT a petición.</p>

Tabla 1-14. Propiedades personalizadas de configuración de redes (continuación)

Propiedad personalizada	Mi valor	Descripción
<code>VirtualMachine.NetworkN.Name</code>		<p>Especifica el nombre de la red con la que se va a establecer la conexión, por ejemplo, el dispositivo de red <i>N</i> al que una máquina se conecta. Esto equivale a una tarjeta de interfaz de red (NIC).</p> <p>Una red se asigna de forma predeterminada desde las rutas de red disponibles en la reserva en la que la máquina se aprovisiona. Consulte también <code>VirtualMachine.NetworkN.AddressType</code>.</p> <p>Si establece el valor de esta propiedad en el nombre de una red en una reserva disponible, garantizará que va a haber un dispositivo de red conectado a una red específica. Por ejemplo, si establece propiedades en <code>N=0</code> y <code>1</code>, obtendrá 2 NIC y su valor asignado, siempre que la red esté seleccionada en la reserva asociada.</p> <p>Las propiedades personalizadas <code>VirtualMachine.NetworkN</code> son específicas de blueprints y máquinas. Cuando se solicita una máquina, la asignación de direcciones IP y de red se realiza antes de que dicha máquina se asigne a una reserva. No utilice esta propiedad en una reserva, dado que no es seguro que los blueprints vayan a estar asignados a una reserva concreta. No se admite esta propiedad para redes enrutadas a petición o NAT a petición.</p> <p>Si desea obtener un ejemplo de cómo utilizar esta propiedad personalizada para configurar <code>VirtualMachine.Network0.Name</code> de forma dinámica con base en la selección que realiza un consumidor a partir de una lista de redes disponibles predefinidas, consulte la publicación de blog correspondiente a la adición de una lista desplegable de selección de redes en vRA 7.</p>

Tabla 1-14. Propiedades personalizadas de configuración de redes (continuación)

Propiedad personalizada	Mi valor	Descripción
VirtualMachine.NetworkN.PortID		<p>Especifica el ID de puerto que se va a usar en el dispositivo de red <i>N</i> cuando se usa un grupo de dvPort con una instancia de vSphere Distributed Switch.</p> <p>Las propiedades personalizadas VirtualMachine.NetworkN son específicas de blueprints y máquinas individuales. Cuando se solicita una máquina, la asignación de direcciones IP y de red se realiza antes de que dicha máquina se asigne a una reserva. No utilice esta propiedad en una reserva, dado que no es seguro que los blueprints vayan a estar asignados a una reserva concreta. No se admite esta propiedad para redes enrutadas a petición o NAT a petición.</p>
VirtualMachine.NetworkN.NetworkProfileName		<p>Especifica el nombre de un perfil de red del que se asigna una dirección IP estática al dispositivo de red <i>N</i> o del que se obtiene un rango de direcciones IP estáticas que se pueden asignar al dispositivo de red <i>N</i> de una máquina clonada, donde <i>N</i>=0 corresponde al primer dispositivo, 1 al segundo y así sucesivamente.</p> <p>El perfil de red al que apunta la propiedad se utiliza para asignar una dirección IP. La propiedad determina la red a la que conecta la máquina, según la reserva.</p>

Tabla 1-14. Propiedades personalizadas de configuración de redes (continuación)

Propiedad personalizada	Mi valor	Descripción
<ul style="list-style-type: none"> ■ VirtualMachine.NetworkN.SubnetMask ■ VirtualMachine.NetworkN.Gateway ■ VirtualMachine.NetworkN.PrimaryDns ■ VirtualMachine.NetworkN.SecondaryDns ■ VirtualMachine.NetworkN.PrimaryWins ■ VirtualMachine.NetworkN.SecondaryWins ■ VirtualMachine.NetworkN.DnsSuffix ■ VirtualMachine.NetworkN.DnsSearchSuffixes 		<p>Si anexa un nombre a una propiedad personalizada, podrá crear varias versiones de dicha propiedad. Por ejemplo, las siguientes propiedades pueden mostrar una lista de los grupos de equilibrio de carga definidos para un uso general y máquinas con requisitos de rendimiento alto, medio y bajo:</p> <ul style="list-style-type: none"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low <p>Configura atributos del perfil de red especificado en VirtualMachine.NetworkN.NetworkProfileName.</p>
VCNS.LoadBalancerEdgePool.Names.name		<p>Especifica los grupos de equilibrio de carga de NSX a los que la máquina virtual se asigna durante el aprovisionamiento. La máquina virtual se asigna a todos los puertos de servicio de todos los grupos especificados. El valor es un nombre de <i>edge/pool</i> o una lista de nombres de <i>edge/pool</i> separados por comas. En estos nombres se distingue entre mayúsculas y minúsculas.</p> <p>Si anexa un nombre a una propiedad personalizada, podrá crear varias versiones de dicha propiedad. Por ejemplo, las siguientes propiedades pueden mostrar una lista de los grupos de equilibrio de carga definidos para un uso general y máquinas con requisitos de rendimiento alto, medio y bajo:</p> <ul style="list-style-type: none"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low

Tabla 1-14. Propiedades personalizadas de configuración de redes (continuación)

Propiedad personalizada	Mi valor	Descripción
VCNS.SecurityGroup.Names.name		<p>Especifica el grupo o los grupos de seguridad de NSX a los que la máquina virtual se asigna durante el aprovisionamiento. El valor es un nombre de grupo de seguridad o una lista de nombres separados por comas. En estos nombres se distingue entre mayúsculas y minúsculas.</p> <p>Si anexa un nombre a una propiedad personalizada, podrá crear varias versiones de dicha propiedad que se pueden usar de forma conjunta o por separado. Por ejemplo, las siguientes propiedades pueden mostrar una lista de los grupos de seguridad pensados para un uso general, para fuerza de ventas y para soporte:</p> <ul style="list-style-type: none"> ■ VCNS.SecurityGroup.Names ■ VCNS.SecurityGroup.Names.sales ■ VCNS.SecurityGroup.Names.support
VCNS.SecurityTag.Names.name		<p>Especifica la etiqueta o las etiquetas de seguridad de NSX a las que la máquina virtual se asocia durante el aprovisionamiento. El valor es un nombre de etiqueta de seguridad o una lista de nombres separados por comas. En estos nombres se distingue entre mayúsculas y minúsculas.</p> <p>Si anexa un nombre a una propiedad personalizada, podrá crear varias versiones de dicha propiedad que se pueden usar de forma conjunta o por separado. Por ejemplo, las siguientes propiedades pueden mostrar una lista de las etiquetas de seguridad pensadas para un uso general, para fuerza de ventas y para soporte:</p> <ul style="list-style-type: none"> ■ VCNS.SecurityTag.Names ■ VCNS.SecurityTag.Names.sales ■ VCNS.SecurityTag.Names.support

Preparar el aprovisionamiento de vCloud Air y vCloud Director

Para preparar el aprovisionamiento de máquinas de vCloud Air y vCloud Director mediante vRealize Automation, debe configurar el centro de datos virtual de la organización con plantillas y objetos de personalización.

Para aprovisionar recursos de vCloud Air y vCloud Director mediante vRealize Automation, la organización requiere una plantilla a partir de la que realizar la clonación, que consiste en uno o varios recursos de máquinas.

Las plantillas que se comparten entre organizaciones deben ser públicas. Solo se pueden usar plantillas reservadas como origen de clonación para vRealize Automation.

Nota Cuando se crea un blueprint mediante la clonación de una plantilla, el identificador exclusivo de esa plantilla se asocia al blueprint. Cuando el blueprint se publica en el catálogo de vRealize Automation y se usa en los procesos de aprovisionamiento y de recopilación de datos, se reconoce la plantilla asociada. Si elimina la plantilla en vCloud Air o vCloud Director, los procesos de aprovisionamiento y de recopilación de datos de vRealize Automation posteriores no se realizarán correctamente debido a que la plantilla asociada ya no existe. En lugar de eliminar y volver a crear una plantilla, para cargar una versión actualizada, por ejemplo, sustituya la plantilla mediante el proceso de sustitución de plantillas de vCloud Air o vCloud Director. Si usa vCloud Air o vCloud Director para sustituir la plantilla, en vez de eliminarla y volver a crearla, el identificador exclusivo de esta se conservará intacto y el aprovisionamiento y la recopilación de datos seguirán funcionando.

La siguiente descripción general expone los pasos que debe seguir antes de usar vRealize Automation para crear endpoints y definir reservas y blueprints. Para obtener más información acerca de estas tareas administrativas, consulte la documentación de producto de vCloud Air y vCloud Director.

- 1 En vCloud Air o vCloud Director, cree una plantilla de clonación y añádala al catálogo de la organización.
- 2 En vCloud Air o vCloud Director, use la plantilla para especificar la configuración personalizada, como las contraseñas, el dominio y los scripts del sistema operativo invitado, en cada máquina.

Puede usar vRealize Automation para reemplazar los ajustes.

La personalización depende del sistema operativo invitado del recurso.

- 3 En vCloud Air o vCloud Director, configure el catálogo para compartirlo con todos los usuarios de la organización.

En vCloud Air o vCloud Director, configure el acceso de administrador de cuenta a las organizaciones que corresponda para permitir que todos los usuarios y los grupos de la organización tengan acceso al catálogo. Sin esta designación de uso compartido, los arquitectos de blueprints o endpoints no podrán ver las plantillas del catálogo en vRealize Automation.

- 4 Recopile la siguiente información para incluirla en los blueprints:

- El nombre de la plantilla de vCloud Air o vCloud Director.
- La cantidad de almacenamiento total especificada para la plantilla.

Preparar el aprovisionamiento de Kickstart de Linux

El aprovisionamiento de Kickstart de Linux usa un archivo de configuración para automatizar la instalación de Linux en una máquina aprovisionada reciente. Para preparar el aprovisionamiento, debe crear una imagen ISO de arranque y un archivo de configuración Kickstart o autoYaST.

A continuación se presenta un resumen de alto nivel de los pasos requeridos para preparar el aprovisionamiento de Kickstart de Linux:

- 1 Compruebe que hay un servidor DHCP disponible en la red. vRealize Automation no puede aprovisionar máquinas mediante el aprovisionamiento Kickstart de Linux a menos que DHCP esté disponible.
- 2 Prepare el archivo de configuración. En el archivo de configuración, debe especificar las ubicaciones del servidor de vRealize Automation y del paquete de instalación del agente de Linux. Consulte [Preparar el archivo de muestra de configuración de Kickstart de Linux](#).
- 3 Edite el archivo `isolinux/isolinux.cfg` o `loader/isolinux.cfg` para especificar el nombre y la ubicación del archivo de configuración y el origen de distribución de Linux apropiado.
- 4 Cree la imagen ISO de arranque y guárdela en la ubicación requerida por la plataforma de virtualización. Consulte la documentación que le ha proporcionado su hipervisor para obtener información sobre la ubicación requerida.
- 5 (opcional) Añada scripts de personalización.
 - a Para especificar scripts de personalización posteriores a la instalación en el archivo de configuración, consulte [Especificar scripts personalizados en un archivo de configuración de kickstart/autoYaST](#).
 - b Para llamar a los scripts de Visual Basic en el blueprint, consulte [Lista de comprobación para ejecutar scripts de Visual Basic durante el aprovisionamiento](#).
- 6 Recopile la siguiente información para que los arquitectos de blueprints la incluyan en sus blueprints:
 - a El nombre y la ubicación de la imagen ISO.
 - b Para integraciones de vCenter Server, la versión del sistema operativo invitado de vCenter Server con el que vCenter Server creará la máquina.

Nota Puede crear un grupo de propiedades con el conjunto de propiedades `BootIsoProperties` para incluir la información del archivo ISO necesaria. De este modo será más fácil incluir la información correctamente en los blueprints.

Preparar el archivo de muestra de configuración de Kickstart de Linux

vRealize Automation proporciona archivos de configuración de muestra que puede modificar y editar para ajustarlos a sus necesidades. Se deben realizar varios cambios para poder usar los archivos.

Procedimiento

- 1 Desplácese hasta la página de la consola de administración del dispositivo de vRealize Automation.

Por ejemplo: `https://va-hostname.domain.com`.

- 2 Haga clic en la **página del agente invitado y el agente de software** en la sección de instalación de componentes de vRealize Automation de la página.

Por ejemplo: `https://va-hostname.domain.com/software/index.html`.

Se abre la página de los **instaladores del agente invitado y del agente de software**, donde se proporcionan vínculos a descargas disponibles.

- 3 Haga clic en los **paquetes de agentes invitados de Linux** en la sección de los instaladores de agentes invitados de la página para descargar y guarde el archivo `LinuxGuestAgentPkgs.zip`.

- 4 Descomprima el archivo `LinuxGuestAgentPkgs.zip` descargado para crear la carpeta `VraLinuxGuestAgent`.

- 5 Navegue hasta el subdirectorio `VraLinuxGuestAgent` que corresponde al sistema operativo invitado para implementar durante el aprovisionamiento.

Por ejemplo: `rhel32`.

- 6 Abra un archivo en el subdirectorio de muestras que corresponde a su sistema de destino.

Por ejemplo, `samples/sample-https-rhel6-x86.cfg`.

- 7 Reemplace todas las instancias de la cadena `host=dcac.example.net` con la dirección IP o el nombre de dominio completo y el número de puerto para el Manager Service, o con el equilibrador de carga para el Manager Service.

Plataforma	Formato requerido
vSphere ESXi	Dirección IP, por ejemplo: <code>--host=172.20.9.59</code>
vSphere ESX	Dirección IP, por ejemplo: <code>--host=172.20.9.58</code>
SUSE 10	Dirección IP, por ejemplo: <code>--host=172.20.9.57</code>
Todas las demás	FQDN, por ejemplo: <code>--host=mycompany-host1.mycompany.local:443</code>

- 8 Encuentre cada instancia de `gugent.rpm` o `gugent.tar.gz` y reemplace la URL `rpm.example.net` con la ubicación del paquete de agente invitado.

Por ejemplo:

```
rpm -i nfs:172.20.9.59/suseagent/gugent.rpm
```

- 9 Guarde el archivo en una ubicación a la que puedan acceder las máquinas aprovisionadas recientes.

Especificar scripts personalizados en un archivo de configuración de kickstart/autoYaST

Puede modificar el archivo de configuración para copiar o instalar scripts personalizados en máquinas recién aprovisionadas. El agente de Linux ejecuta los scripts en el punto especificado del flujo de trabajo.

El script puede hacer referencia a cualquiera de los directorios `./properties.xml` de los directorios `/usr/share/gugent/site/workitem`.

Requisitos previos

- Prepare un archivo de configuración de kickstart o autoYaST. Consulte [Preparar el archivo de muestra de configuración de Kickstart de Linux](#).
- El script debe devolver un valor distinto de cero en caso de error para evitar un error de aprovisionamiento de máquina.

Procedimiento

- 1 Cree o identifique el script que desea usar.
- 2 Guarde el script como *NN_scriptname*.

NN es un número de dos dígitos. Los scripts se ejecutan en orden de inferior a superior. Si dos scripts tienen el mismo número, se sigue el orden alfabético según *scriptname*.
- 3 Haga que el script sea ejecutable.
- 4 Busque la sección posterior a la instalación de su archivo de configuración de kickstart o autoYaST.

En kickstart, se indica mediante `%post`. En autoYaST, se indica mediante `post-scripts`.

- 5 Modifique la sección posterior a la instalación del archivo de configuración para copiar o instalar el script en el directorio `/usr/share/gugent/site/workitem` que elija.

Los scripts personalizados suelen ejecutarse para kickstart/autoYaST virtual con los elementos de trabajo SetupOS (para crear el aprovisionamiento) y CustomizeOS (para clonar el aprovisionamiento), pero puede ejecutar scripts en cualquier punto del flujo de trabajo.

Por ejemplo, puede modificar el archivo de configuración para copiar el script `11_addusers.sh` al directorio `/usr/share/gugent/site/SetupOS` de una máquina recién aprovisionada mediante el siguiente comando:

```
cp nfs:172.20.9.59/linuxscripts/11_addusers.sh /usr/share/gugent/site/SetupOS
```

Resultados

El agente de Linux ejecuta el script en el orden especificado por el directorio de elemento de trabajo y el nombre de archivo del script.

Preparar el aprovisionamiento de SCCM

vRealize Automation arranca una máquina aprovisionada reciente desde una imagen ISO y luego transfiere el control de la secuencia de tareas de SCCM especificada.

El aprovisionamiento de SCCM es compatible con la implementación de sistemas operativos Windows. Linux no es compatible. La distribución y las actualizaciones de software no son compatibles.

A continuación se presenta un resumen de alto nivel de los pasos requeridos para preparar el aprovisionamiento de SCCM:

- 1 La comunicación con SCCM requiere el nombre de NetBIOS del servidor SCCM.

Trabaje con el administrador de red para asegurarse de que al menos una instancia de Distributed Execution Manager (DEM) pueda resolver el FQDN del servidor SCCM en su nombre de NetBIOS.

No es necesario colocar las instancias de DEM directamente en la misma red que el servidor SCCM, pero deben poder comunicarse con el servidor SCCM por IP.

- 2 Cree un paquete de software que incluya el agente invitado de vRealize Automation. Consulte [Crear un paquete de software para el aprovisionamiento de SCCM](#).
- 3 En SCCM, cree la secuencia de tareas deseada para aprovisionar la máquina. El último paso consiste en instalar el paquete de software que ha creado y que contiene el agente invitado de vRealize Automation. Para obtener información acerca de cómo crear secuencias de tareas e instalar paquetes de software, consulte la documentación de SCCM.
- 4 Cree una imagen ISO de arranque sin interacción para la secuencia de tareas. De forma predeterminada, SCCM crea una imagen ISO con poca interacción. Para obtener información sobre la configuración de SCCM para imágenes ISO sin interacción, consulte la documentación de SCCM.
- 5 Copie la imagen ISO en la ubicación requerida por la plataforma de virtualización. Si no sabe cuál es la ubicación correcta, consulte la documentación que le ha facilitado el hipervisor.
- 6 Recopile la siguiente información para que los arquitectos de blueprints la incluyan en los blueprints:
 - a El nombre de la colección que contiene la secuencia de tareas.
 - b El nombre de dominio completo del servidor de SCCM en el que se ubica la colección que contiene la secuencia.
 - c El código de sitio del servidor de SCCM.
 - d Las credenciales de administrador del servidor de SCCM.
 - e (Opcional) La ISO, el disco duro virtual o el perfil de hardware que se asignarán a las máquinas aprovisionadas para integraciones de SCVMM.

Crear un paquete de software para el aprovisionamiento de SCCM

El último paso de la secuencia de tareas de SCCM consiste en instalar un paquete de software que incluya el agente invitado de vRealize Automation.

Procedimiento

- 1 Desplácese hasta la página de la consola de administración del dispositivo de vRealize Automation.
Por ejemplo: <https://va-hostname.domain.com>.
- 2 Haga clic en la **página del agente invitado y el agente de software** en la sección de instalación de componentes de vRealize Automation de la página.
Por ejemplo: <https://va-hostname.domain.com/software/index.html>.
Se abre la página de los **instaladores del agente invitado y del agente de software**, donde se proporcionan vínculos a descargas disponibles.
- 3 Haga clic en los archivos de agentes invitados de Windows (**32 bits** o **64 bits**) en la sección de instalación de componentes de la página para descargar y guarde el archivo `GuestAgentInstaller.exe` o `GuestAgentInstaller_x64.exe`.
- 4 Extraiga los archivos de agente invitado de Windows en una ubicación disponible para SCCM.
Se creará el directorio `C:\VRMGuestAgent`. No cambie el nombre de este directorio.
- 5 Cree un paquete de software a partir del archivo de definición `SCCMPackageDefinitionFile.sms`.
- 6 Ponga este paquete de software disponible en el punto de distribución.
- 7 Seleccione el contenido de los archivos de agente invitado de Windows como archivos de origen.

Preparar el aprovisionamiento de WIM

Aprovisione una máquina mediante el arranque en un entorno WinPE y, a continuación, instale un sistema operativo usando una imagen Windows Imaging File Format (WIM) de una máquina de referencia Windows existente.

A continuación se presenta un resumen de alto nivel de los pasos requeridos para preparar el aprovisionamiento de WIM:

- 1 Identifique o cree el área de almacenamiento provisional. El área de almacenamiento provisional debe ser un directorio de red que se pueda especificar como una ruta de acceso UNC o montar como una unidad de red mediante:
 - La máquina de referencia.
 - El sistema donde se genera la imagen de WinPE.
 - El host de virtualización en el que se aprovisionan las máquinas.

- 2 Asegúrese de que la red contenga un servidor DHCP. vRealize Automation no puede aprovisionar máquinas con una imagen WIM a menos que DHCP esté disponible.
- 3 Identifique o cree la máquina de referencia en la plataforma de virtualización que desea usar para el aprovisionamiento. Para conocer los requisitos de vRealize Automation, consulte [Requisitos de máquina de referencia para el aprovisionamiento WIM](#). Para obtener información sobre la creación de una máquina de referencia, consulte la documentación que le haya facilitado el hipervisor.
- 4 Mediante la System Preparation Utility for Windows, prepare el sistema operativo de la máquina de referencia para la implementación. Consulte [Requisitos de SysPrep para la máquina de referencia](#).
- 5 Cree la imagen WIM de la máquina de referencia. No incluya espacios en el nombre de archivo de la imagen WIM, de lo contrario se producirá un error de aprovisionamiento.
- 6 Cree una imagen WinPE que incluya el agente invitado de vRealize Automation.
 - (opcional) Cree los scripts personalizados que desee usar para personalizar las máquinas aprovisionadas y colóquelos en el directorio de elementos de trabajo adecuado.
 - Si usa VirtIO para interfaces de red o almacenamiento, debe asegurarse de que se han incluido los controladores necesarios en la imagen WinPE y la imagen WIM. Consulte [Preparar el aprovisionamiento WIM con controladores VirtIO](#).

Al crear la imagen de WinPE, debe insertar manualmente el agente invitado de vRealize Automation. Consulte [Introducir manualmente el agente invitado en una imagen de WinPE](#).

- 7 Coloque la imagen WinPE en la ubicación que requiera la plataforma de virtualización. Si desconoce la ubicación, consulte la documentación del hipervisor.
- 8 Recopile la siguiente información para incluirla en el blueprint:
 - a El nombre y la ubicación de la imagen ISO de WinPE.
 - b El nombre del archivo WIM, la ruta UNC del archivo WIM y el índice utilizados para extraer la imagen deseada del archivo WIM.
 - c El nombre de usuario y la contraseña con los que se debe asignar la ruta de la imagen WIM a una unidad de red en la máquina aprovisionada.
 - d (opcional) Si no desea aceptar la letra de unidad predeterminada, K, indique la letra a la que se asignará la ruta de la imagen de WIM en la máquina aprovisionada.
 - e Para integraciones de vCenter Server, la versión del sistema operativo invitado de vCenter Server con el que vCenter Server creará la máquina.

- f (Opcional) La ISO, el disco duro virtual o el perfil de hardware que se asignarán a las máquinas aprovisionadas para integraciones de SCVMM.

Nota Puede crear un grupo de propiedades para incluir toda esta información necesaria. Usar un grupo de propiedades facilita la inclusión de la información correcta en los blueprints.

Procedimiento

1 Requisitos de máquina de referencia para el aprovisionamiento WIM

El aprovisionamiento WIM conlleva crear una imagen WIM a partir de una máquina de referencia. La máquina de referencia debe cumplir los requisitos mínimos para que la imagen WIM funcione para el aprovisionamiento en vRealize Automation.

2 Requisitos de SysPrep para la máquina de referencia

Un archivo de respuesta de SysPrep contiene varias configuraciones necesarias que se utilizan para el aprovisionamiento de WIM.

3 Preparar el aprovisionamiento WIM con controladores VirtIO

Si usa VirtIO para interfaces de red o almacenamiento, debe asegurarse de que se han incluido los controladores necesarios en la imagen WinPE y la imagen WIM. VirtIO normalmente ofrece un mejor rendimiento cuando se aprovisiona mediante KVM (RHEV).

4 Introducir manualmente el agente invitado en una imagen de WinPE

Debe insertar manualmente el agente invitado de vRealize Automation en la imagen WinPE.

Requisitos de máquina de referencia para el aprovisionamiento WIM

El aprovisionamiento WIM conlleva crear una imagen WIM a partir de una máquina de referencia. La máquina de referencia debe cumplir los requisitos mínimos para que la imagen WIM funcione para el aprovisionamiento en vRealize Automation.

A continuación se presenta un resumen de alto nivel de los pasos para preparar una máquina de referencia:

- 1 Si el sistema operativo de la máquina de referencia es Windows Server 2008 R2, Windows Server 2012, Windows 7 o Windows 8, la instalación predeterminada creará una pequeña partición en el disco duro del sistema aparte de la partición principal. vRealize Automation no admite el uso de imágenes WIM creadas en dichas máquinas de referencia de varias particiones. Debe eliminar esa partición durante el proceso de instalación.
- 2 Instale NET 4.5 y el Kit de instalación automatizada de Windows (AIK) para Windows 7 (incluido WinPE 3.0) en la máquina de referencia.
- 3 Si el sistema operativo de la máquina de referencia es Windows Server 2003 o Windows XP, restablezca la contraseña del administrador para que esté en blanco. (No hay contraseña).
- 4 (Opcional) Si desea habilitar la integración de XenDesktop, instale y configure un Citrix Virtual Desktop Agent.

- 5 (Opcional) Se requiere un agente de Instrumental de administración de Windows (WMI) para recopilar ciertos datos de una máquina Windows administrada por vRealize Automation, como por ejemplo el estado de Active Directory del propietario de una máquina. Para asegurar que la administración de las máquinas Windows es correcta, debe instalar un agente de WMI (normalmente en el host de Manager Service) y habilitar el agente para recopilar datos de las máquinas Windows. Consulte *Instalación de vRealize Automation*.

Requisitos de SysPrep para la máquina de referencia

Un archivo de respuesta de SysPrep contiene varias configuraciones necesarias que se utilizan para el aprovisionamiento de WIM.

Tabla 1-15. Configuración necesaria de SysPrep de la máquina de referencia del servidor de Windows o de la máquina de referencia de Windows XP

Configuración de GuiUnattended	Valor
AutoLogon	Sí
AutoLogonCount	1
AutoLogonUsername	<i>username</i> (<i>username</i> y <i>password</i> son las credenciales que se usan para el inicio de sesión automático cuando la máquina recién aprovisionada arranca en el sistema operativo invitado. Se suele usar Administrator).
AutoLogonPassword	<i>password</i> correspondiente a AutoLogonUsername.

Tabla 1-16. Configuración de SysPrep necesaria para las máquinas de referencia que no usan Windows Server 2003 o Windows XP:

Configuración de AutoLogon	Valor
Enabled	Sí
LogonCount	1

Tabla 1-16. Configuración de SysPrep necesaria para las máquinas de referencia que no usan Windows Server 2003 o Windows XP: (continuación)

Configuración de AutoLogon	Valor
Username	<p><i>username</i></p> <p>(<i>username</i> y <i>password</i> son las credenciales que se usan para el inicio de sesión automático cuando la máquina recién aprovisionada arranca en el sistema operativo invitado. Se suele usar Administrator).</p>
Password	<p><i>password</i></p> <p>(<i>username</i> y <i>password</i> son las credenciales que se usan para el inicio de sesión automático cuando la máquina recién aprovisionada arranca en el sistema operativo invitado. Se suele usar Administrator).</p>
<p>Nota Para las máquinas de referencia que usan una plataforma Windows más reciente que Windows Server 2003/Windows XP, debe establecer la contraseña de inicio de sesión automático mediante la propiedad personalizada Sysprep.GuiUnattended.AdminPassword. Una forma cómoda de garantizar que se haga es crear un grupo de propiedades que incluya esta propiedad personalizada para que los administradores de tenant y los administradores de grupos empresariales puedan incluir esta información correctamente en sus blueprints.</p>	

Preparar el aprovisionamiento WIM con controladores VirtIO

Si usa VirtIO para interfaces de red o almacenamiento, debe asegurarse de que se han incluido los controladores necesarios en la imagen WinPE y la imagen WIM. VirtIO normalmente ofrece un mejor rendimiento cuando se aprovisiona mediante KVM (RHEV).

Red Hat Enterprise Virtualization incluye los controladores de Windows para VirtIO, que está ubicados en el directorio `usr/share/virtio-win` del sistema de archivos de Red Hat Enterprise Virtualization Manager. Las herramientas de invitado de Red Hat Enterprise Virtualization también incluyen los controladores, que están ubicados en `/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso`.

El proceso de alto nivel para habilitar el aprovisionamiento basado en WIM con controladores VirtIO es el siguiente:

- 1 Cree una imagen WIM desde una máquina Windows de referencia con controladores VirtIO instalados, o inserte los controladores en una imagen WIM existente.
- 2 Copie los archivos de controladores para VirtIO e inserte los controladores en una imagen de WinPE.
- 3 Cargue el archivo ISO de la imagen WinPE en los dominios de almacenamiento ISO de Red Hat Enterprise Virtualization mediante el comando `rhev-iso-uploader`. Para obtener más información sobre la administración de imágenes ISO en RHEV, consulte la documentación de Red Hat.

- 4 Cree un blueprint de KVM (RHEV) para el aprovisionamiento WIM y seleccione la opción ISO WinPE. Debe incluir la propiedad personalizada `VirtualMachine.Admin.DiskInterfaceType` con el valor **VirtIO**. Un administrador de tejido puede incluir esta información en un grupo de propiedades para incluirla en los blueprints.

Las propiedades personalizadas `Image.ISO.Location` y `Image.ISO.Name` no se usan con los blueprints de KVM (RHEV).

Introducir manualmente el agente invitado en una imagen de WinPE

Debe insertar manualmente el agente invitado de vRealize Automation en la imagen WinPE.

Requisitos previos

- Seleccione un sistema Windows desde el que se pueda acceder al área de almacenamiento provisional que tenga preparada y en el que estén instalados .NET 4.5 y el Kit de instalación automatizada de Windows (AIK) para Windows 7 (WinPE 3.0 incluido).
- Cree una imagen de WinPE.

Procedimiento

1 Insertar el agente invitado en una imagen de WinPE

Debe copiar manualmente los archivos de agente invitado en la imagen de WinPE.

2 Configurar el archivo `doagent.bat`

El archivo `doagent.bat` se debe configurar manualmente.

3 Configurar el archivo `doagentc.bat`

El archivo `doagentc.bat` se debe configurar manualmente.

4 Configurar el archivo de propiedades de agente invitado

Debe configurar manualmente los archivos de propiedades del agente invitado.

Procedimiento

1 Insertar el agente invitado en una imagen de WinPE.

2 Configurar el archivo `doagent.bat`.

3 Configurar el archivo `doagentc.bat`.

4 Configurar el archivo de propiedades de agente invitado.

Insertar el agente invitado en una imagen de WinPE

Debe copiar manualmente los archivos de agente invitado en la imagen de WinPE.

Requisitos previos

- Seleccione un sistema Windows desde el que se pueda acceder al área de almacenamiento provisional que tenga preparada y en el que estén instalados .NET 4.5 y el Kit de instalación automatizada de Windows (AIK) para Windows 7 (WinPE 3.0 incluido).

- Cree una imagen de WinPE.

Procedimiento

- ◆ Descargue e instale el agente invitado de vRealize Automation desde https://vRealize_VA_Hostname_fqdn/software/index.html.
 - a Descargue *GugentZip_version* en la unidad C de la máquina de referencia.
Seleccione *GuestAgentInstaller.exe* (32 bits) o *GuestAgentInstaller_x64.exe* (64 bits) en función de su sistema operativo.
 - b Haga clic con el botón derecho en el archivo y seleccione **Propiedades**.
 - c Haga clic en **General**.
 - d Haga clic en **Desbloquear**.
 - e Extraiga los archivos a C:\.

Se creará el directorio C:\VRMGuestAgent. No cambie el nombre de este directorio.

Pasos siguientes

[Configurar el archivo doagent.bat.](#)

Configurar el archivo doagent.bat

El archivo *doagent.bat* se debe configurar manualmente.

Requisitos previos

[Insertar el agente invitado en una imagen de WinPE.](#)

Procedimiento

- 1 Vaya al directorio *VRMGuestAgent* dentro de la imagen de WinPE.
Por ejemplo: C:\Archivos de programa (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent.
- 2 Haga una copia del archivo *doagent-template.bat* y póngale el nombre *doagent.bat*.
- 3 Abra *doagent.bat* en un editor de texto.

- Reemplace todas las instancias de la cadena `#Dcac Hostname#` por el nombre de dominio completo y el número de puerto del host de IaaS Manager Service.

Opción	Descripción
Si usa un equilibrador de carga	<p>Escriba el nombre de dominio completo y el puerto del equilibrador de carga de IaaS Manager Service. Por ejemplo:</p> <pre>manager_service_LB.mycompany.com:443</pre>
Si no usa un equilibrador de carga	<p>Escriba el nombre de dominio completo y el puerto de la máquina en la que está instalado IaaS Manager Service. Por ejemplo:</p> <pre>manager_service.mycompany.com:443</pre>

- Reemplace todas las instancias de la cadena `#Protocol#` por la cadena `/ssl`.
- Reemplace todas las instancias de la cadena `#Comment#` por la cadena `REM` (`REM` debe ir seguida de un espacio).
- (opcional) Si utiliza certificados autofirmados, quite la marca de comentario del comando `openssl`.

```
echo QUIT | c:\VRMGuestAgent\bin\openssl s_client -connect
```

- Guarde y cierre el archivo.
- Modifique el script `Startnet.cmd` de WinPE de forma que incluya `doagentc.bat` como script personalizado.

Pasos siguientes

[Configurar el archivo doagentc.bat.](#)

Configurar el archivo doagentc.bat

El archivo `doagentc.bat` se debe configurar manualmente.

Requisitos previos

[Configurar el archivo doagentc.bat.](#)

Procedimiento

- Vaya al directorio `VRMGuestAgent` dentro de la imagen de WinPE.
Por ejemplo: `C:\Archivos de programa (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`.
- Haga una copia del archivo `doagentsvc-template.bat` y póngale el nombre `doagentc.bat`.
- Abra `doagentc.bat` en un editor de texto.
- Quite todas las instancias de la cadena `#Comment#`.

- 5 Reemplace todas las instancias de la cadena `#Dcac Hostname#` por el nombre de dominio completo y el número de puerto del host de Manager Service.

El número de puerto predeterminado de Manager Service es 443.

Opción	Descripción
Si usa un equilibrador de carga	<p>Escriba el nombre de dominio completo y el puerto del equilibrador de carga de Manager Service. Por ejemplo:</p> <pre>load_balancer_manager_service.mycompany.com:443</pre>
Si no usa un equilibrador de carga	<p>Escriba el nombre de dominio completo y el puerto de Manager Service. Por ejemplo:</p> <pre>manager_service.mycompany.com:443</pre>

- 6 Reemplace todas las instancias de la cadena `#errorlevel#` por el carácter 1.
- 7 Reemplace todas las instancias de la cadena `#Protocol#` por la cadena `/ssl`.
- 8 Guarde y cierre el archivo.

Pasos siguientes

[Configurar el archivo de propiedades de agente invitado.](#)

Configurar el archivo de propiedades de agente invitado

Debe configurar manualmente los archivos de propiedades del agente invitado.

Requisitos previos

[Configurar el archivo doagentc.bat.](#)

Procedimiento

- 1 Vaya al directorio `VRMGuestAgent` dentro de la imagen de WinPE.
Por ejemplo: `C:\Archivos de programa (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`.
- 2 Haga una copia del archivo `gugent.properties` y póngale el nombre `gugent.properties.template`.
- 3 Haga una copia del archivo `gugent.properties.template` y póngale el nombre `gugentc.properties`.
- 4 Abra `gugent.properties` en un editor de texto.
- 5 Reemplace todas las instancias de la cadena `GuestAgent.log` por la cadena `X:/VRMGuestAgent/GuestAgent.log`.
- 6 Guarde y cierre el archivo.
- 7 Abra `gugentc.properties` en un editor de texto.

- 8 Reemplace todas las instancias de la cadena `GuestAgent.log` por la cadena `C:/VRMGuestAgent/GuestAgent.log`.
- 9 Guarde y cierre el archivo.

Preparar el aprovisionamiento de imágenes de máquina virtual

Antes de aprovisionar instancias con OpenStack, debe tener tipos e imágenes de máquina virtual en el proveedor de OpenStack.

Imágenes de máquina virtual

Durante la creación de blueprints para recursos de OpenStack, puede seleccionar una de las imágenes de máquina virtual disponibles en una lista.

Una imagen de máquina virtual es una plantilla que contiene una configuración de software, incluido un sistema operativo. Las imágenes de máquina virtual se administran mediante el proveedor de OpenStack y se importan durante la recopilación de datos.

Si una imagen de las que sea usa en un blueprint se elimina posteriormente del proveedor de OpenStack, también se quita del blueprint. Si todas las imágenes se quitaron de un blueprint, este se desactiva y no se puede utilizar en solicitudes de máquina hasta que se edite para agregar al menos una imagen.

Tipos de OpenStack

Al crear blueprints de OpenStack, puede seleccionar uno o varios tipos.

Los tipos de OpenStack son plantillas de hardware virtual donde se definen las especificaciones de recurso de máquina de las instancias aprovisionadas en OpenStack. El administrador de OpenStack es quien administra estos tipos, que se importan durante la recopilación de datos.

vRealize Automation admite diversos tipos de OpenStack. Para conocer la información más actualizada sobre la compatibilidad con los tipos de OpenStack, consulte la *Matriz de soporte de vRealize Automation* en <https://www.vmware.com/support/pubs/vcac-pubs.html>.

Preparar el aprovisionamiento de imágenes de máquina de Amazon

Prepare sus imágenes de máquina de Amazon y tipos de instancia para el aprovisionamiento en vRealize Automation.

Explicación de las imágenes de máquina de Amazon

Puede seleccionar una imagen de máquina de Amazon en una lista de imágenes disponibles cuando cree blueprints de máquina de Amazon.

Una imagen de máquina de Amazon es una plantilla que contiene una configuración de software, incluido un sistema operativo. Se administran mediante cuentas de Amazon Web Services. vRealize Automation administra los tipos de instancia disponibles para el aprovisionamiento.

La imagen de máquina de Amazon y el tipo de instancia deben estar disponibles en una región de Amazon. No todos los tipos de instancia están disponibles en todas las regiones.

Puede seleccionar una imagen de máquina de Amazon proporcionada por Amazon Web Services, una comunidad de usuarios o el sitio AWS Marketplace. También puede crear, y compartir si lo desea, sus propias imágenes de máquina de Amazon. Una sola imagen de máquina de Amazon se puede usar para ejecutar una o varias instancias.

Las siguientes consideraciones se aplican a las imágenes de máquina de Amazon de las cuentas de Amazon Web Services desde las que se aprovisionarán las máquinas en la nube:

- Cada blueprint debe especificar una imagen de máquina de Amazon.
Una imagen de máquina de Amazon privada está disponible para una cuenta específica y todas sus regiones. Una imagen de máquina de Amazon pública está disponible para todas las cuentas, pero solo para una región concreta en cada cuenta.
- Cuando se crea un blueprint, la imagen de máquina de Amazon especificada se selecciona entre las regiones para las que se han recopilado datos. Si hay varias cuentas de Amazon Web Services disponibles, el administrador del grupo empresarial debe tener los derechos de todas las imágenes de máquina de Amazon privadas. La región de la imagen de máquina de Amazon y la ubicación del usuario especificado limitan la solicitud de aprovisionamiento a las reservas que coinciden con la región y la ubicación correspondientes.
- Use las reservas y las políticas para distribuir las imágenes de máquina de Amazon entre las cuentas de Amazon Web Services. Use las políticas para restringir el aprovisionamiento de un blueprint a un conjunto concreto de reservas.
- vRealize Automation no puede crear cuentas de usuario en una máquina en la nube. La primera vez que el propietario de una máquina se conecta a una máquina en la nube, debe iniciar sesión como administrador y añadir sus credenciales de usuario de vRealize Automation, o un administrador debe hacerlo por él. Entonces podrá iniciar sesión con sus credenciales de usuario de vRealize Automation.

Si la imagen de máquina de Amazon genera la contraseña del administrador en cada arranque, la página Editar registro de máquina mostrará la contraseña. Si no es así, podrá encontrar la contraseña en la cuenta de Amazon Web Services. Puede configurar todas las imágenes de máquina de Amazon para que generen la contraseña del administrador en cada arranque. También puede proporcionar la información de contraseña del administrador a los usuarios de soporte que aprovisionan máquinas para otros usuarios.

- Para permitir las solicitudes remotas de Instrumental de administración de Windows (WMI) en máquinas en la nube aprovisionadas en cuentas de Amazon Web Services, habilite un agente de Administración remota de Windows (WinRM) para que recopile datos de las máquinas con Windows administradas por vRealize Automation. Consulte *Instalación de vRealize Automation*.
- Una imagen de máquina de Amazon privada se puede ver en todos los tenants.

Para obtener información relacionada, consulte los temas sobre las *Amazon Machine Images (AMI)* en la documentación de Amazon.

Explicación de los tipos de instancia de Amazon

Un arquitecto de IaaS selecciona uno o varios tipos de instancia de Amazon durante la creación de blueprints de Amazon EC2. Un administrador de IaaS puede añadir o quitar tipos de instancia para controlar las opciones disponibles para los arquitectos.

Una instancia de Amazon EC2 es un servidor virtual que puede ejecutar aplicaciones en Amazon Web Services. Las instancias se crean a partir de una imagen de máquina de Amazon, y mediante la selección de un tipo de instancia apropiado.

Para aprovisionar una máquina en una cuenta de Amazon Web Services, se aplica un tipo de instancia a la imagen de máquina de Amazon concreta. Los tipos de instancia disponibles se enumeran cuando los arquitectos crean el blueprint de Amazon EC2. Los arquitectos seleccionan uno o varios tipos de instancia, y dichos tipos de instancia se convierten en las opciones disponibles para los usuarios cuando solicitan el aprovisionamiento de una máquina. Los tipos de instancia deben ser compatibles con la región designada.

Para obtener información relacionada, consulte los temas *Selecting Instance Types* y *Amazon EC2 Instance Details* en la documentación de Amazon.

Añadir un tipo de instancia de Amazon

Hay varios tipos de instancia que se suministran con vRealize Automation y que pueden usarse con blueprints de Amazon. Un administrador puede añadir y quitar tipos de instancia.

Los tipos de instancia de máquina que administran los administradores de IaaS pueden ser utilizados por los arquitectos de blueprints para crear o editar un blueprint de Amazon. Los tipos de instancia y las imágenes de máquina de Amazon se encuentran disponibles a través del producto Amazon Web Services.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de IaaS**.

Procedimiento

- 1 Haga clic en **Infraestructura > Administración > Tipos de instancia**.
- 2 Haga clic en **Nuevo**.
- 3 Añada un nuevo tipo de instancia y especifique los siguientes parámetros.

La información relativa a los tipos de instancia de Amazon disponibles y a los valores de configuración que pueden especificarse para estos parámetros se encuentra disponible en la documentación de Amazon Web Services: *EC2 Instance Types - Amazon Web Services (AWS)* en aws.amazon.com/ec2 e *Instance Types* en docs.aws.amazon.com.

- Name
- Nombre de API
- Nombre de tipo
- Nombre de rendimiento de E/S

- CPU
- Memoria (GB)
- Almacenamiento (GB)
- Unidades informáticas

4 Haga clic en el icono **Guardar** (✔).

Resultados

Cuando los arquitectos de IaaS creen blueprints de Amazon Web Services, podrán usar los tipos de instancia que usted haya personalizado.

Pasos siguientes

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [Crear un grupo de tejidos](#).

Escenario: Preparar recursos de vSphere para el aprovisionamiento de máquinas en Rainpole

Como administrador de vSphere encargado de crear las plantillas de vRealize Automation, necesitará utilizar vSphere Web Client para preparar la clonación de las máquinas CentOS en vRealize Automation.



Necesitará convertir una máquina de referencia CentOS existente en una plantilla de vSphere para que usted y los arquitectos de Rainpole puedan crear blueprints para la clonación de máquinas CentOS en vRealize Automation. Para evitar conflictos que puedan originarse a causa de la implementación de varias máquinas virtuales con una configuración idéntica, también deberá crear una especificación de personalización general que usted y los arquitectos puedan utilizar para crear blueprints de clon para plantillas de Linux.

Procedimiento

1 [Escenario: Convertir la máquina de referencia de CentOS en una plantilla para Rainpole](#)

Mediante el vSphere Client, se convierte la máquina de referencia de CentOS existente en una plantilla de vSphere a la que los arquitectos de IaaS de vRealize Automation hacen referencia como base para sus blueprints clonados.

2 Escenario: Crear una especificación de personalización para la clonación de máquinas de Linux en Rainpole

Con vSphere Client puede crear una especificación de personalización estándar que los arquitectos de IaaS de vRealize Automation pueden usar cuando crean blueprints clonados para máquinas de Linux.

Escenario: Convertir la máquina de referencia de CentOS en una plantilla para Rainpole

Mediante el vSphere Client, se convierte la máquina de referencia de CentOS existente en una plantilla de vSphere a la que los arquitectos de IaaS de vRealize Automation hacen referencia como base para sus blueprints clonados.

Procedimiento

- 1 Inicie sesión en su máquina de referencia como el usuario raíz y prepare la máquina para la conversión.

- a Quite las reglas de persistencia de udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b Permita que las máquinas clonadas desde esta plantilla tengan sus propios identificadores únicos.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c Apague la máquina.

```
shutdown -h now
```

- 2 Inicie sesión en vSphere Web Client como administrador.
- 3 Haga clic en la pestaña **Opciones de VM**.
- 4 Haga clic con el botón derecho en la máquina de referencia y seleccione **Editar configuración**.
- 5 Escriba **Rainpole_centos_63_x86** en el cuadro de texto **Nombre de máquina virtual**.
- 6 Aunque su máquina de referencia tenga un sistema operativo invitado CentOS, seleccione **Red Hat Enterprise Linux 6 (64 bits)** en el menú desplegable **Versión de sistema operativo invitado**.

Si selecciona CentOS, es posible que su plantilla y su especificación de personalización no funcionen del modo esperado.

- 7 Haga clic con el botón derecho en la máquina de referencia **Rainpole_centos_63_x86** en vSphere Web Client y seleccione **Plantilla > Convertir en plantilla**.

Resultados

vCenter Server marca la máquina de referencia Rainpole_centos_63_x86 como plantilla y muestra la tarea en el panel Tareas recientes.

Pasos siguientes

Para evitar conflictos que puedan originarse a causa de la implementación de varias máquinas virtuales con una configuración idéntica, puede crear una especificación de personalización general que usted y los arquitectos de Rainpole puedan utilizar para crear blueprints de clon para plantillas de Linux.

Escenario: Crear una especificación de personalización para la clonación de máquinas de Linux en Rainpole

Con vSphere Client puede crear una especificación de personalización estándar que los arquitectos de IaaS de vRealize Automation pueden usar cuando crean blueprints clonados para máquinas de Linux.

Procedimiento

- 1 En la página principal, haga clic en **Administrador de especificación de personalización** para abrir el asistente.
- 2 Haga clic en el icono **Nuevo**.
- 3 Especifique las propiedades.
 - a Seleccione **Linux** en el menú desplegable **Sistema operativo de la máquina virtual de destino**.
 - b Escriba **Linux** en el cuadro de texto **Nombre de especificación de personalización**.
 - c Escriba **Rainpole Linux cloning with vRealize Automation** en el cuadro de texto **Descripción**.
 - d Haga clic en **Siguiente**.
- 4 Establezca un nombre de equipo.
 - a Seleccione **Usar el nombre de la máquina virtual**.
 - b Escriba en el cuadro de texto **Nombre de dominio** el dominio en el que las máquinas clonadas se aprovisionarán.
 Por ejemplo, **rainpole.local**.
 - c Haga clic en **Siguiente**.
- 5 Configure la zona horaria.
- 6 Haga clic en **Siguiente**.
- 7 Seleccione la opción para **usar configuración de red estándar en el sistema operativo invitado y habilitar DHCP en todas las interfaces de red**.

8 Siga las indicaciones para añadir el resto de información necesaria.

9 En la página **Listo para completar**, revise lo que seleccionó y haga clic en **Finalizar**.

Resultados

Posee una especificación de personalización general que puede usar para crear blueprints para clonar máquinas de Linux.

Pasos siguientes

Inicie sesión en la consola de vRealize Automation como el administrador de la configuración que creó durante la instalación y solicite los elementos del catálogo que configuran rápidamente su prueba de concepto.

Preparar el aprovisionamiento de Software

Use Software para implementar aplicaciones y middleware como parte del proceso de aprovisionamiento de vRealize Automation para máquinas vSphere, vCloud Director, vCloud Air y Amazon AWS.

Puede implementar Software en máquinas si su blueprint es compatible con Software y si instala el agente invitado y el agente de arranque de software en sus máquinas de referencia antes de convertirlas en plantillas o imágenes de máquina de Amazon.

Para obtener información relacionada con la especificación de puertos al preparar el aprovisionamiento, consulte *Guía de configuración segura* y *Arquitectura de referencia* en la [información sobre VMware vRealize Automation](#).

Tabla 1-17. Métodos de aprovisionamiento compatibles con Software

Tipo de máquina	Método de aprovisionamiento	Preparación necesaria
vSphere	Clonar	Un blueprint de clon aprovisiona una máquina virtual completa e independiente basada en una plantilla de máquina virtual de vCenter Server. Si desea que sus plantillas de clonación sean compatibles con componentes de Software, instale el agente invitado y el agente de arranque del software en su máquina de referencia cuando prepare una plantilla para la clonación. Consulte Lista de comprobación para preparar el aprovisionamiento mediante clonación .
vSphere	Clon vinculado	Un blueprint de clon vinculado aprovisiona una copia con eficacia de espacio de una máquina de vSphere basada en un snapshot, usando una cadena de discos delta para realizar un seguimiento de las diferencias respecto a la máquina principal. Si desea que sus blueprints de clon vinculado sean compatibles con componentes de Software, instale el agente invitado y el agente de arranque de software en la máquina antes de tomar la instantánea. Si su máquina de snapshot se ha clonado a partir de una plantilla compatible con Software, los agentes necesarios ya están instalados.

Tabla 1-17. Métodos de aprovisionamiento compatibles con Software (continuación)

Tipo de máquina	Método de aprovisionamiento	Preparación necesaria
vCloud Director	Clonar	Un blueprint de clon aprovisiona una máquina virtual completa e independiente basada en una plantilla de máquina virtual de vCenter Server. Si desea que sus plantillas de clonación sean compatibles con componentes de Software, instale el agente invitado y el agente de arranque del software en su máquina de referencia cuando prepare una plantilla para la clonación. Consulte Lista de comprobación para preparar el aprovisionamiento mediante clonación .
vCloud Air	Clonar	Un blueprint de clon aprovisiona una máquina virtual completa e independiente basada en una plantilla de máquina virtual de vCenter Server. Si desea que sus plantillas de clonación sean compatibles con componentes de Software, instale el agente invitado y el agente de arranque del software en su máquina de referencia cuando prepare una plantilla para la clonación. Consulte Lista de comprobación para preparar el aprovisionamiento mediante clonación .
Amazon AWS	Imagen de máquina de Amazon	<p>Una imagen de máquina de Amazon es una plantilla que contiene una configuración de software, incluido un sistema operativo. Si desea crear una máquina de Amazon compatible con Software, conecte una instancia de Amazon AWS en ejecución que utilice un volumen de EBS para el dispositivo raíz. Instale el agente invitado y el agente de arranque de software en la máquina de referencia y después cree una máquina de Amazon a partir de su instancia. Para obtener instrucciones sobre cómo crear AMI respaldadas por EBS de Amazon, consulte la documentación de Amazon AWS.</p> <p>Para que el agente invitado y el agente de arranque de Software funcionen en máquinas aprovisionadas, debe configurar la conectividad de red a VPC.</p>

Preparar el aprovisionamiento de máquinas con Software

Para admitir componentes de Software, debe instalar el agente invitado y el agente de arranque de Software en su máquina de referencia para poder convertirla en una plantilla para la clonación, crear una imagen de máquina de Amazon o tomar un snapshot.

Preparar una máquina Windows de referencia para que sea compatible con el Software

Se emplea un solo script para instalar la instancia de Java Runtime Environment, el agente invitado y el agente de arranque de Software en un equipo de referencia de Windows. Desde el equipo de referencia, puede crear una plantilla para la clonación, un snapshot o una imagen de máquina de Amazon que admita los componentes de Software.

Software admite la creación de scripts con el símbolo del sistema de Windows y PowerShell 2.0.

Importante No se debe interrumpir el proceso de inicio. Configure la máquina virtual de manera que nada detenga el proceso de inicio de la máquina virtual antes de que se muestre el mensaje de inicio de sesión. Por ejemplo, asegúrese de que ningún proceso o script solicite la interacción del usuario mientras se inicia la máquina virtual.

Requisitos previos

- Identifique o cree una máquina de referencia de Windows.
- Establezca una confianza segura entre la máquina de referencia y el host de IaaS Manager Service. Consulte [Configurar el agente invitado para confiar en un servidor](#).
- Si tiene pensado acceder de forma remota a la máquina para solucionar problemas o por otro motivo, instale Servicios de Escritorio remoto (Remote Desktop Services, RDS).
- Quite los artefactos de configuración de red de los archivos de configuración de la red.

Procedimiento

- 1 Inicie sesión en el servidor de referencia de Windows como administrador.
- 2 En un navegador, abra la página de descarga de software en el dispositivo de vRealize Automation.

`https://vrealize-automation-appliance-FQDN/software`
- 3 Guarde el archivo ZIP de la plantilla en la instancia de Windows Server.

`prepare_vra_template_windows.zip`
- 4 Extraiga el contenido del archivo ZIP en una carpeta y ejecute el archivo por lotes.

`.\prepare_vra_template.bat`
- 5 Siga las indicaciones.
- 6 Cuando termine, apague la máquina virtual de Windows.

Resultados

El script quita agentes invitados o agentes de arranque de Software anteriores, e instala las versiones compatibles de Java Runtime Environment, el agente invitado y el agente de arranque de Software.

Pasos siguientes

Convierta la máquina de referencia en una plantilla para la clonación, un snapshot o una imagen de máquina de Amazon. Cada uno de estos elementos admite componentes de Software y los arquitectos de infraestructuras pueden usarlos al crear blueprints.

Preparar una máquina Linux de referencia para que sea compatible con Software

Se emplea un solo script para instalar la instancia de Java Runtime Environment, el agente invitado y el agente de arranque de Software en un equipo de referencia de Linux. Desde el equipo de referencia, puede crear una plantilla para la clonación, un snapshot o una imagen de máquina de Amazon que admita los componentes de Software.

Software admite scripts de Bash.

Importante No se debe interrumpir el proceso de arranque. Configure la máquina virtual de manera que nada detenga el proceso de arranque de la máquina virtual antes de que se muestre el mensaje de inicio de sesión. Por ejemplo, asegúrese de que ningún proceso o script solicite la interacción del usuario mientras se inicia la máquina virtual.

Requisitos previos

- Identifique o cree una máquina de referencia de Linux.
- En función del sistema Linux, compruebe que los siguientes comandos están disponibles:
 - yum o apt-get
 - wget o curl
 - python
 - dmidecode, si lo solicitan los proveedores de nube
 - Requisitos comunes (como sed, awk, perl, chkconfig, unzip, y grep) en función de su distribución de Linux

También puede utilizar un editor para inspeccionar el script descargado `prepare_vra_template.sh`, que expone los comandos que utiliza.

- Si tiene pensado acceder de forma remota a la máquina para solucionar problemas o por otro motivo, instale OpenSSH.
- Quite los artefactos de configuración de red de los archivos de configuración de la red.

Procedimiento

- 1 Inicie sesión en la máquina de referencia como raíz.
- 2 Descargue el paquete tar.gz de plantilla del dispositivo de vRealize Automation.

```
wget https://vrealize-automation-appliance-FQDN/software/download/prepare_vra_template.tar.gz
```

Si el entorno usa certificados autofirmados, puede que necesite la opción `--no-check-certificate`.

```
wget --no-check-certificate https://vrealize-automation-appliance-FQDN/software/download/prepare_vra_template.tar.gz
```

- 3 Descomprima el paquete.

```
tar -xvf prepare_vra_template.tar.gz
```

- 4 En el resultado de la descompresión, busque el script del instalador y conviértalo en un ejecutable.

```
chmod +x prepare_vra_template.sh
```


5 Ejecute el script del instalador.

```
./prepare_vra_template.sh
```

Si necesita información sobre opciones no interactivas y valores esperados, consulte la ayuda del script.

```
./prepare_vra_template.sh --help
```

6 Siga las indicaciones.

Si la instalación se realiza correctamente, aparecerá una confirmación. Si se muestran errores y logs, solucione los errores y vuelva a ejecutar el script.

7 Cuando termine, apague la máquina virtual de Linux.**Resultados**

El script quita agentes invitados o agentes de arranque de Software anteriores, e instala las versiones compatibles de Java Runtime Environment, el agente invitado y el agente de arranque de Software.

Pasos siguientes

En el hipervisor o el proveedor de nube, convierta la máquina de referencia en una plantilla para la clonación, un snapshot o una imagen de máquina de Amazon. Cada uno de estos elementos admite componentes de Software y los arquitectos de infraestructuras pueden usarlos al crear blueprints.

Actualizar plantillas de máquina virtual existentes en vRealize Automation

Si está actualizando sus plantillas, imágenes de máquinas de Amazon o snapshots para la versión más reciente del agente de arranque de Software de Windows o si está actualizando manualmente al agente de arranque de Software de Linux más reciente en lugar de utilizar el script `prepare_vra_template.sh`, debe retirar las versiones existentes y eliminar los logs.

Linux

Para las máquinas de referencia de Linux, al ejecutar el script `prepare_vra_template.sh` script se restablece el agente y se eliminan los logs por usted antes de volver a instalar. No obstante, si tiene planeado instalar manualmente, debe iniciar sesión en la máquina de referencia como usuario raíz y ejecutar el comando para restablecer y eliminar los artefactos.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

Windows

Para máquinas de referencia de Windows, debe quitar el agente de arranque de Software existente y el agente invitado de vRealize Automation 6.0 o posterior y eliminar los archivos log en tiempo de ejecución existentes. En una ventana de comandos de PowerShell, ejecute los comandos para quitar el agente y los artefactos.

```
c:\opt\vmware-appdirector\agent-bootstrap\appd_bootstrap_removal.bat
```

Escenario: Preparar una plantilla de CentOS de vSphere para los blueprints de componente de software y de máquina clonada

Como administrador de vCenter Server, desea preparar una plantilla de vSphere que los arquitectos de vRealize Automation puedan usar para clonar máquinas CentOS de Linux. Como desea asegurarse de que la plantilla admita blueprints con componentes de software, instala el agente invitado y el agente de arranque de software antes de convertir la máquina de referencia en una plantilla.

Requisitos previos

- Identifique o cree una máquina de referencia CentOS de Linux que tenga VMware Tools instalado. Incluya, al menos, un adaptador de red para proporcionar conexión a Internet en caso de que los arquitectos de blueprints no añadan esta funcionalidad en el nivel de blueprint. Para obtener información sobre cómo crear máquinas virtuales, consulte la documentación de vSphere.
- Debe estar conectado a un vCenter Server para convertir una máquina virtual en una plantilla. No puede crear plantillas si conecta vSphere directamente a un host de vSphere ESXi.

Procedimiento

1 [Escenario: Preparar la máquina de referencia para personalizaciones de agente invitado y componentes de software](#)

Para que su plantilla admita componentes de software, instale el agente de arranque de software y su requisito previo, el agente invitado, en la máquina de referencia. Los agentes se aseguran de que los arquitectos de vRealize Automation que usen su plantilla puedan incluir componentes de software en sus blueprints.

2 [Escenario: Convertir la máquina de referencia de CentOS en una plantilla](#)

Después de instalar el agente invitado y el agente de arranque del software en su máquina de referencia, convierte la máquina de referencia en una plantilla que los arquitectos de vRealize Automation pueden utilizar para crear blueprints de máquinas clonadas.

3 [Escenario: Crear una especificación de personalización para la clonación de vSphere](#)

Cree una especificación de personalización que los arquitectos de blueprints puedan usar con la plantilla cpb_centos_63_x84.

Resultados

Ha creado una plantilla y una especificación de personalización desde su máquina de referencia que los arquitectos de blueprints pueden usar para crear blueprints de vRealize Automation que clonen máquinas CentOS de Linux. Como ha instalado el agente de arranque de Software y el agente invitado en la máquina de referencia, los arquitectos pueden usar la plantilla para crear blueprints de elementos del catálogo elaborados que incluyan componentes de Software u otras personalizaciones de agente invitado como, por ejemplo, ejecutar scripts o formatear discos. Como ha instalado VMware Tools, los arquitectos y los administradores del catálogo pueden permitir que los usuarios realicen acciones en las máquinas, como Reconfigurar, Snapshot y Reiniciar.

Pasos siguientes

Después de configurar los usuarios, grupos y recursos de vRealize Automation, puede usar la plantilla y la especificación de personalización para crear un blueprint de máquina para la clonación. Consulte *Instalación y configuración de vRealize Automation para el escenario de Rainpole*.

Escenario: Preparar la máquina de referencia para personalizaciones de agente invitado y componentes de software

Para que su plantilla admita componentes de software, instale el agente de arranque de software y su requisito previo, el agente invitado, en la máquina de referencia. Los agentes se aseguran de que los arquitectos de vRealize Automation que usen su plantilla puedan incluir componentes de software en sus blueprints.

Para simplificar el proceso, debe descargar y ejecutar un script de vRealize Automation que instala ambos agentes, en lugar de descargar e instalar paquetes independientes.

El script también se conecta a la instancia de Manager Service y descarga el certificado SSL, que establece la confianza entre Manager Service y las máquinas implementadas desde la plantilla. Tenga en cuenta que la opción de que el script descargue el certificado ofrece menos seguridad que obtener manualmente el certificado SSL de Manager Service e instalarlo en la máquina de referencia en `/usr/share/gugent/cert.pem`.

Procedimiento

- 1 En el navegador web, abra la siguiente dirección URL.

`https://vrealize-automation-appliance-FQDN/software/index.html`

- 2 Guarde el script `prepare_vra_template.sh` en la máquina de referencia.
- 3 En la máquina de referencia, convierta `prepare_vra_template.sh` en ejecutable.

```
chmod +x prepare_vra_template.sh
```

- 4 Ejecute `prepare_vra_template.sh`.

```
./prepare_vra_template.sh
```

5 Siga las indicaciones.

Si necesita información no interactiva sobre opciones y valores, escriba `./prepare_vra_template.sh --help`.

Resultados

Cuando la instalación finalice, se mostrará un mensaje de confirmación. Si aparecen logs y mensajes de error, corrija los problemas y vuelva a ejecutar el script.

Escenario: Convertir la máquina de referencia de CentOS en una plantilla

Después de instalar el agente invitado y el agente de arranque del software en su máquina de referencia, convierte la máquina de referencia en una plantilla que los arquitectos de vRealize Automation pueden utilizar para crear blueprints de máquinas clonadas.

Después de convertir la máquina de referencia en una plantilla, no puede editar ni activar la plantilla a menos que la vuelva a convertir en una máquina virtual.

Procedimiento

- 1 Inicie sesión en su máquina de referencia como el usuario raíz y prepare la máquina para la conversión.

- a Quite las reglas de persistencia de udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b Permita que las máquinas clonadas desde esta plantilla tengan sus propios identificadores únicos.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c Si reinició o volvió a configurar la máquina de referencia después de instalar el agente de arranque del software, restablezca el agente.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- d Apague la máquina.

```
shutdown -h now
```

- 2 Inicie sesión en vSphere Web Client como administrador.
- 3 Haga clic con el botón derecho en la máquina de referencia y seleccione **Editar configuración**.
- 4 Escriba **cpb_centos_63_x84** en el cuadro de texto **Nombre de máquina virtual**.

- 5 Aunque su máquina de referencia tenga un sistema operativo invitado CentOS, seleccione **Red Hat Enterprise Linux 6 (64 bits)** en el menú desplegable **Versión de sistema operativo invitado**.

Si selecciona CentOS, es posible que su plantilla y su especificación de personalización no funcionen del modo esperado.

- 6 Haga clic con el botón derecho en la máquina de referencia en vSphere Web Client y seleccione **Plantilla > Convertir en plantilla**.

Resultados

vCenter Server marca la máquina de referencia cpb_centos_63_x84 como plantilla y muestra la tarea en el panel Tareas recientes. Si ya ha puesto su entorno de vSphere bajo la administración de vRealize Automation, la plantilla se detecta durante la siguiente recopilación de datos automatizada. Si todavía no ha configurado vRealize Automation, la plantilla se recopila durante ese proceso.

Escenario: Crear una especificación de personalización para la clonación de vSphere

Cree una especificación de personalización que los arquitectos de blueprints puedan usar con la plantilla cpb_centos_63_x84.

Procedimiento

- 1 Inicie sesión en vSphere Web Client como administrador.
- 2 En la página principal, haga clic en **Administrador de especificación de personalización** para abrir el asistente.
- 3 Haga clic en el icono **Nuevo**.
- 4 Haga clic en el icono **Nuevo**.
- 5 Especifique las propiedades.
 - a Seleccione **Linux** en el menú desplegable **Sistema operativo de la máquina virtual de destino**.
 - b Escriba **Customspecs** en el cuadro de texto **Nombre de especificación de personalización**.
 - c Escriba **cpb_centos_63_x84 cloning with vRealize Automation** en el cuadro de texto **Descripción**.
 - d Haga clic en **Siguiente**.

- 6 Establezca un nombre de equipo.
 - a Seleccione **Usar el nombre de la máquina virtual**.
 - b Escriba en el cuadro de texto **Nombre de dominio** el dominio en el que las máquinas clonadas se aprovisionarán.
 - c Haga clic en **Siguiente**.
- 7 Configure la zona horaria.
- 8 Haga clic en **Siguiente**.
- 9 Seleccione la opción para **usar configuración de red estándar en el sistema operativo invitado y habilitar DHCP en todas las interfaces de red**.

Los administradores de tejido y los arquitectos de infraestructura controlan la configuración de red de la máquina aprovisionada mediante la creación y el uso de perfiles de red en vRealize Automation.
- 10 Siga las indicaciones para añadir el resto de información necesaria.
- 11 En la página **Listo para completar**, revise lo que seleccionó y haga clic en **Finalizar**.

Resultados

Escenario: Preparar la importación del blueprint de la aplicación de muestra Dukes Bank de vSphere

Como administrador de vCenter Server, desea preparar una especificación de personalización y una plantilla de CentOS Linux 6.x de vSphere que pueda utilizar para aprovisionar la aplicación de muestra Dukes Bank de vRealize Automation.

Desea asegurarse de que la plantilla sea compatible con los componentes de software de la aplicación de muestra, de modo que instale el agente invitado y el agente de arranque del software en la máquina de referencia de Linux antes de convertirla en una plantilla y crear una especificación de personalización. Desactive SELinux en la máquina de referencia para asegurarse de que la plantilla es compatible con la implementación específica de MySQL que utiliza la aplicación de muestra Dukes Bank.

Requisitos previos

- Identifique o cree una máquina de referencia de CentOS Linux 6.x que tenga VMware Tools instalado. Para obtener información sobre cómo crear máquinas virtuales, consulte la documentación de vSphere.

- Debe estar conectado a un vCenter Server para convertir una máquina virtual en una plantilla. No puede crear plantillas si conecta vSphere directamente a un host de vSphere ESXi.

Procedimiento

1 Escenario: Preparar la máquina de referencia para la aplicación de muestra Dukes Bank de vSphere

Como desea que su plantilla sea compatible con la aplicación de muestra Dukes Bank, debe instalar tanto el agente invitado como el agente de arranque del software en la máquina de referencia para que vRealize Automation pueda aprovisionar los componentes de software. Para simplificar el proceso, descargue y ejecute un script de vRealize Automation que instale tanto el agente invitado como el agente de arranque del software en lugar de descargar e instalar los paquetes por separado.

2 Escenario: Convertir la máquina de referencia en una plantilla para la aplicación Dukes Bank de vSphere

Tras la instalación del agente invitado y agente de arranque de software en la máquina de referencia, desactiva SELinux para asegurarse de que la plantilla es compatible con la implementación específica de MySQL que se utiliza en la aplicación de muestra Dukes Bank. Convierte la máquina de referencia en una plantilla que puede emplear para aprovisionar la aplicación de muestra Dukes Bank de vSphere.

3 Escenario: Crear una especificación de personalización para clonar máquinas de la aplicación de muestra Dukes Bank de vSphere

Crea una especificación de personalización para utilizarla con su plantilla de máquina de Dukes Bank.

Resultados

Creó una plantilla y una especificación de personalización desde la máquina de referencia que admite la aplicación de muestra Dukes Bank de vRealize Automation.

Escenario: Preparar la máquina de referencia para la aplicación de muestra Dukes Bank de vSphere

Como desea que su plantilla sea compatible con la aplicación de muestra Dukes Bank, debe instalar tanto el agente invitado como el agente de arranque del software en la máquina de referencia para que vRealize Automation pueda aprovisionar los componentes de software. Para simplificar el proceso, descargue y ejecute un script de vRealize Automation que instale tanto el agente invitado como el agente de arranque del software en lugar de descargar e instalar los paquetes por separado.

Procedimiento

- 1 Inicie sesión en su máquina de referencia como el usuario raíz.
- 2 Descargue el script de instalación del dispositivo de vRealize Automation.

```
wget https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

Si en su entorno se usan certificados autofirmados, es posible que deba usar la opción `--no-check-certificate` de `wget`. Por ejemplo:

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

- 3 Convierta el script `prepare_vra_template.sh` en ejecutable.

```
chmod +x prepare_vra_template.sh
```

- 4 Ejecute el script del instalador `prepare_vra_template.sh`.

```
./prepare_vra_template.sh
```

Puede ejecutar el comando de ayuda `./prepare_vra_template.sh --help` para obtener información acerca de opciones no interactivas y valores esperados.

- 5 Siga las indicaciones para completar la instalación.

Verá un mensaje de confirmación cuando la instalación se haya completado correctamente. Si ve un mensaje de error y logs en la consola, solucione los errores y ejecute de nuevo el script del instalador.

Resultados

Instaló tanto el agente de arranque del software como su requisito previo, el agente invitado, para asegurarse de que la aplicación de muestra Dukes Bank aprovisiona correctamente los componentes de software. El script también se conectó a la instancia de Manager Service y descargó el certificado SSL para establecer la confianza entre Manager Service y las máquinas implementadas desde la plantilla. Este enfoque es menos seguro que obtener el certificado SSL de Manager Service e instalarlo manualmente en la máquina de referencia en `/usr/share/gugent/cert.pem`, y puede reemplazar manualmente este certificado si la seguridad es una prioridad alta.

Escenario: Convertir la máquina de referencia en una plantilla para la aplicación Dukes Bank de vSphere

Tras la instalación del agente invitado y agente de arranque de software en la máquina de referencia, desactiva SELinux para asegurarse de que la plantilla es compatible con la implementación específica de MySQL que se utiliza en la aplicación de muestra Dukes Bank. Convierte la máquina de referencia en una plantilla que puede emplear para aprovisionar la aplicación de muestra Dukes Bank de vSphere.

Después de convertir la máquina de referencia en una plantilla, no puede editar ni activar la plantilla a menos que la vuelva a convertir en una máquina virtual.

Procedimiento

- 1 Inicie sesión en su máquina de referencia como el usuario raíz.

- a Edite el archivo `/etc/selinux/config` para desactivar SELinux.

```
SELINUX=disabled
```

Si no desactiva SELinux, puede que el componente de software MySQL de la aplicación de muestra Dukes Bank no funcione como se espera.

- b Quite las reglas de persistencia de udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- c Permita que las máquinas clonadas desde esta plantilla tengan sus propios identificadores únicos.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- d Si reinició o volvió a configurar la máquina de referencia después de instalar el agente de arranque del software, restablezca el agente.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- e Apague la máquina.

```
shutdown -h now
```

- 2 Inicie sesión en vSphere Web Client como administrador.
- 3 Haga clic con el botón derecho en la máquina de referencia y seleccione **Editar configuración**.
- 4 Escriba **dukes_bank_template** en el cuadro de texto **Nombre de máquina virtual**.
- 5 Si su máquina de referencia tiene un sistema operativo invitado CentOS, seleccione **Red Hat Enterprise Linux 6 (64 bits)** en el menú desplegable **Versión de sistema operativo invitado**.
Si selecciona CentOS, es posible que su plantilla y su especificación de personalización no funcionen del modo esperado.
- 6 Haga clic en **Aceptar**.
- 7 Haga clic con el botón derecho en la máquina de referencia en vSphere Web Client y seleccione **Plantilla > Convertir en plantilla**.

Resultados

vCenter Server marca la máquina de referencia `dukes_bank_template` como plantilla y muestra la tarea en el panel Tareas recientes. Si ya ha puesto su entorno de vSphere bajo la administración de vRealize Automation, la plantilla se detecta durante la siguiente recopilación de datos automatizada. Si todavía no ha configurado vRealize Automation, la plantilla se recopila durante ese proceso.

Escenario: Crear una especificación de personalización para clonar máquinas de la aplicación de muestra Dukes Bank de vSphere

Crea una especificación de personalización para utilizarla con su plantilla de máquina de Dukes Bank.

Procedimiento

- 1 Inicie sesión en vSphere Web Client como administrador.
- 2 En la página principal, haga clic en **Administrador de especificación de personalización** para abrir el asistente.
- 3 Haga clic en el icono **Nuevo**.
- 4 Especifique las propiedades.
 - a Seleccione **Linux** en el menú desplegable **Sistema operativo de la máquina virtual de destino**.
 - b Escriba **Customspecs_sample** en el cuadro de texto **Nombre de especificación de personalización**.
 - c Escriba **Especificación de personalización de Dukes Bank** en el cuadro de texto **Descripción**.
 - d Haga clic en **Siguiente**.
- 5 Establezca un nombre de equipo.
 - a Seleccione **Usar el nombre de la máquina virtual**.
 - b Escriba el dominio en el que desea aprovisionar la aplicación de muestra Dukes Bank en el cuadro de texto **Nombre de dominio**.
 - c Haga clic en **Siguiente**.
- 6 Configure la zona horaria.
- 7 Haga clic en **Siguiente**.
- 8 Seleccione la opción para **usar configuración de red estándar en el sistema operativo invitado y habilitar DHCP en todas las interfaces de red**.

Los administradores de tejido y los arquitectos de infraestructura controlan la configuración de red de la máquina aprovisionada mediante la creación y el uso de perfiles de red en vRealize Automation.

- 9 Siga las indicaciones para añadir el resto de información necesaria.
- 10 En la página **Listo para completar**, revise lo que seleccionó y haga clic en **Finalizar**.

Resultados

Creó una plantilla y una especificación de personalización que puede utilizar para aprovisionar la aplicación de muestra Dukes Bank.

Pasos siguientes

- 1 Cree un perfil de red externa para proporcionar una puerta de enlace y un intervalo de direcciones IP. Consulte [Crear un perfil de red externa mediante un proveedor de IPAM de terceros](#).
- 2 Asigne el perfil de red externa a la reserva de vSphere. Consulte [Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer](#). La aplicación de muestra no puede aprovisionar correctamente sin un perfil de red externa.
- 3 Importe la aplicación de muestra Dukes Bank en el entorno. Consulte [Escenario: importar Dukes Bank para la aplicación de muestra de vSphere y configurar el entorno](#).

Preparación de tenants y recursos para el aprovisionamiento de blueprints

2

Puede configurar varios entornos de tenant, cada uno con sus propios grupos de usuarios y con acceso exclusivo a los recursos administrados mediante vRealize Automation.

Este capítulo incluye los siguientes temas:

- [Configurar las opciones de tenant](#)
- [Configurar recursos](#)
- [Preferencias del usuario para notificaciones y delegados](#)

Configurar las opciones de tenant

Los administradores de tenants configuran los parámetros de estos, tales como autenticación de usuario, y administran los roles de usuario y los grupos empresariales. Los administradores de sistemas y los administradores de tenants configuran opciones como los servidores de correo electrónico que se encargan de las notificaciones y las personalizaciones de marca para la consola de vRealize Automation.

Puede utilizar la Lista de comprobación para la configuración de tenants para ver una descripción general de la secuencia de pasos necesarios para configurar tenants.

Tabla 2-1. Lista de comprobación para la configuración de tenants

Tarea	Función de vRealize Automation	Detalles
❑ Crear cuentas de usuario locales y asignar un administrador de tenants.	Administrador del sistema	Para obtener un ejemplo de cómo crear cuentas de usuario locales, consulte <i>Instalación y configuración de vRealize Automation para el escenario de Rainpole</i> .
❑ Configurar la administración de directorios para establecer los parámetros de control de acceso y administración de identidad de tenants.	Administrador de tenants	Elegir opciones de configuración de Administración de directorios
❑ Crear grupos empresariales y grupos personalizados, y conceder a los usuarios derechos de acceso a la consola de vRealize Automation.	Administrador de tenants	Configurar funciones de usuarios y grupos

Tabla 2-1. Lista de comprobación para la configuración de tenants (continuación)

Tarea	Función de vRealize Automation	Detalles
❑ (Opcional) Crear tenants adicionales para que los usuarios puedan obtener acceso a las aplicaciones y los recursos correspondientes que necesitan para completar las asignaciones de trabajo.	Administrador del sistema	Crear tenants adicionales
❑ (Opcional) Configurar la personalización de marca en las páginas de inicio de sesión y aplicación del tenant de la consola de vRealize Automation.	<ul style="list-style-type: none"> ■ Administrador del sistema ■ Administrador de tenants 	Configurar la personalización de marca
❑ (Opcional) Configurar vRealize Automation para enviar notificaciones a los usuarios cuando se produzcan determinados eventos.	<ul style="list-style-type: none"> ■ Administrador del sistema ■ Administrador de tenants 	Lista de comprobación para la configuración de notificaciones
❑ (Opcional) Configurar vRealize Orchestrator para que admita XaaS y otras extensibilidades.	<ul style="list-style-type: none"> ■ Administrador del sistema ■ Administrador de tenants 	Configurar vRealize Orchestrator
❑ (Opcional) Crear un archivo de protocolo de escritorio remoto personalizado que los arquitectos de IaaS usan en blueprints para configurar las opciones de RDP.	Administrador del sistema	Crear un archivo RDP personalizado para admitir conexiones RDP para máquinas aprovisionadas
❑ (Opcional) Definir las ubicaciones del centro de datos que los administradores de tejido y los arquitectos de IaaS pueden aprovechar para permitir que los usuarios seleccionen una ubicación apropiada para el aprovisionamiento cuando soliciten máquinas.	Administrador del sistema	Para obtener un ejemplo de cómo agregar ubicaciones del centro de datos, consulte Escenario: Añadir ubicaciones de centros de datos para implementaciones en varias regiones .

Elegir opciones de configuración de Administración de directorios

Puede utilizar las funciones de administración de directorios de vRealize Automation para configurar un vínculo de Active Directory de acuerdo con sus requisitos de autenticación de usuarios.

La administración de directorios proporciona numerosas opciones para permitir una autenticación de usuarios totalmente personalizada.

Tabla 2-2. Elegir opciones de configuración de Administración de directorios

Opción de configuración	Procedimiento
Configure un vínculo a Active Directory.	<ol style="list-style-type: none"> 1 Configure un vínculo a Active Directory. Consulte Configurar una instancia de Active Directory mediante un vínculo LDAP/IWA. 2 Si configuró vRealize Automation para una alta disponibilidad, consulte Configurar Administración de directorios para alta disponibilidad.
(Opcional) Mejorar la seguridad de un vínculo de directorio basado en ID de usuario y contraseña configurando la integración bidireccional con los Servicios federados de Active Directory.	Configurar una relación de confianza bidireccional entre vRealize Automation y Active Directory
(Opcional) Añadir usuarios y grupos a un vínculo de Active Directory existente.	Añadir usuarios o grupos a una conexión de Active Directory .
(Opcional) Editar la política predeterminada para aplicar reglas personalizadas para un vínculo de Active Directory.	Administrar la política de acceso de usuarios .
(Opcional) Configurar rangos de redes para restringir las direcciones IP con las que los usuarios podrán iniciar sesión en el sistema, administrar restricciones de inicio de sesión (tiempo de espera, número de intentos de inicio de sesión antes de se bloquee la cuenta).	Añadir o editar un rango de redes .

Descripción de la administración de directorios

Los administradores de tenants pueden configurar la administración de identidades de tenants y la configuración de control de acceso mediante las opciones de la administración de directorios de la consola de aplicaciones de vRealize Automation.

Puede administrar la siguiente configuración desde la pestaña **Administración > Administración de directorios**.

Tabla 2-3. Configuración de la administración de directorios

Configuración	Descripción
Directorios	<p>La página Directorios le permite crear y administrar vínculos de Active Directory para que admitan la autenticación y autorización de usuarios de tenants de vRealize Automation. Se crean uno o varios directorios y después se sincronizan con la implementación de Active Directory. En esta página se muestran el número de grupos y usuarios que se sincronizan con el directorio y la hora de la última sincronización. Puede hacer clic en Sincronizar ahora para iniciar manualmente la sincronización del directorio.</p> <p>Consulte Usar Administración de directorios para crear un vínculo de Active Directory.</p> <p>Cuando se hace clic en un directorio y, a continuación, en el botón Configuración de sincronización, se puede editar la configuración de sincronización, navegar por la página de Proveedores de identidades y ver el log de sincronización.</p> <p>Desde la página de configuración de sincronización de directorios, puede programar la frecuencia de sincronización, consultar la lista de dominios asociados a este directorio, cambiar la lista de atributos asignados, actualizar el usuario y la lista de grupos que se sincroniza y configurar los destinos de protección.</p>
Conectores	<p>En la página Conectores se muestran los conectores implementados de su red empresarial. Un conector sincroniza los datos de grupo y usuario entre Active Directory y el servicio de administración de directorios y, cuando se utiliza como el proveedor de identidades, autentica a los usuarios para su acceso al servicio. De manera predeterminada, cada dispositivo de vRealize Automation contiene un conector. Consulte Administración de conectores y clústeres de conectores.</p>
Atributos de usuario	<p>En la página Atributos de usuario se muestran los atributos de usuario predeterminados que se sincronizan en el directorio y podrá añadir otros atributos que puede asignar a atributos de Active Directory. Consulte Seleccionar atributos para sincronizar con el directorio.</p>
Rangos de redes	<p>En esta página se muestran los rangos de redes configurados del sistema. Al configurar un rango de redes, se permite el acceso de los usuarios a través de esas direcciones IP. Puede añadir rangos de redes adicionales, así como editar los rangos existentes. Consulte Añadir o editar un rango de redes.</p>
Proveedores de identidades	<p>En la página Proveedores de identidades se muestran los proveedores de identidades disponibles en el sistema. Los sistemas vRealize Automation contienen un conector que funciona como el proveedor de identidades predeterminado, el cual satisface muchas de las necesidades del usuario. Puede añadir instancias de proveedor de identidades de terceros o combinar ambas.</p> <p>Consulte Configurar una conexión de proveedor de identidades de terceros.</p>
Políticas	<p>En la página Políticas se muestra la política de acceso predeterminada y otras políticas de acceso de aplicaciones web que haya creado. Las políticas son un conjunto de reglas que especifican los criterios que deben reunirse para que los usuarios puedan acceder a sus portales de aplicaciones o lanzar aplicaciones web que les hayan habilitado. La política predeterminada debería ser adecuada para la mayoría de las implementaciones de vRealize Automation, aunque puede editarla en caso necesario. Consulte Administrar la política de acceso de usuarios.</p>

Conceptos importantes relacionados con Active Directory

Varios conceptos relativos a Active Directory son fundamentales para entender cómo Directories Management interactúa con sus entornos de Active Directory.

Conector

El conector, un componente del servicio, realiza las siguientes funciones.

- Sincroniza los datos de usuarios y grupos entre Active Directory y el servicio.
- Cuando se usa como proveedor de identidades, autentica a los usuarios en el servicio.

El conector es el proveedor de identidades predeterminado. Para conocer los métodos de autenticación que el conector admite, consulte la sección sobre la *administración de VMware Identity Manager*. También puede usar proveedores de identidades de terceros que admitan el protocolo SAML 2.0. Use un proveedor de identidades de terceros para un tipo de autenticación que el conector no admita o para uno que el conector sí admita, si el proveedor de identidades de terceros es preferible en función de la política de seguridad de su empresa.

Nota Incluso si usa proveedores de identidades de terceros, debe configurar el conector para que sincronice los datos de usuarios y grupos.

Directorio

El servicio de Directories Management cuenta con su propio concepto de directorio, que usa los atributos y los parámetros de Active Directory para definir usuarios y grupos. Se crean uno o varios directorios y después se sincronizan con la implementación de Active Directory. Puede crear los siguientes tipos de directorio en el servicio.

- Active Directory a través de LDAP. Cree este tipo de directorio si va a conectarse a un solo entorno de dominio de Active Directory. Para el tipo de directorio Active Directory a través de LDAP, el conector se enlaza a Active Directory mediante la autenticación de enlace simple.
- Active Directory, Autenticación de Windows integrada. Cree este tipo de directorio si va a conectarse a un entorno de Active Directory con varios dominios o bosques. El conector se enlaza a Active Directory mediante Autenticación de Windows integrada.

El tipo y el número de directorios que cree varían según el entorno de Active Directory, es decir, con un solo dominio o con varios, y según el tipo de confianza usada entre los dominios. En la mayoría de los entornos, se crea un solo directorio.

El servicio no posee acceso directo a Active Directory. El conector es el único con acceso directo a Active Directory. Por tanto, se asocia cada directorio creado en el servicio con una instancia del conector.

Trabajo

Cuando se asocia un directorio a una instancia del conector, el conector crea una partición para el directorio asociado que se denomina trabajo. Una instancia del conector tiene varios trabajos asociados a ella. Cada trabajo actúa como proveedor de identidades. Se definen y configuran los métodos de autenticación para cada trabajo.

El conector sincroniza los datos de usuarios y grupos entre Active Directory y el servicio a través de uno o varios trabajos.

No puede tener dos trabajos del tipo Autenticación de Windows integrada en la misma instancia del conector.

Entornos de Active Directory

Es posible integrar el servicio con un entorno de Active Directory formado por un único dominio de Active Directory, varios dominios en un único bosque de Active Directory o varios dominios en varios bosques de Active Directory.

Entorno de dominio único de Active Directory

La implementación única de Active Directory permite sincronizar usuarios y grupos desde un único dominio de Active Directory.

Consulte [Configurar una instancia de Active Directory mediante un vínculo LDAP/IWA](#) . Para este tipo de entorno, cuando añada un directorio al servicio, seleccione la opción Active Directory en LDAP.

Entorno de varios dominios y un único bosque de Active Directory

La implementación en varios dominios y un único bosque de Active Directory permite sincronizar usuarios y grupos desde varios dominios de Active Directory dentro de un único bosque.

Puede configurar el servicio para este tipo de entorno de Active Directory como un tipo de directorio único de Active Directory con Autenticación de Windows integrada o, si lo desea, como un tipo de directorio Active Directory en LDAP configurado con la opción de catálogo global.

- La opción que se recomienda es crear un tipo de directorio único de Active Directory con Autenticación de Windows integrada.

Consulte [Configurar una instancia de Active Directory mediante un vínculo LDAP/IWA](#) . Cuando añada un directorio a este entorno, seleccione la opción Active Directory (Autenticación de Windows integrada).

Entorno de varios bosques de Active Directory con relaciones de confianza

La implementación de varios bosques de Active Directory con relaciones de confianza permite sincronizar usuarios y grupos de varios dominios de Active Directory de diversos bosques entre los que exista una relación de confianza bidireccional.

Consulte [Configurar una instancia de Active Directory mediante un vínculo LDAP/IWA](#) . Cuando añada un directorio a este entorno, seleccione la opción Active Directory (Autenticación de Windows integrada).

Entorno de varios bosques de Active Directory sin relaciones de confianza

La implementación de varios bosques de Active Directory sin relaciones de confianza permite sincronizar usuarios y grupos de varios dominios de Active Directory de diversos bosques sin la existencia de una relación de confianza entre los dominios. Para este tipo de entorno se crean varios directorios en el servicio, uno para cada bosque.

Consulte [Configurar una instancia de Active Directory mediante un vínculo LDAP/IWA](#) . El tipo de directorios que se creen en el servicio dependerá del bosque. En el caso de bosques con varios dominios, seleccione la opción Active Directory (Autenticación de Windows integrada). En el caso de un bosque con un único dominio, seleccione la opción Active Directory en LDAP.

Usar Administración de directorios para crear un vínculo de Active Directory

Después de crear tenants de vRealize Automation, debe iniciar sesión en la consola del sistema como administrador de tenants y crear un vínculo de Active Directory para admitir la autenticación de usuario.

Se ofrecen tres opciones de protocolo de comunicación de Active Directory al configurar una conexión de Active Directory mediante Administración de directorios.

- Active Directory en LDAP: el protocolo Active Directory en LDAP admite de forma predeterminada la búsqueda de ubicaciones de servicio de DNS.
- Active Directory (Autenticación de Windows integrada): con Active Directory (Autenticación de Windows integrada) se puede configurar el dominio al que se unirá. Active Directory en LDAP es adecuado para las implementaciones de un solo dominio. Use Active Directory (Autenticación de Windows integrada) para todas las implementaciones de varios dominios y varios bosques.
- OpenLDAP: puede utilizar la versión de código abierto de LDAP para admitir la autenticación de usuarios de Administración de directorios.

Después de seleccionar un protocolo de comunicación y configurar un vínculo de Active Directory, puede especificar los dominios que se usarán con la configuración de Active Directory y, a continuación, seleccionar los usuarios y los grupos que se deben sincronizar con la configuración especificada.

Configurar una instancia de Active Directory mediante un vínculo LDAP/IWA

Puede configurar una instancia de Active Directory mediante un vínculo LDAP/IWA a fin de permitir la autenticación de usuarios con la característica Directories Management para configurar un vínculo a Active Directory y permitir la autenticación de usuarios de todos los tenants, así como seleccionar los usuarios y los grupos que se sincronizarán con el directorio de Directories Management.

Para obtener información e instrucciones acerca del uso de OpenLDAP con Administración de directorios, consulte [Configurar una conexión del directorio OpenLDAP](#).

En el caso de Active Directory (Autenticación de Windows integrada), si tiene configurado Active Directory con varios bosques y el grupo local de dominio contiene miembros de dominios de distintos bosques, compruebe que se añade el usuario de enlace al grupo de administradores del dominio en el que reside el grupo local del dominio. Si no lo hace, estos miembros no formarán parte del grupo local del dominio.

Requisitos previos

- Seleccione los atributos predeterminados necesarios y añada atributos adicionales a la página Atributos de usuario. Consulte [Seleccionar atributos para sincronizar con el directorio](#).
- Lista de grupos y usuarios de Active Directory para sincronizar desde Active Directory.
- Si su Active Directory necesita que el acceso sea mediante SSL o STARTTLS, se requerirá el certificado de CA raíz del controlador de dominio de Active Directory.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Directorios**.
- 2 Haga clic en **Añadir directorio** y seleccione **Añadir Active Directory en LDAP/IWA**.
- 3 En la página Añadir directorio, especifique la dirección IP del servidor de Active Directory en el cuadro de texto **Nombre del directorio**.
- 4 Seleccione el protocolo de comunicación apropiado de Active Directory mediante los botones de opción situados debajo del cuadro de texto **Nombre del directorio**.

Opción	Descripción
Autenticación de Windows	Seleccione Active Directory (Autenticación de Windows integrada) . Para la Autenticación de Windows integrada de Active Directory, la información necesaria incluye la dirección UPN del usuario de enlace del dominio y la contraseña.
LDAP	Seleccione Active Directory en LDAP . Para Active Directory en LDAP, la información necesaria incluye DN base, DN de enlace y contraseña de DN de enlace.

- 5 Configure el conector que sincroniza usuarios desde Active Directory hacia el directorio de VMware Directories Management en la sección de sincronización y autenticación del directorio.

Opción	Descripción
Conector de sincronización	<p>Seleccione el conector apropiado que ha de usarse para su sistema. Cada dispositivo de vRealize Automation incluye un conector predeterminado. Consulte con el administrador del sistema en el caso de que necesite ayuda para elegir el conector apropiado.</p>
Autenticación	<p>Haga clic en el botón de opciones apropiado para indicar si el conector seleccionado también realiza la autenticación.</p> <p>Si utiliza Active Directory (autenticación integrada de Windows) con un proveedor de identidades de terceros para autenticar usuarios, haga clic en No. Después de configurar la conexión de Active Directory para sincronizar usuarios y grupos, utilice la página Proveedores de identidades para agregar el proveedor de identidades de terceros para la autenticación.</p> <p>Para obtener información sobre el uso de adaptadores de autenticación, como PasswordIpddAdapter, SecurIDAdapter y RadiusAuthAdapter, consulte la <i>guía de administración de VMware Identity Manager</i>.</p>
Atributo de búsqueda directa	<p>Seleccione el atributo de cuenta apropiado que contiene el nombre de usuario. VMware recomienda utilizar el atributo sAMAccount en lugar de userPrincipalName. Si utiliza userPrincipalName en las operaciones de sincronización, la integración con software de terceros que requiera un nombre de usuario puede no funcionar correctamente.</p> <p>Nota Si selecciona sAMAccountName al usar un catálogo global (cosa que se indica activando la casilla de verificación Este directorio tiene un catálogo global en el área Ubicación del servidor), los usuarios no podrán iniciar sesión.</p>

- 6 Escriba la información apropiada en el cuadro de texto Ubicación del servidor si ha seleccionado Active Directory en LDAP, o introduzca información en los cuadros de texto de Detalles de unión a dominio si ha seleccionado Active Directory (Autenticación de Windows integrada).

Opción	Descripción
Ubicación del servidor - Mostrada cuando se selecciona Active Directory en LDAP	<p>■ Si quiere usar la ubicación del servicio de DNS para encontrar dominios de Active Directory, deje activa la casilla de verificación Este directorio admite ubicación de servicio de DNS.</p> <hr/> <p>Nota No se puede cambiar la asignación del puerto 636 si selecciona esta opción.</p> <hr/> <p>Se crea un archivo <code>domain_krb.properties</code>, que se rellena automáticamente con una lista de controladores de dominio, junto con el directorio. Consulte Acerca de la selección de controladoras de dominio.</p> <p>Si Active Directory requiere el cifrado STARTTLS, seleccione la casilla Este directorio requiere que todas las conexiones usen STARTTLS en la sección Certificados, copie el certificado de CA raíz de Active Directory y péguelo en el campo Certificado SSL.</p> <p>■ Si la instancia de Active Directory especificada no utiliza la búsqueda de ubicaciones de servicio de DNS, desactive la casilla de verificación situada junto a Este directorio admite la ubicación de servicio de DNS en los campos de Ubicación del servidor y escriba el nombre de host y el número de puerto del servidor de Active Directory en los cuadros de texto correspondientes.</p> <p>Active la casilla de verificación Este directorio tiene un catálogo global si el Active Directory asociado utiliza un catálogo global. Un catálogo global contiene una representación de todos los objetos en cada dominio de un bosque de Active Directory con varios dominios.</p> <p>Para configurar el directorio como un catálogo global, consulte la sección Entorno de varios dominios y un único bosque de Active Directory de Entornos de Active Directory.</p> <p>Si Active Directory requiere de acceso mediante SSL, active la casilla Este directorio requiere que todas las conexiones usen SSL bajo el título Certificados, y proporcione el certificado de SSL de Active Directory.</p> <p>Si se selecciona esta opción, el puerto 636 se utiliza automáticamente y no se puede cambiar.</p> <p>Asegúrese de que el certificado esté en formato PEM e incluya las líneas BEGIN CERTIFICATE y END CERTIFICATE.</p>
Detalles de unión a dominio: se muestra cuando se selecciona Active Directory (Autenticación de Windows integrada)	<p>Escriba las credenciales apropiadas en los cuadros de texto Nombre de dominio, Nombre de usuario administrador del dominio y Contraseña del administrador del dominio.</p> <p>Si Active Directory requiere el cifrado STARTTLS, seleccione la casilla Este directorio requiere que todas las conexiones usen STARTTLS en la sección Certificados, copie el certificado de CA raíz de Active Directory y péguelo en el campo Certificado SSL.</p> <p>Asegúrese de que el certificado esté en formato PEM e incluya las líneas BEGIN CERTIFICATE y END CERTIFICATE.</p>

Opción	Descripción
	Si el directorio utiliza varios dominios, agregue los certificados de CA raíz para todos los dominios de uno en uno.
	Nota Si Active Directory requiere STARTTLS y no se proporciona el certificado, no se podrá crear el directorio.

- 7 En la sección para vincular detalles de usuarios, introduzca las credenciales apropiadas para facilitar la sincronización de directorios.

Para Active Directory en LDAP:

Opción	Descripción
DN de la base	Escriba el nombre distintivo base de búsqueda. Por ejemplo, cn=users,dc=corp,dc=local .
DN de enlace	Escriba el nombre distintivo del enlace. Por ejemplo, cn=fritz infra,cn=usuarios,dc=empresa,dc=local .

Para Active Directory (Autenticación de Windows integrada):

Opción	Descripción
UPN del usuario de enlace	Escriba el nombre principal del usuario que puede autenticar con el dominio. Por ejemplo, NombreDeUsuario@ejemplo.com.
Contraseña de DN de enlace	Escriba la contraseña del usuario de enlace.

- 8 Haga clic en **Probar conexión** para probar la conexión al directorio configurado.

Este botón no aparece si ha seleccionado Active Directory (Autenticación de Windows integrada).

- 9 Haga clic en **Guardar y Siguiente**.

Aparece la página Seleccione los dominios con la lista de dominios.

- 10 Revise y actualice los dominios que se enumeran para la conexión de Active Directory.

- Para Active Directory (Autenticación de Windows integrada), seleccione los dominios que deberán asociarse con esta conexión de Active Directory.
- Para Active Directory en LDAP, el dominio disponible se muestra con una marca de verificación.


Nota Si añade un dominio de confianza una vez creado el directorio, el servicio no detectará automáticamente el nuevo dominio de confianza. Para permitir que el servicio detecte el dominio, el conector deberá abandonar el dominio y, a continuación, volver a unirse a él. Una vez que el conector vuelva a unirse al dominio, el dominio de confianza aparecerá en la lista.

- 11 Haga clic en **Siguiente**.

- 12** Compruebe que los nombres de atributos del directorio de Directories Management estén asignados a los atributos correctos de Active Directory.

Si los nombres de atributos del directorio no se asignan correctamente, seleccione el atributo correcto de Active Directory en el menú desplegable.

- 13** Haga clic en **Siguiente**.

- 14** Haga clic en  para seleccionar los grupos que desea sincronizar entre Active Directory y el directorio.

Cuando se añade un grupo de Active Directory, si los miembros de ese grupo no están incluidos en la lista de usuarios, entonces se añaden. Cuando sincroniza un grupo, los usuarios que no tengan Usuarios del dominio como su grupo principal en Active Directory no se sincronizan.

Nota El sistema de autenticación de usuarios de Directories Management importa los datos de Active Directory al añadir grupos y usuarios, y la velocidad del sistema quedará limitada por las prestaciones de Active Directory. En consecuencia, las operaciones de importación podrían tardar mucho tiempo en completarse en función del número de grupos y usuarios que se añada. Para minimizar la posibilidad de retrasos o problemas, limite el número de grupos y usuarios a únicamente los necesarios para el funcionamiento de vRealize Automation.


Si el rendimiento del sistema se degrada o si se producen errores, cierre las aplicaciones que no sean necesarias y asegúrese de que su sistema tenga asignada a Active Directory la memoria adecuada. Si los problemas persisten, aumente la asignación de memoria a Active Directory según sea necesario. En el caso de sistemas con una gran cantidad de usuarios y grupos, es posible que deba aumentar la asignación de memoria de Active Directory hasta los 24 GB.

- 15** Haga clic en **Siguiente**.

- 16** Haga clic en  para añadir más usuarios.

Los valores correspondientes son los siguientes:

- Usuario único: **CN=username,CN=Users,OU=Users,DC=myCorp,DC=com**
- Varios usuarios: **OU=Users,OU=myUnit,DC=myCorp,DC=com**

Para excluir a usuarios, haga clic en  para crear un filtro de exclusión de determinados tipos de usuarios. Debe seleccionar el atributo de usuario por el que desea filtrar, la regla de consulta y el valor.

- 17** Haga clic en **Siguiente**.

- 18** Revise la página para ver cuántos usuarios y grupos se han sincronizado en el directorio.

Si desea realizar cambios en los usuarios y grupos, haga clic en los vínculos Editar.

Nota Asegúrese de especificar los DN de usuario que se encuentren bajo el DN base especificado anteriormente. Si el DN de usuario está fuera del DN base, los usuarios de dicho DN se sincronizarán, pero no podrán iniciar sesión.

- 19** Haga clic en **Mover a Workspace** para iniciar la sincronización con el directorio.

Resultados

La conexión con Active Directory queda completada y los usuarios y grupos seleccionados se añaden al directorio. Ahora puede asignar el usuario y los grupos a las funciones apropiadas de vRealize Automation seleccionando **Administración > Usuarios y grupos > Usuarios y grupos de directorios**. Consulte [Asignar funciones a usuarios o grupos de directorios](#) para obtener más información.

Pasos siguientes

Si su entorno de vRealize Automation está configurado para alta disponibilidad, debe configurar específicamente la administración de directorios para alta disponibilidad. Consulte [Configurar Administración de directorios para alta disponibilidad](#).

- Configure los métodos de autenticación. Una vez sincronizados los usuarios y grupos con el directorio, si también se utiliza el conector para la autenticación, podrá configurar otros métodos de autenticación en este último. Si el proveedor de identidades de autenticación es un tercero, configúrelo en el conector.
- Revise la política de acceso predeterminada. La política de acceso predeterminada se configura para permitir que todos los dispositivos de todos los rangos de redes accedan al explorador web, con un tiempo de espera de sesión definido en ocho horas, o bien acceder a una aplicación del cliente con un tiempo de espera de sesión de 2.160 horas (90 días). Puede cambiar la política de acceso predeterminada. Asimismo, cuando añada aplicaciones web al catálogo, podrá crear otras nuevas.
- Aplique la personalización de marca a la consola de administración, a las páginas del portal de usuario y a la pantalla de inicio de sesión.

Configurar una conexión del directorio OpenLDAP

Puede configurar una conexión del directorio OpenLDAP con Administración de directorios.

Aunque existen varios protocolos LDAP diferentes, OpenLDAP es el único que ha sido probado y autorizado para su uso con Administración de directorios de vRealize Automation.

Para integrar el directorio LDAP, cree el directorio Directories Management correspondiente y sincronice los usuarios y los grupos del directorio LDAP al directorio Directories Management. Puede programar una sincronización periódica para las actualizaciones siguientes.

Seleccione también los atributos LDAP que quiera sincronizar para los usuarios y asígneles a los atributos de Directories Management.

La configuración del directorio LDAP puede basarse en las programaciones predeterminadas o puede crear programaciones personalizadas. También debe definir los atributos personalizados. Para que Directories Management pueda solicitar el directorio LDAP para obtener los objetos de grupo o usuario, debe proporcionar los nombres de los filtros de búsqueda de LDAP que se apliquen a su directorio LDAP.

En concreto, debe proporcionar la siguiente información.

- Los filtros de búsqueda para obtener los grupos, los usuarios y el usuario de enlace
- Los nombres de atributos LDAP de la pertenencia a grupos, UUID y el nombre distintivo

Nota Administración de directorios utiliza el tamaño de página predeterminado, el cual es 1500, para las consultas de LDAP. Si configura una conexión de directorio OpenLDAP, debe habilitar la extensión de control de resultados de página simple de OpenLDAP para limitar el número de resultados que se muestran. Si no se utiliza esta extensión, se pueden producir errores de sincronización de usuarios y grupos.

Requisitos previos

- Revise la configuración en la página Atributos de usuario y añada más atributos que quiera sincronizar. Asignará los atributos de Directories Management a los atributos del directorio LDAP cuando cree el directorio. Estos atributos se sincronizarán para los usuarios del directorio.

Nota Si realiza cambios en los atributos de usuario, tenga en cuenta los efectos que puedan tener en otros directorios del servicio. Si tiene previsto agregar los directorios LDAP y Active Directory, asegúrese de que ningún atributo está marcado como obligatorio excepto **userName**. Las opciones de configuración de la página Atributos de usuario se aplican a todos los directorios del servicio. Si un atributo está marcado como obligatorio, los usuarios sin dicho atributo no se sincronizan con el servicio de Directories Management.

- Cuenta de usuario DN de enlace. Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque.
- En el directorio LDAP, el UUID de los usuarios y los grupos debe aparecer como texto sin formato.
- En el directorio LDAP, debe existir un atributo de dominio para todos los usuarios y los grupos.

Asígnelo al atributo del **dominio** de Directories Management cuando cree el directorio Directories Management.

- Los nombres de usuario no deben tener espacios. Si un nombre de usuario tiene un espacio, el usuario se sincroniza pero las autorizaciones no están disponibles para dicho usuario.
- Si utiliza la autenticación con certificado, los usuarios deben tener los valores para los atributos de la dirección de correo electrónico y userPrincipalName.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Directorios**.
- 2 Haga clic en **Añadir directorio** y seleccione **Añadir directorio LDAP**.
- 3 Introduzca la información solicitada en la página Agregar directorio LDAP.

Opción	Descripción
Nombre de directorio	Especifique un nombre para el directorio de Directories Management.
Sincronización de directorio y autenticación	<p>a En el campo Conector de sincronización, seleccione el conector que desee utilizar para sincronizar usuarios y grupos del directorio LDAP con el directorio de Directories Management.</p> <p>De forma predeterminada, un componente del conector estará siempre disponible con el servicio de Directories Management. Este conector aparecerá en la lista desplegable. Si instala varios dispositivos de Directories Management para lograr una alta disponibilidad, el componente del conector de cada uno aparecerá en la lista.</p> <p>No es necesario un conector diferente para un directorio LDAP. Un conector puede ser compatible con varios directorios, independientemente de si cuentan con directorios LDAP o Active Directory.</p> <p>b En el campo Autenticación, seleccione Sí si desea utilizar el directorio LDAP para autenticar a los usuarios.</p> <p>Si desea utilizar un proveedor de identidades externo para autenticar a los usuarios, seleccione No. Después de añadir la conexión del directorio para sincronizar los usuarios y los grupos, acceda a la página Administración > Administración de directorios > Proveedores de identidades para agregar el proveedor de identidades de terceros para realizar la autenticación.</p> <p>c En la mayoría de las configuraciones, deje seleccionada la opción predeterminada Personalizado en el cuadro de texto Atributo de búsqueda de directorios. En el campo Atributo de búsqueda de directorios personalizada, especifique el atributo de directorio LDAP que se utilizará para los nombres de usuario y de grupo. Este atributo identifica entidades de forma exclusiva, como usuarios y grupos, del servidor LDAP. Por ejemplo, cn.</p>
Ubicación del servidor	<p>Introduzca el número de puerto y el host del servidor del directorio LDAP. En el caso del host del servidor, puede especificar el nombre del dominio plenamente cualificado o la dirección IP. Por ejemplo, myLDAPserver.example.com o 100.00.00.0.</p> <p>Si cuenta con un clúster de servidores bajo un equilibrador de carga, introduzca la información de este último en su lugar.</p>

Opción	Descripción
Configuración LDAP	<p>Especifica los atributos y los filtros de búsqueda de LDAP que Directories Management puede utilizar para solicitar su directorio LDAP. Los valores predeterminados se proporcionan según el esquema principal de LDAP.</p> <p>Consultas de filtro</p> <ul style="list-style-type: none"> ■ Grupos: es el filtro de búsqueda que permite obtener los objetos de grupo. Por ejemplo: (objectClass=group) ■ Usuario de enlace: es el filtro de búsqueda que permite obtener el objeto de usuario de enlace, es decir, el usuario que puede enlazarse con el directorio. Por ejemplo: (objectClass=person) ■ Usuarios: es el filtro de búsqueda que permite obtener los usuarios para la sincronización. Por ejemplo: (&(objectClass=user)(objectCategory=person)) <p>Atributos</p> <ul style="list-style-type: none"> ■ Afiliación: es el atributo que se utiliza en su directorio LDAP para definir los miembros de un grupo. Por ejemplo: member ■ UUID del objeto: es el atributo que se utiliza en su directorio LDAP para definir el UUID. Por ejemplo: entryUUID ■ Nombre distintivo: es el atributo que se utiliza en su directorio LDAP para definir el nombre distintivo de un usuario o un grupo. Por ejemplo: entryDN
Certificados	<p>Si el directorio LDAP requiere acceso mediante SSL, active la casilla de verificación Este directorio requiere que todas las conexiones usen SSL. A continuación, copie el certificado CA SSL raíz del servidor de directorios LDAP y péguelo en el cuadro de texto Certificado SSL. Asegúrese de que el certificado esté en formato PEM e incluya las líneas "BEGIN CERTIFICATE" y "END CERTIFICATE".</p> <p>Finalmente, asegúrese de que se especifica el número de puerto correcto en el campo Puerto del servidor en la sección Ubicación del servidor de la página.</p>
Detalles del usuario de enlace	<p>DN base: introduzca el DN desde el que deben empezar las búsquedas. Por ejemplo, cn=users,dc=example,dc=com</p> <p>Todos los usuarios correspondientes deben residir en el DN base. Si un usuario determinado no se encuentra bajo el DN base, ese usuario no podrá iniciar sesión aunque sea un miembro de un grupo situado bajo el DN base.</p> <p>DN de enlace: introduzca el DN que se utilizará para enlazar con el directorio LDAP. También puede introducir nombres de usuario, pero un DN es más apropiado para la mayoría de las implementaciones.</p> <p>Nota Se recomienda utilizar una cuenta de usuario de DN de enlace con una contraseña que no caduque.</p> <p>Contraseña DN de enlace: introduzca la contraseña del usuario DN de enlace.</p>

- 4 Para probar la conexión al servidor del directorio LDAP, haga clic en **Probar conexión**.

Si no se realizó la conexión correctamente, compruebe la información que introdujo y haga los cambios necesarios.

- 5 Haga clic en **Guardar y Siguiente**.

- 6 Compruebe que se haya seleccionado el dominio correcto en la página Seleccione los dominios y, a continuación, haga clic en **Siguiente**.

- 7 En la página Asignar atributos, compruebe que los atributos de Directories Management se asignaron a los atributos LDAP correctos.

Estos atributos se sincronizarán para los usuarios.

Importante Debe especificar una asignación para los atributos de **dominio**.

Puede agregar atributos a la lista desde la página Atributos de usuario.

- 8 Haga clic en **Siguiente**.

- 9 Haga clic en **+** para seleccionar los grupos del directorio LDAP que desea sincronizar con el directorio de Directories Management en la página Seleccionar los grupos (usuarios) que desea sincronizar.

Si cuenta con varios grupos con el mismo nombre en su directorio LDAP, debe especificar nombres únicos para ellos en la página de grupos.

Cuando se añade un grupo de Active Directory, si los miembros de ese grupo no están incluidos en la lista de usuarios, entonces se añaden. Cuando sincroniza un grupo, los usuarios que no tengan Usuarios del dominio como su grupo principal en Active Directory no se sincronizan.

La opción **Sincronizar miembros de grupo anidados** se habilita de forma predeterminada. Cuando se habilita esta opción, todos los usuarios que pertenezcan al grupo que seleccione y los que pertenezcan a grupos anidados dentro de este grupo se sincronizan. Tenga en cuenta que los grupos anidados no se sincronizan. Solo se sincronizarán los usuarios que pertenezcan a los grupos anidados. En el directorio de Directories Management, estos usuarios aparecerán como los miembros del grupo de nivel superior que seleccionó para sincronizarse. Efectivamente, la jerarquía en un grupo seleccionado se aplanará y los usuarios de todos los niveles se muestran en Directories Management como miembros del grupo seleccionado.

Si desactiva esta opción, todos los usuarios que pertenezcan directamente a ese grupo se sincronizarán cuando especifique un grupo para que se sincronice. Los usuarios que pertenezcan a grupos anidados bajo este grupo no se sincronizarán. Deshabilitar esta opción resulta útil para las grandes configuraciones del directorio en las que atravesar un árbol de grupo requiera demasiado tiempo o demasiados recursos. Si desactiva esta opción, asegúrese de seleccionar todos los grupos cuyos usuarios desea sincronizar.

Nota El sistema de autenticación de usuarios de Directories Management importa los datos de Active Directory al añadir grupos y usuarios, y la velocidad del sistema quedará limitada por las prestaciones de Active Directory. En consecuencia, las operaciones de importación podrían tardar mucho tiempo en completarse en función del número de grupos y usuarios que se añada. Para minimizar la posibilidad de retrasos o problemas, limite el número de grupos y usuarios a únicamente los necesarios para el funcionamiento de vRealize Automation.

Si el rendimiento del sistema disminuye o si se producen errores, cierre todas las aplicaciones que no sean necesarias y asegúrese de que el sistema haya asignado la cantidad de memoria adecuada a Administración de directorios. Si los problemas continúan, aumente la asignación de memoria de Administración de directorios, según sea necesario. En el caso de sistemas con una gran cantidad de usuarios y grupos, puede que deba aumentar la asignación de memoria de Administración de directorios hasta 24 GB.

10 Haga clic en **Siguiente**.

11 Haga clic en **+** para agregar más usuarios. Por ejemplo, introduzca **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.

Aquí puede añadir unidades organizativas, así como usuarios individuales.

Puede crear un filtro que excluya algunos tipos de usuarios. Seleccione el atributo de usuario por el que desea filtrar, la regla de consulta y el valor.

12 Haga clic en **Siguiente**.

13 Revise la página para ver cuántos usuarios y grupos se sincronizarán con el directorio así como la programación de la sincronización predeterminada.

Para realizar cambios en los usuarios y los grupos o en la frecuencia de sincronización, haga clic en los vínculos **Editar**.

14 Haga clic en **Sincronizar directorio** para iniciar la sincronización del directorio.

Resultados

Se establece la conexión al directorio LDAP y los usuarios y los grupos se sincronizan desde el directorio LDAP al directorio Directories Management.

Ahora puede asignar el usuario y los grupos a las funciones apropiadas de vRealize Automation seleccionando **Administración > Usuarios y grupos > Usuarios y grupos de directorios**. Consulte [Asignar funciones a usuarios o grupos de directorios](#) para obtener más información.

Limitaciones de la integración del directorio LDAP

Existen diversas limitaciones importantes relacionadas con la integración del directorio LDAP en Administración de directorios.

- Solo puede integrar un entorno del directorio LDAP con un dominio único.
Para integrar varios dominios desde un directorio LDAP, necesita crear directorios de Directories Management adicionales, uno para cada dominio.
- Los siguientes métodos de autenticación no son compatibles para los directorios de Directories Management de tipo LDAP.
 - autenticación de Kerberos
 - RSA Adaptive Authentication
 - ADFS como proveedor de identidades externo
 - SecurID
 - Autenticación de Radius con el servidor de código de acceso SMS y Vasco
- No puede unirse a un dominio LDAP.
- La integración a los recursos publicados por Citrix o de View no es compatible para los directorios de Directories Management de tipo LDAP.
- Los nombres de usuario no deben tener espacios. Si un nombre de usuario tiene un espacio, el usuario se sincroniza pero las autorizaciones no están disponibles para dicho usuario.
- Si tiene previsto agregar los directorios LDAP y Active Directory, asegúrese de que no marca ningún atributo obligatorio en la página Atributo de usuario, excepto userName, que puede ser obligatorio que se marque. Las configuraciones de la página Atributos de usuario se aplican a todos los directorios del servicio. Si un atributo está marcado como obligatorio, los usuarios sin dicho atributo no se sincronizan con el servicio de Directories Management.
- Si cuenta con varios grupos con el mismo nombre en su directorio LDAP, debe especificar nombres únicos para ellos en el servicio de Directories Management. Puede especificar los nombres cuando selecciona los grupos que desea sincronizar.
- La opción para permitir a los usuarios restablecer las contraseñas caducadas no está disponible.
- No es compatible el archivo `domain_krb.properties`.

Configurar Administración de directorios para alta disponibilidad

Puede usar Administración de directorios para configurar una conexión de Active Directory de alta disponibilidad en vRealize Automation.

Cada dispositivo de vRealize Automation incluye un conector que admite la autenticación de usuarios, aunque normalmente solo hay un conector configurado para realizar la sincronización de directorios. No importa qué conector elija como conector de sincronización. Para admitir la alta disponibilidad de Administración de directorios, es necesario configurar manualmente un

segundo conector que corresponda al segundo dispositivo de vRealize Automation, el cual se conecta con el proveedor de identidades y apunta a la misma instancia de Active Directory. Con esta configuración, si se produce un error en un dispositivo, el otro se encarga de administrar la autenticación de usuarios.

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

También se utiliza un conector para la sincronización de usuarios, pero se configura un solo conector para realizar la sincronización de directorios. Los usuarios sincronizados se guardan en la base de datos de dispositivos, que todos los nodos agrupados en clúster pueden leer. Si se produce un error en el conector responsable de la sincronización de directorios, esta sincronización deja de funcionar. Para recuperar la función, el administrador de tenants debe solicitar manualmente otro conector a fin de sincronizar los directorios mediante la interfaz de usuario de vRealize Automation. Consulte [Habilitar la sincronización de directorios en un conector secundario](#).

Para obtener más información acerca del trabajo con conectores, consulte [Administración de conectores y clústeres de conectores](#).

Requisitos previos

- Configure la implementación de vRealize Automation con al menos dos instancias del dispositivo de vRealize Automation.
- Instale vRealize Automation en modo Enterprise que funcione en un único dominio con dos instancias del dispositivo de vRealize Automation.
- Instale y configure un equilibrador de carga adecuado para que funcione con la implementación de vRealize Automation.
- Configure los tenants y la administración de directorios usando uno de los conectores proporcionados con las instancias instaladas del dispositivo de vRealize Automation. Para obtener más información acerca de la configuración de tenants, consulte [Configurar las opciones de tenant](#).

Procedimiento

- 1 Inicie sesión en el equilibrador de carga de la implementación de vRealize Automation como administrador de tenants.

La URL del equilibrador de carga es <dirección del equilibrador de carga>/vcac/org/*tenant_name*.

- 2 Seleccione **Administración > Administración de directorios > Proveedores de identidades**.

- 3 Haga clic en el proveedor de identidades que está en uso en su sistema actualmente.
Se muestran el directorio y el conector existentes responsables de la administración de identidades básica en el sistema.
- 4 En la página de propiedades del proveedor de identidades, haga clic en la lista desplegable **Añadir un conector** y seleccione el conector que corresponda al dispositivo de vRealize Automation secundario.
- 5 Escriba la contraseña adecuada en el cuadro de texto **Enlazar contraseña de DN** que aparece al seleccionar el conector.
- 6 Haga clic en **Añadir conector**.
- 7 El conector principal aparece en el cuadro de texto **Nombre de host de IDP** de forma predeterminada. Cambie el nombre de host para que apunte al equilibrador de carga.

Habilitar la sincronización de directorios en un conector secundario

Si se produce un error en el conector principal, otra instancia del conector gestiona automáticamente la autenticación. En el caso de un error de sincronización de directorios, es necesario modificar la configuración de los directorios en Administración de directorios para utilizar la instancia del conector secundario correspondiente. Puede habilitar la sincronización de directorios en un solo conector a la vez.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Directorios**.
- 2 Seleccione el directorio asociado a la instancia del conector original.

Nota Puede consultar esta información en la página **Directorios > Conectores**.

- 3 En la sección Autenticación y sincronización de directorios de la página Directorio, seleccione otra instancia del conector en la lista desplegable **Conector de sincronización**.
- 4 En la sección Detalles del usuario de enlace, introduzca la contraseña de la cuenta de enlace de Active Directory en el cuadro de texto **Enlazar contraseña de DN**.
- 5 Haga clic en **Guardar**.

Configurar una relación de confianza bidireccional entre vRealize Automation y Active Directory

Puede mejorar la seguridad del sistema de una conexión de Active Directory de vRealize Automation básica mediante la configuración de una relación de confianza bidireccional entre el proveedor de identidades y los Servicios federados de Active Directory.

Para configurar una relación de confianza bidireccional entre vRealize Automation y Active Directory, debe crear un proveedor de identidades personalizado y añadirle a continuación los metadatos de Active Directory a dicho proveedor. Asimismo, deberá modificar la política predeterminada que utiliza su implementación de vRealize Automation. Por último, deberá configurar Active Directory para que reconozca a su proveedor de identidades.

Requisitos previos

- Compruebe que ha configurado tenants para su implementación de vRealize Automation y un vínculo adecuado de Active Directory que admita la autenticación básica mediante ID de usuario y contraseña de Active Directory.
- Active Directory deberá estar instalado y configurado para utilizarse en su red.
- Obtenga los metadatos apropiados de los Servicios federados de Active Directory (ADFS).
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Obtenga el archivo de metadatos de federación.

Puede descargar el archivo desde <https://servername.domain/FederationMetadata/2007-06/FederationMetadata.xml>.

- 2 Busque la palabra "logout" y edite la ubicación de cada instancia para que señale a <https://servername.domain/adfs/ls/logout.aspx>.

Por ejemplo, la siguiente:

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/ "/>
```

Deberá cambiarse por lo siguiente:

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/logout.aspx"/>
```

3 Cree un nuevo proveedor de identidades para su implementación.

- Seleccione **Administración > Administración de directorios > Proveedores de identidades**.
- Haga clic en **Añadir proveedor de identidades** y rellene los campos según corresponda.

Opción	Descripción
Nombre de proveedor de identidades	Escriba el nombre del nuevo proveedor de identidades.
Metadatos del proveedor de identidades (URI o XML)	Pegue ahí el contenido del archivo de metadatos de los Servicios federados de Active Directory.
Política de ID de nombres en la solicitud SAML (opcional)	Si corresponde, escriba el nombre de la solicitud SAML de la política de identidades.
Usuarios	Seleccione los dominios para los que desea que los usuarios tengan privilegios de acceso.
Procesar metadatos de IDP	Haga clic para procesar el archivo de metadatos que ha añadido.
Red	Seleccione los rangos de redes a los que desea que los usuarios tengan acceso.
Métodos de autenticación	Escriba un nombre para el método de autenticación utilizado por este proveedor de identidades.
Contexto SAML	Seleccione el contexto apropiado para el sistema.
Certificado de firma de SAML	Haga clic en el vínculo que hay junto al encabezado de metadatos de SAML para descargar los metadatos de administración de directorios.

- Guarde el archivo de metadatos de administración de directorios con el nombre `sp.xml`.
- Haga clic en **Agregar**.

4 Añada una regla a la política predeterminada.

- Seleccione **Administración > Administración de directorios > Políticas**.
- Haga clic en el nombre de la política predeterminada.
- Haga clic en el icono + situado debajo del encabezado **Reglas de políticas** para añadir una nueva regla.

Utilice los campos de la página Añadir una regla de política para crear una regla que especifique los métodos correspondientes de autenticación principal y secundario que se utilizarán para el rango de redes y el dispositivo en cuestión.

Por ejemplo, si su rango de redes es **Mi máquina** y necesita acceder a contenido de **Todos los tipos de dispositivos**, en el caso de una implementación típica, deberá autenticarse con el siguiente método: **Nombre de usuario y contraseña de ADFS**.

- Haga clic en **Guardar** para guardar los cambios en la política.
- En la página Política predeterminada, arrastre la nueva regla hasta la parte superior de la tabla para que tenga prioridad ante las demás reglas existentes.

- 5 Mediante la consola de administración de los Servicios federados de Active Directory u otra herramienta apropiada, configure una relación de confianza de receptor con el proveedor de identidades de vRealize Automation.

Para configurar esta relación de confianza, deberá importar los metadatos de administración de directorios que descargó previamente. Consulte la documentación de Microsoft Active Directory para obtener más información sobre cómo configurar los Servicios federados de Active Directory para relaciones de confianza bidireccionales. Como parte de este proceso, debe hacer lo siguiente:

- Configurar una relación de confianza de receptor. Cuando configure esta relación de confianza, deberá importar el archivo XML de metadatos del servicio de proveedor de identidades de VMware que había copiado y guardado.
- Crear una regla de notificación que transforme los atributos recuperados de LDAP de la regla Obtener atributos en el formato deseado de SAML. Después de crear la regla, añada el siguiente texto para editar la regla:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/
format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties["http://
schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"vmwareidentity.domain.com");
```

Configurar la federación de SAML entre Directories Management y SSO2

Puede establecer una federación de SAML entre vRealize Automation Directories Management y los sistemas que utilicen SSO2 para admitir el Single Sign-On.

Establezca una federación entre Directories Management y SSO2 creando una conexión de SAML entre las dos partes. Actualmente, el único flujo compatible de un extremo a otro se produce cuando SSO2 actúa como proveedor de identidades (IdP) y Directories Management actúa como proveedor de servicios (SP).

En la autenticación de usuario de SSO2, la misma cuenta debe existir tanto en Directories Management como en SSO2. Como mínimo, el valor de UserPrincipalName (UPN) del usuario tiene que coincidir en ambos extremos. Otros atributos pueden diferir ya que son necesarios para identificar el asunto de SAML.

Para usuarios locales en SSO2, como `admin@vsphere.local`, las cuentas correspondientes también deben existir en Directories Management (donde coincide al menos el UPN del usuario). Cree esas cuentas de forma manual o mediante un script con las API de creación de usuario local de Directories Management.

La configuración de SAML entre SSO2 y Directories Management requiere configurar los componentes de Administración de directorios y SSO.

Tabla 2-4. Configuración del componente de federación de SAML

Componente	Configuración
Administración de directorios	Configure SSO2 como proveedor de identidades externo en Directories Management y actualice la política de autenticación predeterminada. Puede crear un script automatizado para configurar Directories Management.
Componente de SSO2	Configure Directories Management como proveedor de servicios importando el archivo <code>sp.xml</code> de Directories Management. Este archivo le permite configurar SSO2 para que use Directories Management como proveedor de servicios (SP).

Requisitos previos

- Configure tenants para su implementación de vRealize Automation. Consulte [Crear tenants adicionales](#).
- Establezca un vínculo de Active Directory adecuado que admita la autenticación básica con identificador de usuario y contraseña de Active Directory.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Descargue los metadatos del proveedor de identidades de SSO2 a través de la interfaz de usuario de SSO2.
 - a Inicie sesión en vCenter como administrador en `https://<cloudvm-hostname>/`.
 - b Haga clic en el vínculo para iniciar sesión en vSphere Web Client.
 - c En el panel de navegación izquierdo, seleccione **Administración > Single Sign On > Configuración**.
 - d Haga clic en **Descargar** junto a los metadatos para su encabezado del proveedor de servicios de SAML.
Debería comenzar la descarga del archivo `vsphere.local.xml`.
 - e Copie el contenido del archivo `vsphere.local.xml`.
- 2 En la página de proveedores de identidades de administración de directorios de vRealize Automation, cree un nuevo proveedor de identidades.
 - a Inicie sesión en vRealize Automation como **administrador de tenants**.
 - b Seleccione **Administración > Administración de directorios > Proveedores de identidades**.

- c Haga clic en **Añadir proveedor de identidades** y proporcione la información de configuración.

Opción	Acción
Nombre del proveedor de identidades	Escriba el nombre del nuevo proveedor de identidades.
Cuadro de texto Metadatos del proveedor de identidades (URI o XML)	Pegue el contenido del archivo de metadatos <code>idp.xml</code> de SSO2 en el cuadro de texto y haga clic en Procesar metadatos de IDP .
Política de ID de nombres en la solicitud SAML (opcional)	Escriba <code>http://schemas.xmlsoap.org/claims/UPN</code> .
Usuarios	Seleccione los dominios para los que desea que los usuarios tengan privilegios de acceso.
Red	<p>Seleccione los rangos de redes a los que desea que los usuarios tengan privilegios de acceso.</p> <p>Si desea autenticar usuarios desde una dirección IP, seleccione Todos los rangos.</p>
Métodos de autenticación	Escriba un nombre para el método de autenticación. A continuación, use el menú desplegable Contexto de SAML que se encuentra a la derecha para asignar el método de autenticación a <code>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</code> .
Certificado de firma de SAML	Haga clic en el vínculo que hay junto al encabezado de metadatos de SAML para descargar los metadatos de administración de directorios.

- d Guarde el archivo de metadatos de administración de directorios con el nombre `sp.xml`.
- e Haga clic en **Agregar**.

- 3** Actualice la política de autenticación pertinente usando la página de políticas de administración de directorios para redirigirla al proveedor de identidades de SSO2 externo.

- a Seleccione **Administración > Administración de directorios > Políticas**.
- b Haga clic en el nombre de la política predeterminada.
- c Haga clic en el método de autenticación que se encuentra bajo el encabezado **Reglas de política** para editar la regla de autenticación existente.
- d En la página Editar una regla de política, cambie el método de autenticación de contraseña al método adecuado.
- En este caso, el método debe ser SSO2.
- e Haga clic en **Guardar** para guardar las actualizaciones de la política.

- 4** En el panel de navegación izquierdo, seleccione **Administración > Single Sign-On > Configuración** y haga clic en **Actualizar** para cargar el archivo `sp.xml` en vSphere.

Añadir usuarios o grupos a una conexión de Active Directory

Puede añadir usuarios o grupos a una conexión existente de Active Directory.

El sistema de autenticación de usuarios de Administración de directorios importa los datos de Active Directory cuando se añaden grupos y usuarios. La velocidad con la que se realiza el transporte de los datos está limitada por las capacidades de Active Directory. Por lo tanto, las acciones pueden durar mucho tiempo en función del número de grupos y usuarios que se añadan. Para minimizar los problemas, limite los grupos y usuarios a únicamente los grupos y usuarios que hagan falta para una acción de vRealize Automation. Si se producen errores, cierre las aplicaciones que no sean necesarias y compruebe que su implementación tenga asignada una cantidad de memoria adecuada a Active Directory. Si el problema persiste, aumente la asignación de memoria para Active Directory. En el caso de implementaciones con grandes números de usuarios y grupos, quizás tenga que aumentar la asignación de memoria de Active Directory hasta los 24 GB.

Si sincroniza una implementación de vRealize Automation con muchos usuarios y grupos, se pueden producir retrasos antes de que estén disponibles los detalles del registro. La marca de hora del archivo de log y la hora de finalización que se muestra en la consola pueden ser diferentes.

Si los miembros de un grupo no están en la lista de usuarios, se añadirán a esta cuando se añada el grupo desde Active Directory. Cuando sincroniza un grupo, los usuarios que no tengan Usuarios del dominio como su grupo principal en Active Directory no se sincronizan.

Nota No se puede cancelar una acción de sincronización una vez que se inicia.

Requisitos previos

- Conector instalado y con el código de activación activado. Seleccione los atributos predeterminados necesarios y añada atributos adicionales a la página Atributos de usuario.
Consulte [Seleccionar atributos para sincronizar con el directorio](#) en [Configuración de vRealize Automation](#).
- Lista de grupos y usuarios de Active Directory para sincronizar desde Active Directory.
- Para Active Directory en LDAP, la información necesaria incluye DN base, DN de enlace y contraseña de DN de enlace.
- Para la Autenticación de Windows integrada de Active Directory, la información necesaria incluye la dirección UPN del usuario de enlace del dominio y la contraseña.
- Si se accede a Active Directory sobre SSL, se necesita una copia del certificado SSL.
- Si tiene un Active Directory de varios bosques integrado con la autenticación de Windows y el grupo local de dominios contiene a miembros de bosques diferentes, haga lo siguiente. Añada al usuario de enlace al grupo Administradores del grupo local de dominios. De lo contrario, estos miembros no estarán en el grupo local de dominios.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Directorios**.

- 2 Haga clic en el nombre de directorio que desee.
- 3 Haga clic en **Configuración de sincronización** para abrir un cuadro de diálogo con opciones de sincronización.
- 4 Haga clic en el icono adecuado, en función de si desea cambiar la configuración del usuario o del grupo.

Para editar la configuración del grupo:

- Para añadir grupos, haga clic en el icono + para añadir una línea para definiciones de DN de grupo e introduzca el DN de grupo adecuado.
- Si desea eliminar una definición de DN de grupo, haga clic en el icono x para el DN de grupo que desee.

Para editar la configuración del usuario:

- ◆ Para añadir usuarios, haga clic en el icono + para añadir una línea para la definición de DN de usuario e introduzca el DN de usuario adecuado.

Si desea eliminar una definición de DN de usuario, haga clic en el icono x para el DN de usuario que desee.

- 5 Haga clic en **Guardar** para guardar los cambios sin tener que sincronizar las actualizaciones de forma inmediata. Haga clic en **Guardar y sincronizar** para guardar los cambios y sincronizar las actualizaciones de forma inmediata.

Seleccionar atributos para sincronizar con el directorio

Cuando configura el directorio de Directories Management para que se sincronice con Active Directory, especifica los atributos de usuario que se sincronizan con el directorio. Antes de configurar el directorio, puede especificar en la página Atributos de usuario qué atributos predeterminados son necesarios y, si lo desea, añadir atributos adicionales que desee asignar a los atributos de Active Directory.

Cuando configura la página Atributos de usuario antes de que se cree el directorio, puede cambiar los atributos predeterminados de obligatorios a no obligatorios, marcar atributos como obligatorios y añadir atributos personalizados.

Para obtener una lista de los atributos asignados predeterminados, consulte [Administrar atributos de usuario que se sincronizan desde Active Directory](#).

Una vez creado el directorio, puede convertir un atributo obligatorio en no obligatorio, y puede eliminar atributos personalizados. No se puede convertir un atributo en atributo obligatorio.

Cuando añada otros atributos para que se sincronicen con el directorio, una vez creado el directorio, vaya a la página Atributos asignados del directorio para asignar estos atributos a atributos de Active Directory.

Procedimiento

- 1 Inicie sesión en vRealize Automation como administrador del sistema o administrador de tenants.

- 2 Haga clic en la pestaña Administración.
- 3 Seleccione **Administración de directorios > Atributos de usuario**
- 4 En la sección Atributos predeterminados, repase la lista de atributos obligatorios y realice los cambios necesarios para reflejar cuáles deben serlo.
- 5 En la sección Atributos, añada el nombre de atributo de directorio de Directories Management a la lista.
- 6 Haga clic en **Guardar**.
Se actualiza el estado de atributo predeterminado y los atributos que añadió se incorporan a la lista Atributos asignados del directorio.
- 7 Tras la creación del directorio, vaya a la página Almacenes de identidades y seleccione el directorio.
- 8 Haga clic en **Configuración de sincronización > Atributos asignados**.
- 9 En el menú desplegable de los atributos que haya añadido, seleccione el atributo de Active Directory al que realizar la asignación.
- 10 Haga clic en **Guardar**.

Resultados

El directorio se actualizará la próxima vez que se sincronice con Active Directory.

Añadir memoria a Administración de directorios

Es posible que necesite asignar más memoria a Directories Management si dispone de conexiones de Active Directory que contienen una gran cantidad de usuarios o grupos.

Se asignan de forma predeterminada 4 GB de memoria al servicio Directories Management. Esta cantidad es suficiente para un gran número de implementaciones de pequeño a mediano tamaño. Si cuenta con una conexión de Active Directory que utiliza un gran número de usuarios o grupos, es posible que necesite aumentar la asignación de memoria. El aumento de asignación de memoria es recomendable para sistemas de más de 100.000 usuarios, repartidos en 30 grupos para un total de 750 grupos. Para este tipo de sistema, VMware recomienda aumentar la asignación de memoria de Directories Management a 6 GB.

La memoria de Administración de directorios se calcula a partir de la memoria total asignada al dispositivo de vRealize Automation. En la siguiente tabla, se muestran las asignaciones de memoria para los respectivos componentes.

Tabla 2-5. Asignación de memoria del dispositivo de vRealize Automation

Memoria de dispositivos virtuales	Memoria del servicio vRA	Memoria del servicio vIDM
18 GB	3,3 GB	4 GB
24 GB	4,9 GB	6 GB
30 GB	7,4 GB	9,1 GB

Nota Estas asignaciones dan por hecho que todos los servicios predeterminados están habilitados y ejecutándose en el dispositivo virtual. Podrían cambiar en el caso de que se hayan detenido algunos servicios.

Requisitos previos

- Debe haberse configurado una conexión adecuada de Active Directory y estar operativa en su implementación de vRealize Automation.

Procedimiento

- 1 Detenga cada máquina en la que se ejecute un dispositivo de vRealize Automation.
- 2 Aumente la asignación de memoria del dispositivo virtual en cada máquina.
Si utiliza la asignación de memoria predeterminada de 18 GB, VMware recomienda aumentar la asignación de memoria a 24 GB.
- 3 Reinicie las máquinas con el dispositivo de vRealize Automation.

Crear un archivo de búsqueda de hosts de dominio que reemplace la búsqueda de la ubicación de servicio DNS (SRV)

Cuando habilite Autenticación de Windows integrada, la configuración del directorio cambiar para habilitar el campo de ubicación de servicio DNS. La búsqueda de la ubicación de servicio conector no se basa en el sitio. Si desea reemplazar la selección DC aleatoria, puede crear un archivo denominado `domain_krb.properties` y añadir el dominio para hospedar valores que tengan prioridad con respecto a la búsqueda SRV.

Procedimiento

- 1 Desde la línea de comandos `appliance-va`, inicie sesión como usuario con privilegios raíz.
- 2 Cambie los directorios a `/usr/local/horizon/conf` y cree un archivo llamado `domain_krb.properties`.
- 3 Edite el archivo `domain_krb.properties` para añadir la lista al dominio para hospedar valores. Añada la información como `<AD Domain>=<host:port>, <host2:port2>, <host2:port2>`.
Por ejemplo, especifique la lista como `example.com=examplehost.com:636, examplehost2.example.com:389`
- 4 Cambie la propiedad del archivo `domain_krb.properties` `horizon` y agrupe en `www`. Escriba `chown horizon:www /usr/local/horizon/conf/domain_krb.properties`.

5 Reinicie el servicio. Escriba **service horizon-workspace restart**.

Configurar el aprovisionamiento de usuarios de Just-in-Time

Puede configurar el aprovisionamiento de Just-in-Time (JIT) para que admita la inclusión de usuarios sin sincronización desde Active Directory.

Para admitir el aprovisionamiento de Just-in-Time, debe añadir un proveedor de identidades de terceros y, a continuación, configurar una conexión a él en la implementación de vRealize Automation para integrar la administración de directorios con otros proveedores de SSO a través de un protocolo SAML. Asimismo, debe crear un nuevo directorio con el nombre apropiado (por ejemplo, Directorio de JIT).

Al habilitar el aprovisionamiento de Just-in-Time, puede agregar usuarios de Just-in-Time a un grupo personalizado designado. Para admitir esta funcionalidad, cree un grupo personalizado con los miembros adecuados. Consulte [Agregar usuarios de Just-in-Time con reglas y grupos personalizados](#).

Nota Le recomendamos que no configure el aprovisionamiento de Just-in-Time en el tenant predeterminado vsphere.local.

Requisitos previos

Configure un proveedor de identidades de terceros adecuado para utilizarlo con el aprovisionamiento de JIT.

Procedimiento

- 1** Cree un proveedor de identidades para el aprovisionamiento de Just-in-Time.
 - a Seleccione **Administración > Administración de directorios > Proveedores de identidades**.
 - b Haga clic en **Añadir proveedor de identidades** y edite la configuración de la instancia del proveedor de identidades según corresponda.
 - Para el aprovisionamiento de Just-in-Time, cree un proveedor de identidades de terceros.
 - En la sección Crear directorio de Just-in-Time, escriba nombres para el directorio, así como uno o varios dominios.
 - Debe seleccionar una red para la configuración del proveedor de identidades de terceros.
 - Si utiliza una instancia externa de VMware Identity Manager como proveedor de identidades de terceros y emplea userPrincipalName para autenticar usuarios, debe cambiar la configuración de asignación de identificador de nombre para userPrincipalName del valor predeterminado de x509SubjectName a unspecified.

Consulte [Configurar una conexión de proveedor de identidades de terceros](#) para obtener más información sobre la creación de proveedores de identidades.

2 Configure SAML en el proveedor de identidades de Just-in-Time.

- a Copie los metadatos de IdP del proveedor de identidades.
- b En vRealize Automation, seleccione el proveedor de identidades y pegue los metadatos de IdP en el cuadro de texto **Metadatos del proveedor de identidades (URL o XML)**.
- c Haga clic en **Guardar**.
- d En el menú desplegable **Política de identificador de nombre en solicitud SAML (opcional)**, seleccione el formato adecuado.

Por ejemplo, si va a utilizar la dirección de correo electrónico como identificador de usuario único, debe seleccionar `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.
- e Seleccione el directorio adecuado bajo el encabezado Usuarios.
- f Seleccione las redes que utilizará este proveedor de identidades bajo el encabezado Red.
- g Especifique un nombre adecuado en el cuadro de texto **Métodos de autenticación**.
- h En el menú desplegable **Contexto de SAML**, seleccione `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`.
- i Haga clic con el botón secundario en el vínculo **Metadatos del proveedor de servicios (SP)** y ábralo en una pestaña nueva del navegador.
- j Use estos metadatos para configurar la conexión de SAML en el proveedor de identidades.

Si va a utilizar VMware Identity Manager, consulte la documentación de VMware Identity Manager para obtener todas las instrucciones sobre cómo configurar SAML.

3 Haga clic en **Agregar**.

Se crea el nuevo directorio con el nombre de directorio especificado.

4 Configure la política de acceso de vRealize Automation.

- a Seleccione **Administración > Políticas**.
- b Haga clic en el icono + de color verde situado en la parte superior derecha de la tabla de reglas de políticas.
- c Configure la regla de políticas para que se aplique a rangos y tipos de dispositivos correspondientes.
- d Seleccione el método de autenticación que creó al configurar el proveedor de identidades de terceros para el aprovisionamiento de JIT del método de autenticación.

Administrar atributos de usuario que se sincronizan desde Active Directory

En la página Atributos de usuario de la administración de directorios se muestran los atributos de usuario que se sincronizan con la conexión de Active Directory.

Los cambios que se realicen y se guarden en la página Atributos de usuario se añadirán a la página Atributos asignados en el directorio de Directories Management. Los cambios en los atributos se actualizan en el directorio durante la siguiente sincronización con Active Directory.

En la página Atributos de usuario, se muestran los atributos de directorio predeterminados que puede asignar a atributos de Active Directory. Seleccione los atributos que sean obligatorios, si bien también puede añadir otros atributos de Active Directory y sincronizarlos con el directorio.

Tabla 2-6. Atributos de Active Directory predeterminados para sincronizar con el directorio

Nombre del atributo de directorio	Asignación predeterminada al atributo de Active Directory
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
domain	canonicalName. Añade el nombre de dominio completo del objeto.
disabled (usuario externo deshabilitado)	userAccountControl. Marcado con UF_Account_Disable. Cuando se deshabilita una cuenta, los usuarios no pueden iniciar sesión en sus aplicaciones ni en sus recursos. Los recursos para los que los usuarios tienen autorización no se quitan de la cuenta para que, cuando se quite la marca de la cuenta, puedan iniciar sesión y acceder a los recursos autorizados.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName

En la página Atributos de usuario, se muestran los atributos de directorio predeterminados que puede asignar a atributos de Active Directory. Seleccione los atributos que sean obligatorios, si bien también puede añadir otros atributos de Active Directory y sincronizarlos con el directorio.

Tabla 2-7. Atributos de Active Directory predeterminados para sincronizar con el directorio

Nombre del atributo de directorio	Asignación predeterminada al atributo de Active Directory
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
domain	canonicalName. Añade el nombre de dominio completo del objeto.

Tabla 2-7. Atributos de Active Directory predeterminados para sincronizar con el directorio (continuación)

Nombre del atributo de directorio	Asignación predeterminada al atributo de Active Directory
disabled (usuario externo deshabilitado)	userAccountControl. Marcado con UF_Account_Disable. Cuando se deshabilita una cuenta, los usuarios no pueden iniciar sesión en sus aplicaciones ni en sus recursos. Los recursos para los que los usuarios tienen autorización no se quitan de la cuenta para que, cuando se quite la marca de la cuenta, puedan iniciar sesión y acceder a los recursos autorizados.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName

Administración de conectores y clústeres de conectores

En la página Conectores se muestran los conectores implementados de su red empresarial. Un conector sincroniza los datos de grupo y usuario entre Active Directory y el servicio de administración de directorios y, cuando se utiliza como el proveedor de identidades, autentica a los usuarios para su acceso al servicio.

En vRealize Automation, cada Dispositivo de vRealize Automation contiene su propio conector; estos conectores son adecuados para la mayoría de las implementaciones.

Cuando se asocia un directorio con una instancia de conectores, el conector crea una partición para el directorio asociado llamada trabajo. Una instancia de conector puede tener varios trabajos asociados. Cada trabajo actúa como proveedor de identidades. El conector sincroniza datos de usuarios y de grupos entre Active Directory y el servicio a través de uno o varios trabajos. Los métodos de autenticación se definen y configuran en cada trabajo.

Desde la página Conectores puede administrar diversos aspectos de un vínculo de Active Directory. Esta página contiene una tabla y varios botones que le permiten completar diversas tareas administrativas.

- En la columna Trabajo, seleccione un trabajo para ver los detalles del conector y vaya a la página de autenticación de adaptadores para ver el estado de los métodos de autenticación disponibles. Para obtener información sobre la configuración, consulte [Integrar productos de autenticación de usuario alternativos con Administración de directorios](#).
- En la columna proveedor de identidades, seleccione el IdP que desea ver, editar o desactivar. Consulte [Configurar una conexión de proveedor de identidades de terceros](#).
- En la columna Directorio asociado, acceda al directorio asociado a este trabajo.

- Haga clic en **Unirse a un dominio** para unir el conector a un dominio específico de Active Directory. Por ejemplo, al configurar la autenticación Kerberos, debe unirse al dominio Active Directory que contenga usuarios o al que tenga relación de confianza con los dominios que contengan usuarios.
- Al configurar un directorio con un Active Directory de autenticación de Windows integrada, el conector se une al dominio de acuerdo con los detalles de configuración.

Conectores en un entorno de clústeres

En una implementación distribuida de vRealize Automation, todos los conectores que hay disponibles realizan cualquier autorización de usuario necesaria, mientras que un solo conector designado gestiona toda la sincronización de configuración. Por lo general, la sincronización incluye adiciones, eliminaciones o cambios en la configuración de usuario y se realiza automáticamente siempre y cuando todos los conectores estén disponibles. Existen algunas situaciones específicas en las que no puede producirse la sincronización automática.

Para los cambios relacionados con la configuración de directorios, por ejemplo, el dn de base, vRealize Automation intenta transmitir las actualizaciones automáticamente a todos los conectores en un clúster. Si no se puede acceder a un conector o este deja de funcionar por algún motivo, dicho conector no recibirá la actualización, incluso cuando se reanude la operación en línea. Para implementar los cambios de configuración en los conectores que no los hayan recibido automáticamente, los administradores del sistema deben guardar manualmente los cambios en todos los conectores aplicables.

Para los cambios relacionados con el perfil de sincronización de directorios, vRealize Automation también intenta transmitir automáticamente las actualizaciones a todos los conectores. Si el conector de sincronización funciona, la actualización se guarda y se transmite a todos los conectores de autorización disponibles. Si no se puede acceder a uno o más conectores, el administrador del sistema recibe una advertencia que indica que no todos los conectores se actualizaron. Si el conector de sincronización no funciona, la actualización falla y se produce un error. Si el administrador del sistema cambia el conector que se ha designado como conector de sincronización, el nuevo conector de sincronización recibe la información de perfil disponible más reciente, y esta información se transmite a todos los conectores aplicables y disponibles.

Unir una máquina de conector a un dominio

En algunos casos, puede que deba unir una máquina que contenga un conector de administración de directorios a un dominio.

En el caso de directorios de Active Directory mediante LDAP, puede unirse a un dominio tras crear el directorio. En el caso de directorios Active Directory (autenticación integrada de Windows), el conector se unirá al dominio de forma automática cuando se cree el directorio. En ambos casos, deberá introducir las credenciales correspondientes.

Para unirse a un domino, necesita credenciales de Active Directory con el privilegio para unir equipos a dominios de AD. Esto se configura en Active Directory con los siguientes derechos:

- Crear objetos de equipo

■ Eliminar objetos de equipo

Cuando se une a un dominio, se crea un objeto de equipo en la ubicación predeterminada de Active Directory.

Si no tiene derechos para unirse a un dominio, o si la política de la empresa requiere una ubicación personalizada para el objeto de equipo, debe pedir al administrador que cree el objeto y, a continuación, unir la máquina de conector al dominio.

Procedimiento

- 1 Pida a su administrador de Active Directory que cree el objeto de equipo en Active Directory, en una ubicación determinada por la política de la empresa. Debe proporcionar el nombre de host del conector. Asegúrese de que proporciona el nombre de dominio completo; por ejemplo, `servidor.ejemplo.com`.

Encontrará el nombre de host en la columna Nombre de host de la página Conectores de la consola de administración. Seleccione **Administración > Administración de directorios > Conectores**.

- 2 Tras la creación del objeto de equipo, haga clic en **Unirse al dominio** en la página Conectores para unirse al dominio con cualquier cuenta de usuario de dominio disponible en la administración de directorios.

Acerca de la selección de controladoras de dominio

El archivo `domain_krb.properties` determina las controladoras de dominio que se usan para los directorios en los que se ha habilitado la búsqueda de ubicaciones del servicio DNS (registros SRV). Contiene una lista de las controladoras de dominio de cada dominio. El conector crea el archivo inicialmente, pero es su responsabilidad mantenerlo. El archivo reemplaza la búsqueda de ubicaciones del servicio DNS (SRV).

La búsqueda de ubicaciones del servicio DNS está habilitada en los siguientes tipos de directorios.

- Active Directory mediante LDAP con la opción **Este directorio es compatible con las ubicaciones del servicio DNS** seleccionada
- Active Directory (autenticación integrada de Windows), donde la búsqueda de ubicaciones del servicio DNS siempre está habilitada.

Cuando se crea un directorio con la búsqueda de ubicaciones del servicio DNS habilitada por primera vez, se crea un archivo `domain_krb.properties` de forma automática en el directorio `/usr/local/horizon/conf` de la máquina virtual y se rellena automáticamente con las controladoras de dominio de cada dominio. Para rellenar el archivo, el conector intenta encontrar controladoras de dominio que se encuentren en el mismo sitio que el conector y selecciona los dos a los que se puede acceder que respondan con más rapidez.

Cuando se crean directorios adicionales con la búsqueda de ubicaciones del servicio DNS habilitada, o cuando se añaden nuevos dominios a un directorio de autenticación integrada de Windows, los nuevos dominios se añaden al archivo junto con una lista de controladoras de dominio para estos.

Puede editar el archivo `domain_krb.properties` reemplazar la selección predeterminada cuando lo desee. Tras crear un directorio, se recomienda abrir el archivo `domain_krb.properties` y comprobar que las controladoras de dominio enumeradas son óptimas para la configuración. Para una implementación global de Active Directory que contiene varias controladoras de dominio en diferentes ubicaciones geográficas, el uso de una controladora de dominio cercana al conector es la mejor forma de asegurar una comunicación rápida con Active Directory.

También debe actualizar el archivo de forma manual para realizar otros cambios. Se aplican las siguientes reglas.

- El archivo `domain_krb.properties` se crea en la máquina virtual que contiene el conector. En una implementación típica, sin conectores adicionales implementados, el archivo se crea en la máquina virtual del servicio de Directories Management. Si usa un conector adicional para el directorio, el archivo se crea en la máquina virtual del conector. Una máquina virtual solo puede contener un archivo `domain_krb.properties`.
- El archivo se crea y se rellena de forma automática con las controladoras de dominio de cada dominio cuando se crea por primera vez un directorio con la búsqueda de ubicaciones del servicio DNS habilitada.
- Las controladoras de dominio de cada dominio se enumeran en orden de prioridad. Para conectarse a Active Directory, el conector probará la primera controladora de dominio de la lista. Si no puede acceder a ella, probará con la segunda de la lista, y así sucesivamente.
- El archivo solo se actualiza cuando se crea un nuevo directorio con la búsqueda de ubicaciones del servicio DNS habilitada o cuando se añade un dominio a un directorio de autenticación integrada de Windows. El dominio nuevo y una lista de controladoras de dominio para este se añaden al archivo.

Tenga en cuenta que, si ya existe una entrada de dominio en el archivo, este no se actualizará. Por ejemplo, si ha creado un directorio y lo ha eliminado posteriormente, la entrada de dominio original permanecerá en el archivo y no se actualizará.

- El archivo no se actualizará automáticamente en ningún otro caso. Por ejemplo, si elimina un directorio, la entrada de dominio no se eliminará del archivo.
- Si no se puede acceder a una controladora de dominio enumerada en el archivo, edite el archivo y elimínela.
- Si añade o edita una entrada de dominio de forma manual, los cambios no se sobrescribirán.

Seleccionar las controladoras de dominio para rellenar de forma automática el archivo `domain_krb.properties`

Para rellenar de forma automática el archivo `domain_krb.properties`, las controladoras de dominio se seleccionan determinando primero la subred en la que se encuentra el conector (en función de la dirección IP y la máscara de red), y después usando la configuración de Active Directory para identificar el sitio de dicha subred a fin de obtener la lista de controladoras de dominio del sitio, filtrando la lista para el dominio apropiado y eligiendo las dos controladoras de dominio que respondan más rápido.

Para detectar las controladoras de dominio más cercanas, VMware Identity Manager requiere lo siguiente:

- La subred del conector debe estar presente en la configuración de Active Directory, o se debe especificar una subred en el archivo `runtime-config.properties`.

La subred se usa para determinar el sitio.

- La configuración de Active Directory debe reconocer el sitio.

Si no se puede determinar la subred, o si la configuración de Active Directory no reconoce el sitio, la búsqueda de ubicaciones del servicio DNS se usará para buscar controladoras de dominio y el archivo se rellenará con algunas controladoras de dominio a las que se pueda acceder. Tenga en cuenta que puede que dichas controladoras de dominio no se encuentren en la misma ubicación geográfica que el conector, lo que podría causar retrasos o que se agote el tiempo de espera durante la comunicación con Active Directory. En este caso, edite el archivo `domain_krb.properties` de forma manual y especifique las controladoras de dominio correctas que se deben usar para cada dominio.

Archivo `domain_krb.properties` de muestra

```
example.com=host1.example.com:389,host2.example.com:389
```

- [Reemplazar la selección de subred predeterminada](#)

Para rellenar automáticamente el archivo `domain_krb.properties`, el conector intenta buscar controladoras de dominio que se encuentren en el mismo sitio para que la latencia entre el conector y Active Directory sea mínima.

- [Editar el archivo `domain_krb.properties`](#)

El archivo `/usr/local/horizon/conf/domain_krb.properties` determina las controladoras de dominio que se usarán para los directorios donde se ha habilitado la búsqueda de ubicaciones del servicio DNS. Puede editar el archivo cuando lo desee para modificar la lista de controladoras de dominio de un dominio, o para añadir o eliminar entradas de dominio. Los cambios no se reemplazarán.

- [Solución de problemas de `domain_krb.properties`](#)

Use esta información para solucionar problemas en el archivo `domain_krb.properties`.

Reemplazar la selección de subred predeterminada

Para rellenar automáticamente el archivo `domain_krb.properties`, el conector intenta buscar controladoras de dominio que se encuentren en el mismo sitio para que la latencia entre el conector y Active Directory sea mínima.

Para buscar el sitio, el conector determina la subred donde este se encuentra, en función de su dirección IP y su máscara de red; a continuación, usa la configuración de Active Directory para identificar el sitio de dicha subred. Si la subred de la máquina virtual no está en Active Directory, o si desea reemplazar la selección de subred automática, puede especificar una subred en el archivo `runtime-config.properties`.

Procedimiento

- 1 Inicie sesión en la máquina virtual del de Directories Management como usuario raíz.

Nota Si usa un conector adicional para el directorio, inicie sesión en la máquina virtual del conector.

- 2 Edite el archivo `/usr/local/horizon/conf/runtime-config.properties` y añada el siguiente atributo.

`siteaware.subnet.override=subnet`

donde *subnet* es una subred del sitio cuyas controladoras de dominio desea usar. Por ejemplo:

`siteaware.subnet.override=10.100.0.0/20`

- 3 Guarde y cierre el archivo.

- 4 Reinicie el servicio.

```
service horizon-workspace restart
```

Editar el archivo `domain_krb.properties`

El archivo `/usr/local/horizon/conf/domain_krb.properties` determina las controladoras de dominio que se usarán para los directorios donde se ha habilitado la búsqueda de ubicaciones del servicio DNS. Puede editar el archivo cuando lo desee para modificar la lista de controladoras de dominio de un dominio, o para añadir o eliminar entradas de dominio. Los cambios no se reemplazarán.

El conector crea y rellena automáticamente el archivo inicialmente. Deberá actualizarlo de forma manual en algunos casos.

- Si las controladoras de dominio seleccionados de forma predeterminada no son óptimos para la configuración, edite el archivo y especifique las controladoras de dominio que se usarán.
- Si elimina un directorio, elimine la entrada de dominio correspondiente del archivo.
- Si no se puede acceder a alguna controladora de dominio del archivo, elimínelo del archivo.

Consulte también [Acerca de la selección de controladoras de dominio](#).

Procedimiento

- 1 Inicie sesión en la máquina virtual del de Directories Management como usuario raíz.

Nota Si usa un conector adicional para el directorio, inicie sesión en la máquina virtual del conector.

- 2 Cambie los directorios por `/usr/local/horizon/conf`.
- 3 Edite el archivo `domain_krb.properties` para añadir o editar la lista de valores de dominio a host.

Use el siguiente formato:

domain=host:port,host2:port,host3:port

Por ejemplo, .

`example.com=examplehost1.example.com:389,examplehost2.example.com:389`

Enumere las controladoras de dominio en orden de prioridad. Para conectarse a Active Directory, el conector probará la primera controladora de dominio de la lista. Si no puede acceder a ella, probará con la segunda de la lista, y así sucesivamente.

Importante Los nombres de los dominios deben estar en minúscula.

- 4 Cambie el propietario del archivo `domain_krb.properties` a `horizon` y el grupo a `www` mediante el siguiente comando:

`chown horizon:www /usr/local/horizon/conf/domain_krb.properties`

- 5 Reinicie el servicio.

`service horizon-workspace restart`

Solución de problemas de domain_krb.properties

Use esta información para solucionar problemas en el archivo `domain_krb.properties`.

Error "Error al resolver dominio"

Si el archivo `domain_krb.properties` ya incluye una entrada para un dominio, e intenta crear un nuevo directorio de otro tipo para el mismo dominio, se producirá un error con el mensaje "Error al resolver dominio". Debe editar el archivo `domain_krb.properties` y eliminar de forma manual la entrada de domino antes de crear el nuevo directorio.

No se puede acceder a las controladoras del dominio.

Cuando se añade una entrada de dominio al archivo `domain_krb.properties`, no se actualiza automáticamente. Si no se puede acceder a una controladora de dominio enumerado en el archivo, edite el archivo de forma manual y elimínelo.

Administrar políticas de acceso

Las políticas de Directories Management son un conjunto de reglas que especifican criterios que deben reunirse para que los usuarios accedan a su portal de aplicaciones o lancen aplicaciones web específicas.

La regla se crea como parte de la política. Toda regla en una política puede especificar la siguiente información.

- El rango de redes, desde donde los usuarios pueden iniciar sesión, como, por ejemplo, dentro o fuera de la red empresarial.
- El tipo de dispositivo al que puede acceder a través de esta política.
- El orden que se aplica a los métodos de autenticación habilitados.
- El número de horas que es válida la autenticación.
- Personalizar el mensaje de acceso denegado.

Nota Las políticas no controlan el tiempo que dura una sesión de aplicación web. Controlan el tiempo de que disponen los usuarios para lanzar una aplicación web.

El servicio de Directories Management incluye una política predeterminada que puede editar. Esta política controla el acceso al servicio en su conjunto. Consulte [Aplicar la política de acceso predeterminada](#). Para controlar el acceso a aplicaciones web específicas, podrá crear políticas adicionales. Si no aplica ninguna política a la aplicación web, se aplicará la política predeterminada.

Configurar la política de acceso

Una política contiene una o más reglas de acceso. Cada regla consta de configuraciones que se pueden ajustar para administrar el acceso de los usuarios a los portales de la aplicación en su totalidad o a aplicaciones web específicas.

Rango de redes

Para cada regla, determine la base de usuarios especificando un rango de redes. Un rango de redes está compuesto por uno o varios rangos de IP. Los rangos de redes se crean en la pestaña Administración de acceso e identidades, Configuración > página Rangos de redes antes de configurarse los conjuntos de políticas de acceso.

Tipo de dispositivo

Seleccione el tipo de dispositivo que administra la regla. Los tipos de cliente son Navegador web, Aplicación cliente de Identity Manager, iOS, Android y Todos los tipos de dispositivos.

Métodos de autenticación

Establezca la prioridad de los métodos de autenticación para la regla de política. Los métodos de autenticación se aplican en el orden en que se muestran. Se selecciona la primera instancia de proveedor de identidades que cumple la configuración de método de autenticación y rango de redes de la política y se reenvía la solicitud de autenticación de usuario a la instancia de proveedor de identidades para su autenticación. En caso de error de autenticación, se selecciona el siguiente método de autenticación de la lista. Si se usa la autenticación de certificado, este método debe ser el primero en la lista.

Puede configurar reglas de política de acceso que requieran que los usuarios pasen credenciales mediante dos métodos de autenticación para poder iniciar sesión. Si uno o ambos métodos de autenticación generan errores y también hay configurados métodos de reserva, se solicita a los usuarios que proporcionen sus credenciales para los siguientes métodos de autenticación que estén configurados. En los dos siguientes escenarios, se describe cómo funcionan las cadenas de autenticación.

- En el primer escenario, se configura la regla de política de acceso para que requiera que los usuarios se autenticuen con su contraseña y con la credencial de Kerberos. Se ha configurado la autenticación de reserva para que solicite la contraseña y la credencial de RADIUS para la autenticación. Un usuario escribe la contraseña correctamente, pero no proporciona la credencial de autenticación Kerberos correcta. Como el usuario escribió la contraseña correcta, la solicitud de autenticación de reserva corresponde solo a la credencial de RADIUS. No es necesario que el usuario vuelva a escribir la contraseña.
- En el segundo escenario, se configura la regla de política de acceso para que requiera que los usuarios se autenticuen con su contraseña y con la credencial de Kerberos. Se ha configurado la autenticación de reserva para que solicite RSA SecurID y una credencial de RADIUS para la autenticación. Un usuario escribe la contraseña correctamente, pero no proporciona la credencial de autenticación Kerberos correcta. La solicitud de autenticación de reserva es tanto para la credencial de RSA SecurID como para la de RADIUS.

Duración de la sesión de autenticación

Para cada regla, establezca la duración de la validez de esta autenticación. Este valor determina la cantidad máxima de tiempo de la que los usuarios disponen desde el último evento de autenticación para obtener acceso a su portal o iniciar una aplicación web concreta. Por ejemplo, el valor 4 en una regla de aplicación web proporciona a los usuarios cuatro horas para iniciar la aplicación web, a menos que inicien otro evento de autenticación que prolongue la duración.

Mensaje de error personalizado de acceso denegado

Cuando los usuarios intentan iniciar sesión y se produce un error porque las credenciales no son válidas, la configuración no es correcta o se produce un error en el sistema, se mostrará un mensaje de acceso denegado. El mensaje predeterminado es

Se ha denegado el acceso, ya que no se han encontrado métodos de autenticación válidos.

Puede crear un mensaje de error personalizado para cada regla de la directiva de acceso para anular el mensaje predeterminado. El mensaje personalizado puede incluir texto y un vínculo de un mensaje de llamada a la acción. Por ejemplo, en las reglas de una política para dispositivos móviles que desea administrar, si un usuario intenta iniciar sesión desde un dispositivo que no esté inscrito, podría aparecer el siguiente mensaje de error personalizado:

Inscriba su dispositivo para acceder a los recursos corporativos, para ello, haga clic en el vínculo que encontrará al final de este mensaje. Si su dispositivo ya está registrado, póngase en contacto con el equipo de soporte técnico para obtener ayuda.

Ejemplo de política predeterminada

La siguiente política sirve de ejemplo de cómo puede configurar la política predeterminada para controlar el acceso al portal de aplicaciones. Consulte [Administrar la política de acceso de usuarios](#).

Las reglas de política se evalúan en el orden en que se muestran. Para cambiar el orden de la política, arrástrela y colóquela en la sección Reglas de política.

En el siguiente caso de uso, este ejemplo de política se aplica a todas las aplicaciones.

DIRECTIVA PREDETERMINADA

* Nombre de directiva: default_access_policy_set

Descripción: Default access policy set

Se aplica a: Todas las aplicaciones

Reglas de la directiva

Puede crear una lista de reglas para acceder a estas aplicaciones web. Para cada regla, seleccione el rango de redes IP, los tipos de dispositivos que pueden acceder a las aplicaciones, los métodos y el orden de autenticación y el número máximo de horas que los usuarios pueden usar la aplicación sin tener que realizar la autenticación de nuevo.

Rango de redes	Tipo de dispositivo	Método de autenticación	Nueva autenticación	
TODOS LOS INTERVALOS	Navegador web	Password	8 Hora(s)	✗ +
TODOS LOS INTERVALOS	Aplicación cliente de Identity Manager	Password	2160 Hora(s)	✗ +

Guardar Cancelar

- Para la red interna (Rango de redes internas), se configuran dos métodos de autenticación para la regla: Kerberos y la autenticación con contraseña como método de reserva. Para acceder al portal de aplicaciones desde una red interna, el servicio intenta autenticar a los usuarios en primer lugar con autenticación Kerberos, ya que es el primer método de autenticación mostrado en la regla. Si esto genera un error, se solicita a los usuarios que escriban la contraseña de Active Directory. Los usuarios inician sesión en un navegador y ahora tienen acceso a su portal de aplicaciones durante una sesión de ocho horas.
 - Para el acceso desde la red externa (Todos los rangos), solamente se configura un método de autenticación, RSA SecurID. Para acceder al portal de aplicaciones desde una red externa, es necesario que los usuarios inicien sesión con SecurID. Los usuarios inician sesión en un navegador y ahora tienen acceso a su portal de aplicaciones durante una sesión de cuatro horas.

- 2 Cuando un usuario intenta acceder a un recurso, excepto las aplicaciones web cubiertas por una política específica para aplicaciones web, se aplica la política predeterminada de acceso al portal.

Por ejemplo, el tiempo de reautenticación para estos recursos coincide con el de la regla de la política de acceso predeterminada. Si el tiempo para un usuario que inicia sesión en el portal de aplicaciones es ocho horas según la regla de la política de acceso predeterminada, cuando intente iniciar un recurso durante la sesión, se inicia la aplicación sin necesidad de que se reautentique.

Administrar políticas específicas de aplicaciones web

Cuando añade aplicaciones web al catálogo, puede crear políticas de acceso específicas de aplicaciones web. Por ejemplo, puede crear una política con reglas para una aplicación web que especifique qué direcciones IP tienen acceso a la aplicación, con qué métodos de autenticación y durante cuánto tiempo hasta que sea necesaria la reautenticación.

La siguiente política específica de aplicaciones web proporciona un ejemplo de política que puede crear para controlar el acceso a aplicaciones web especificadas.

Ejemplo 1 Política estricta específica de aplicaciones web

En este ejemplo, se crea una nueva política y se aplica a una aplicación web confidencial.

Sensitive Web Application
To be applied to Web application that should have limited access.

Nombre de directiva* Sensitive Web Application

Descripción To be applied to Web application that should have limited access.

Se aplica a Seleccione las aplicaciones de su Catálogo a las que se le aplique esta directiva.
AirWatch
Content Locker
[Editar aplicaciones]

Reglas de la directiva
Puede crear una lista de reglas para acceder a estas aplicaciones. Para cada regla, seleccione el rango de redes IP, el tipo de dispositivos que pueden acceder a las aplicaciones, los métodos y el orden de autenticación, así como el número máximo de horas que los usuarios pueden utilizar la aplicación antes de volver a realizar la autenticación.

Rango de redes	Tipo de dispositivo	Método de auten...	Nueva autentic...	Grupos	
Internal Network	Navegador web	En primer lugar, pruebe: Kerberos y 1 reserva(s) más...	8 hora(s)	Todos los usuarios	✗ +
TODOS LOS RANGOS	Navegador web	SecurID	4 hora(s)	Todos los usuarios	✗ +

[Guardar] [Cancelar]

- 1 Para acceder al servicio desde fuera de la red empresarial, es necesario que el usuario inicie sesión con RSA SecurID. El usuario inicia sesión en un navegador y ahora tiene acceso al portal de aplicaciones durante una sesión de cuatro horas, como indica la regla de acceso predeterminada.
- 2 Una vez transcurridas las cuatro horas, el usuario trata de iniciar una aplicación web con el conjunto de políticas de aplicaciones web aplicadas.

- 3 El servicio comprueba las reglas de la política y la aplica con el rango de redes TODOS LOS RANGOS dado que la solicitud del usuario procede de un navegador web y del rango de redes TODOS LOS RANGOS.

El usuario inicia sesión con el método de autenticación RSA SecurID, pero la sesión acaba de caducar. Se redirige al usuario para que haya reautenticación. La reautenticación proporciona al usuario otra sesión de cuatro horas y la posibilidad de iniciar la aplicación. Durante las próximas cuatro horas, el usuario puede continuar iniciando la aplicación sin necesidad de reautenticarse.

Ejemplo 2 Política más estricta específica de aplicaciones web

Para aplicar una regla más estricta en aplicaciones web extra confidenciales, transcurrida una hora podría ser necesaria la reautenticación con SecureID en cualquier dispositivo. El siguiente es un ejemplo de cómo se implementa este tipo de regla de acceso de la política.

- 1 El usuario inicia sesión desde dentro de la red empresarial con el método de autenticación de contraseñas.
Ahora el usuario tiene acceso al portal de aplicaciones durante ocho horas, como se indica en el Ejemplo 1.
- 2 El usuario trata de iniciar una aplicación web inmediatamente con la regla de política del Ejemplo 2 aplicada, que requiere autenticación RSA SecurID.
- 3 El usuario es redirigido a un proveedor de identidades que ofrece autenticación RSA SecurID.
- 4 Tras haber iniciado el usuario la sesión correctamente, el servicio inicia la aplicación y guarda el evento de autenticación.

El usuario puede seguir iniciando esta aplicación durante una hora, pero transcurrido este tiempo se le solicita la reautenticación, ta y como dicta la regla de política.

Administrar la política de acceso de usuarios

vRealize Automation se proporciona con una política de acceso de usuarios predeterminada que puede utilizar tal cual o bien editarla de la forma necesaria para administrar el acceso de los tenants a las aplicaciones.

vRealize Automation se proporciona con una política de acceso de usuarios predeterminada, aunque puede añadir otras políticas nuevas. Puede editar la política existente para añadirle reglas.

Requisitos previos

- Seleccione o configure los proveedores de identidades apropiados para su implementación. Consulte [Configurar una conexión de proveedor de identidades de terceros](#).
- Configure los rangos de redes apropiados para su implementación. Consulte [Añadir o editar un rango de redes](#).

- Configure los métodos de autenticación apropiados para su implementación. Consulte [Integrar productos de autenticación de usuario alternativos con Administración de directorios](#).
- Si tiene previsto editar la política predeterminada (para controlar el acceso de usuarios al servicio de manera global), configúrela antes de crear la política específica de la aplicación web.
- Añada aplicaciones web al catálogo. Las aplicaciones web deben aparecer enumeradas en la página Catálogo para poder añadir una política.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Políticas**.
- 2 Haga clic en **Editar política** para añadir una nueva política.
- 3 Añada un nombre y una descripción a la política en los cuadros de texto correspondientes.
- 4 En la sección Se aplica a, haga clic en **Seleccionar** y, en la página que aparece, seleccione las aplicaciones web que se asociarán con esta política.
- 5 En la sección Reglas de políticas, haga clic en **+** para añadir una regla.
Aparece la página Añadir una regla de política.
 - a Seleccione el rango de redes que se aplicará a esta regla.
 - b Seleccione el tipo de dispositivo que podrá acceder a las aplicaciones web de esta regla.
 - c Seleccione los métodos de autenticación que se utilizarán en el orden en que deberán aplicarse.
 - d Especifique el número de horas que permanecerá abierta la sesión de la aplicación web.
 - e Haga clic en **Guardar**.
- 6 Configure otras reglas según crea conveniente.
- 7 Haga clic en **Guardar**.

Configuración de conexiones del proveedor de identidades adicionales

Puede configurar más conexiones del proveedor de identidades según sea necesario para admitir distintos escenarios de administración de identidades, incluidos proveedores de identidades de terceros y proveedores de identidades integrados adicionales.

Puede crear tres tipos de conexiones del proveedor de identidades mediante la administración de directorios.

- Crear IDP de terceros: utilice este elemento para crear una conexión a un proveedor de identidades de terceros externo. Asegúrese de tener lo siguiente antes de añadir una instancia del proveedor de identidades de terceros.
 - Compruebe que las instancias externas cumplen con SAML 2.0 y que el servicio puede acceder a la instancia externa.
 - Obtenga la información de metadatos externa adecuada para añadir cuando configure el proveedor de identidades en la consola de administración. La información de metadatos que obtenga de la instancia externa será la URL a los metadatos o los metadatos reales.
- Crear IDP de Workspace: cuando se habilita un conector para autenticar a los usuarios durante la configuración de la administración de directorios, se crea un IDP de Workspace como proveedor de identidades y se habilita la autenticación de contraseñas. Puede configurar otros proveedores de identidades de Workspace adicionales detrás de distintos equilibradores de carga.
- Crear IDP integrado: los proveedores de identidades integrados usan los mecanismos de administración de directorios internos para admitir la autenticación. Puede configurar proveedores de identidades integrados para usar los métodos de autenticación que no requieren el uso de un conector en las instalaciones. Cuando configure el proveedor integrado, asocie los métodos de autenticación que desea utilizar con el proveedor.
- [Configurar una conexión de proveedor de identidades de terceros](#)
vRealize Automation se proporciona con una instancia de conexión de proveedor de identidades predeterminada. Es posible que los usuarios deseen crear conexiones de proveedor de identidades adicionales para admitir el aprovisionamiento de usuarios de Just-in-Time u otras configuraciones personalizadas.
- [Configurar más proveedores de identidades de Workspace](#)
Cuando se configura un conector de la administración de directorios para autenticar usuarios, se crea un IDP de Workspace y se habilita la autenticación de contraseña.
- [Configurar una conexión del proveedor de identidades integrado](#)
Puede configurar varios proveedores de identidades integrados y asociar con ellos métodos de autenticación.

Configurar una conexión de proveedor de identidades de terceros

vRealize Automation se proporciona con una instancia de conexión de proveedor de identidades predeterminada. Es posible que los usuarios deseen crear conexiones de proveedor de identidades adicionales para admitir el aprovisionamiento de usuarios de Just-in-Time u otras configuraciones personalizadas.

vRealize Automation se proporciona con un proveedor de identidades predeterminado. En la mayoría de los casos, el proveedor predeterminado cumple con las necesidades del cliente. No obstante, si utiliza una solución de administración de identidades empresarial existente, puede configurar un proveedor de identidades personalizado para redirigir a los usuarios a su solución de identidades existente.

Cuando se utiliza un proveedor de identidades personalizado, la administración de directorios utiliza los metadatos de SAML de ese proveedor para establecer una relación de confianza con el proveedor. Una vez establecida esta relación, la administración de directorios asigna los usuarios de la aserción de SAML a la lista de usuarios internos de vRealize Automation según el identificador del nombre de asunto.

Requisitos previos

- Configure los rangos de redes que desea dirigir hacia esta instancia del proveedor de identidades para la autenticación. Consulte [Añadir o editar un rango de redes](#).
- Acceda al documento de metadatos de terceros. Puede ser la dirección URL de los metadatos o los propios metadatos.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Proveedores de identidades**.

En esta página se muestran los distintos proveedores de identidades configurados.

- 2 Haga clic en **Añadir proveedor de identidades**.

Aparecerá un menú con las opciones del proveedor de identidades.

- 3 Seleccione **Crear IDP de terceros**.

- 4 Introduzca la información apropiada para configurar el proveedor de identidades.

Opción	Descripción
Nombre de proveedor de identidades	Escriba un nombre para la instancia del proveedor de identidades.
Metadatos de SAML	<p>Añada el documento de metadatos basado en XML de IDP de terceros para establecer una relación de confianza con el proveedor de identidades.</p> <ol style="list-style-type: none"> 1 Escriba la dirección URL de los metadatos de SAML o bien el contenido xml en el cuadro de texto. 2 Haga clic en Procesar metadatos de IDP. Los formatos de ID de nombre compatibles con el IDP se extraen de los metadatos y se añaden a la tabla Formato de ID de nombre. 3 En la columna de valor de ID de nombre, seleccione el atributo de usuario del servicio para asignarlo a los formatos de ID que aparecen. Puede añadir formatos de ID de nombre personalizados de terceros y asignarlos a los valores de atributos de usuario del servicio. 4 (Opcional) Seleccione el formato de cadena de identificador de respuesta NameIDPolicy.

Opción	Descripción
Usuarios	Seleccione los directorios de Directories Management de los usuarios que pueden autenticarse con este proveedor de identidades.
Aprovisionamiento de usuarios de Just-in-Time	<p>Seleccione las opciones adecuadas para admitir el aprovisionamiento de Just-in-Time mediante un proveedor de identidades de terceros apropiado.</p> <p>En Nombre de directorio, introduzca el nombre de directorio que se utilizará para el aprovisionamiento de Just-in-Time.</p> <p>En Dominios, especifique uno o varios dominios que existan en el proveedor de identidades externo que se va a utilizar para el aprovisionamiento de Just-in-Time.</p>
Red	<p>Incluye una lista de los rangos de redes existentes configurados en el servicio.</p> <p>Seleccione los rangos de redes para los usuarios, basados en sus direcciones IP, que desea dirigir hacia la instancia en cuestión del proveedor de identidades para la autenticación.</p>
Métodos de autenticación	<p>Añada los métodos de autenticación que admite el proveedor de identidades de terceros.</p> <p>Seleccione la clase de contexto de autenticación de SAML compatible con el método de autenticación.</p>
Certificado de firma de SAML	Haga clic en Metadatos del proveedor de servicios (SP) para ver la dirección URL de los metadatos del proveedor de servicios de SAML de Directories Management. Copie la dirección URL y guárdela. Esta dirección URL se configura al editar la aserción de SAML en el proveedor de identidades de terceros para asignar usuarios de Directories Management.
Nombre de host	Si aparece el campo Hostname , escriba el nombre de host al que será redirigido el proveedor de identidades para la autenticación. Si utiliza un puerto no estándar distinto del 443, puede definirlo con el formato Nombredehost:Puerto. Por ejemplo, miemp.ejemplo.com:8443.

5 Haga clic en **Agregar**.

Pasos siguientes

- Copie y guarde los metadatos del proveedor de servicios de Directories Management necesarios para configurar la instancia del proveedor de identidades de terceros. Estos metadatos están disponibles en la sección Certificado de firma de SAML de la página Proveedor de identidades.
- Añada el método de autenticación del proveedor de identidades a la política predeterminada de servicios.

Consulte la guía de *Configuración de recursos en Directories Management* para obtener información sobre cómo añadir y personalizar los recursos que añade al catálogo.

Configurar más proveedores de identidades de Workspace

Cuando se configura un conector de la administración de directorios para autenticar usuarios, se crea un IDP de Workspace y se habilita la autenticación de contraseña.

Puede configurar otros conectores para que operen detrás de varios equilibradores de carga. Si la implementación incluye más de un equilibrador de carga, se pueden configurar más proveedores de identidades de Workspace para la autenticación en cada configuración de equilibrio de carga.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Proveedores de identidades**.

En esta página se muestran los distintos proveedores de identidades configurados.

- 2 Haga clic en **Añadir proveedor de identidades**.

Aparecerá un menú con las opciones del proveedor de identidades.

- 3 Seleccione **Crear IDP de Workspace**.

- 4 Introduzca la información apropiada para configurar el proveedor de identidades.

Opción	Descripción
Nombre de proveedor de identidades	Introduzca el nombre de esta instancia del proveedor de identidades integrado.
Usuarios	Seleccione los usuarios que se van a autenticar. Los directorios configurados aparecen en la lista.
Usuarios	Seleccione el grupo de usuarios que pueden autenticarse con este proveedor de identidades de Workspace.
Red	Incluye una lista de los rangos de redes existentes configurados en el servicio. Seleccione el rango de redes para los usuarios en función de las direcciones IP que desea dirigir a esta instancia del proveedor de identidades para la autenticación.
Métodos de autenticación	Se muestran los métodos de autenticación que están configurados para el servicio. Seleccione la casilla de verificación de los métodos de autenticación para asociarlos con este proveedor de identidades. De conformidad con el dispositivo y la contraseña, con AirWatch y AirWatch Connector, asegúrese de que está habilitada la opción en la página de configuración de AirWatch.

- 5 Haga clic en **Agregar**.

Configurar una conexión del proveedor de identidades integrado

Puede configurar varios proveedores de identidades integrados y asociar con ellos métodos de autenticación.

Requisitos previos

Si se usa la autenticación Kerberos integrada, descargue el certificado del emisor KDC que se utilizará en la configuración de AirWatch del perfil de administración de dispositivos iOS.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Proveedores de identidades**.

En esta página se muestran los distintos proveedores de identidades configurados.

- 2 Haga clic en **Añadir proveedor de identidades**.

Aparecerá un menú con las opciones del proveedor de identidades.

- 3 Seleccione **Crear IDP integrado**.

4 Introduzca la información apropiada para configurar el proveedor de identidades.

Opción	Descripción
Nombre de proveedor de identidades	Introduzca el nombre de esta instancia del proveedor de identidades integrado.
Usuarios	Seleccione los usuarios que se van a autenticar. Los directorios configurados aparecen en la lista.
Red	Incluye una lista de los rangos de redes existentes configurados en el servicio. Seleccione el rango de redes para los usuarios en función de las direcciones IP que desea dirigir a esta instancia del proveedor de identidades para la autenticación.
Métodos de autenticación	Se muestran los métodos de autenticación que están configurados para el servicio. Seleccione la casilla de verificación de los métodos de autenticación para asociarlos con este proveedor de identidades. De conformidad con el dispositivo y la contraseña, con AirWatch y AirWatch Connector, asegúrese de que está habilitada la opción adecuada en la página de configuración de AirWatch.

5 Haga clic en **Agregar**.

Integrar productos de autenticación de usuario alternativos con Administración de directorios

Normalmente, cuando se configura inicialmente Administración de directorios, se utilizan los conectores que facilita la infraestructura existente de vRealize Automation para crea una conexión de Active Directory para la administración y autenticación basada en el ID y la contraseña de usuario. Otra opción consiste en integrar Administración de directorios con otras soluciones de autenticación como Kerberos o RSA SecurID.

La instancia del proveedor de identidades puede ser la instancia del conector de Directories Management, instancias de proveedores de identidades de terceros o una combinación de ambas.

La instancia del proveedor de identidades que utiliza con los servicios de Directories Management crea una entidad de federación en red que se comunica con el servicio utilizando aserciones de SAML 2.0.

Cuando implementa inicialmente el servicio Directories Management, el conector es el proveedor de identidades inicial del servicio. La infraestructura existente de Active Directory se utiliza para la gestión y la autenticación del usuario.

Se admiten los siguientes métodos de autenticación. Puede configurar estos métodos de autenticación desde la consola de administración.

Tabla 2-8. Tipos de autenticación de usuario admitidos por Administración de directorios

Tipos de autenticación	Descripción
Contraseña (implementación en las instalaciones)	Sin ninguna configuración después de haber configurado Active Directory, Directories Management admite la autenticación con contraseña en Active Directory. Con este método, los usuarios se autentican directamente en Active Directory.
Kerberos para escritorios	La autenticación de Kerberos proporciona acceso al portal de aplicaciones a los usuarios de dominio que cuentan con un inicio de sesión único. No es necesario que los usuarios vuelvan a iniciar sesión después de hacerlo en la red.
Certificado (implementación en las instalaciones)	Se puede configurar la autenticación basada en certificados para permitir que los clientes se autenticquen con certificados desde su escritorio y dispositivos móviles, o bien para utilizar un adaptador de tarjeta inteligente para la autenticación. La autenticación basada en certificados se basa en lo que tiene el usuario y en lo que sabe la persona. Un certificado X.509 utiliza el estándar de infraestructura de clave pública para comprobar que una clave pública contenida en el certificado pertenezca al usuario.
RSA SecurID (implementación en las instalaciones)	Cuando está configurada la autenticación RSA SecurID, se configura Directories Management como agente de autenticación en el servidor RSA SecurID. La autenticación RSA SecurID requiere que los usuarios utilicen un sistema de autenticación basado en tokens. RSA SecurID es un método de autenticación para los usuarios que obtienen acceso a Directories Management desde fuera de la red empresarial.
RADIUS (implementación en las instalaciones)	La autenticación RADIUS proporciona opciones de autenticación en dos fases. Se configura el servidor RADIUS que sea accesible para el servicio de Directories Management. Cuando los usuarios inician sesión con su nombre de usuario y código de acceso, se envía una solicitud de acceso al servidor RADIUS para la autenticación.
Autenticación adaptativa de RSA (implementación en las instalaciones)	La autenticación RSA proporciona una autenticación multifactor más segura que la que solo usa un nombre de usuario y una contraseña en Active Directory. Si se habilita la autenticación adaptativa de RSA, los indicadores de riesgo especificados en la directiva de riesgos se configuran en la aplicación de administración de directivas de RSA. La configuración del servicio Directories Management de la autenticación adaptativa se utiliza para determinar la autenticación necesaria.
SSO móvil (para iOS)	La autenticación SSO móvil para iOS se utiliza para una autenticación Single Sign-On en los dispositivos iOS administrados por AirWatch. La autenticación SSO móvil (para iOS) utiliza un centro de distribución de claves (KDC, Key Distribution Center) que forma parte del servicio Directories Management. Debe iniciar el servicio KDC en VMware Identity Manager antes de habilitar el método de autenticación.
SSO móvil (para Android)	El SSO móvil para la autenticación de Android se utiliza para la autenticación Single Sign-On en los dispositivos Android gestionados por AirWatch. Se configura un servicio de proxy entre el servicio Directories Management y AirWatch para recuperar el certificado desde AirWatch para la autenticación.
Contraseña (AirWatch Connector)	AirWatch Cloud Connector puede tener integrado el servicio Directories Management para la autenticación de la contraseña del usuario. Configure el servicio Directories Management para sincronizar los usuarios desde el directorio de AirWatch.

Los usuarios se autentican siguiendo los métodos de autenticación, la reglas de la directiva de acceso por defecto, los rangos de la red y la instancia del proveedor de identidades de identidad que configura. Después de configurar los métodos de autenticación, crea reglas de directivas de acceso que especifiquen los métodos de autenticación que se debe utilizar según el tipo de dispositivo.

Configurar SecurID para Directories Management

Cuando se configura el servidor RSA SecurID, debe añadir la información del servicio de de Directories Management como el agente de autenticación del servidor RSA SecurID y configurar la información del servidor de RSA SecurID en el servicio de de Directories Management.

Cuando configura SecurID para proporcionar seguridad adicional, debe asegurarse de que la red está correctamente configurada para la implementación de Directories Management. En concreto para SecurID, debe asegurarse que que el puerto correcto está abierto para habilitar SecurID para autenticar usuarios fuera de la red.

Tras ejecutar el asistente para la instalación de de Directories Management y configurar la conexión de Active Directory, dispone de la información necesaria para preparar el servidor RSA SecurID. Tras preparar el servidor RSA SecurID de Directories Management, habilite SecurID en la consola de administración.

■ Preparar el servidor RSA SecurID

El servidor RSA SecurID debe configurarse con información acerca del dispositivo de Directories Management como el agente de autenticación. La información necesaria es el nombre de host y las direcciones IP de las interfaces de red.

■ Configurar la autenticación de RSA SecurID

Después de configurar Administración de directorios como agente de autenticación en el servidor RSA SecurID, es necesario añadir la información de configuración de RSA SecurID al conector.

Preparar el servidor RSA SecurID

El servidor RSA SecurID debe configurarse con información acerca del dispositivo de Directories Management como el agente de autenticación. La información necesaria es el nombre de host y las direcciones IP de las interfaces de red.

Requisitos previos

- Compruebe que una de las siguientes versiones del administrador de autenticación RSA esté instalada y en funcionamiento en la red empresarial: RSA AM 6.1.2, 7.1 SP2 y versiones posteriores, y 8.0 y versiones posteriores. El servidor de Directories Management utiliza AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1), que solo admite las versiones anteriores del administrador de autenticación RSA (el servidor RSA SecurID). Para obtener más información acerca de la instalación y configuración del administrador de autenticación RSA (servidor RSA SecurID), consulte la documentación de RSA.

Procedimiento

- 1 En una versión admitida del servidor RSA SecurID, añada Directories Management Connector como agente de autenticación. Escriba la siguiente información.

Opción	Descripción
Nombre de host	El nombre de host de Directories Management.
Dirección IP	La dirección IP de Directories Management.
Dirección IP alternativa	Si el tráfico del conector pasa a través de un dispositivo de traducción de direcciones de red (NAT) para alcanzar el servidor RSA SecurID, escriba la dirección IP privada del dispositivo.

- 2 Descargue el archivo de configuración comprimido y extraiga el archivo `sdconf.rec`.

Esté preparado para cargar este archivo más tarde cuando configure RSA SecurID en Directories Management.

Pasos siguientes

Vaya a la consola administrativa y, en las páginas Configuración de administración de identidad y acceso, seleccione el conector y en la página Adaptadores de autenticación configure SecurID.

Configurar la autenticación de RSA SecurID

Después de configurar Administración de directorios como agente de autenticación en el servidor RSA SecurID, es necesario añadir la información de configuración de RSA SecurID al conector.

Requisitos previos

- Compruebe que el administrador de autenticación RSA (el servidor RSA SecurID) esté instalado y configurado de forma correcta.
- Descargue el archivo comprimido del servidor RSA SecurID y extraiga el archivo de configuración del servidor.

Procedimiento

- 1 Como administrador de tenants, navegue a **Administración > Administración de directorios > Conectores**
- 2 En la página Conectores, seleccione el vínculo Trabajo para el conector que se vaya a configurar con RSA SecurID.
- 3 Haga clic en **Adaptadores de autenticación** y después en **SecurIDIdpAdapter**.
Se le redirige a la página de inicio de sesión del administrador de identidades.
- 4 En la página Adaptadores de autenticación, en la fila SecurIDIdpAdapter, haga clic en **Editar**.
- 5 Configure la página Adaptador de autenticación SecurID.

La información usada y los archivos generados en el servidor RSA SecurID son necesarios cuando se configura la página de SecurID.

Opción	Acción
Nombre	Es necesario un nombre. El nombre predeterminado es SecurIDdpAdapter. Puede cambiarlo.
Habilitar SecurID	Active esta casilla para habilitar la autenticación SecurID.
Número de intentos de autenticación permitidos	Escriba el número máximo de intentos de inicio de sesión fallidos cuando se usa el token de RSA SecurID. El valor predeterminado es cinco intentos.
Dirección del conector	Escriba la dirección IP de la instancia del conector. El valor que escriba debe coincidir con el que usó cuando añadió el dispositivo de conector como agente de autenticación al servidor RSA SecurID. Si el servidor RSA SecurID tiene un valor asignado para la indicación Dirección IP alternativa, escriba ese valor como dirección IP del conector. Si no hay ninguna dirección IP asignada, escriba el valor asignado a la indicación Dirección IP.
Dirección IP del agente	Escriba el valor asignado a la indicación Dirección IP en el servidor RSA SecurID.
Configuración del servidor	Cargue el archivo de configuración del servidor RSA SecurID. En primer lugar, debe descargar el archivo comprimido dese el servidor RSA SecurID y extraer el archivo de configuración del servidor, que de forma predeterminada se denomina <code>sdconf.rec</code> .
Secreto del nodo	Si deja el campo Secreto del nodo en blanco, dicho secreto se vuelve a generar. Se recomienda que borre el archivo de secreto del nodo en el servidor RSA SecurID y no cargue, de forma intencionada, el archivo de secreto del nodo. Asegúrese de que el archivo de secreto del nodo en el servidor RSA SecurID y en la instancia del conector del servidor siempre coincidan. Si cambia el secreto del nodo en una ubicación, cámbielo también en la otra.

6 Haga clic en **Guardar**.

Pasos siguientes

Añada el método de autenticación a la política de acceso predeterminada. Navegue a **Administración > Administración de directorios > Políticas** y haga clic en **Editar política predeterminada** para editar las reglas de la política predeterminada con objeto de añadir el método de autenticación de SecurID a la regla en el orden de autenticación correcto.

Configurar RADIUS para Directories Management

Puede configurar Directories Management para que los usuarios necesiten utilizar la autenticación RADIUS (Servicio de autenticación remota telefónica de usuario). La información del servidor RADIUS se configura en el servicio de Directories Management.

El soporte de RADIUS ofrece un amplio rango de opciones de autenticación alternativas en dos fases basada en tokens. Dado que las soluciones de autenticación de dos fases, como RADIUS, trabajan con administradores de autenticación instalados en servidores separados, el servidor RADIUS debe ser accesible para el servicio del administrador de identidad.

Cuando los usuarios inician la sesión en el portal Mis aplicaciones y la autenticación RADIUS está habilitada, aparece en el navegador un cuadro de diálogo de inicio de sesión especial. Los usuarios escriben el nombre de usuario y código de acceso de autenticación RADIUS en el cuadro de diálogo de inicio de sesión. Si el servidor RADIUS emite un desafío de acceso, el servicio del administrador de identidad muestra un cuadro de diálogo que solicita un segundo código de acceso. Actualmente, el soporte para los desafíos RADIUS se limita a solicitar la entrada de texto.

Cuando un usuario ha escrito sus credenciales en el cuadro de diálogo, el servidor RADIUS puede enviarle un código a través de un mensaje de correo electrónico, un mensaje de texto SMS o bien algún otro mecanismo fuera de banda. El usuario puede escribir este texto y código en el cuadro de diálogo de inicio de sesión para completar la autenticación.

Si el servidor RADIUS ofrece la posibilidad de importar usuarios desde Active Directory, puede que a los usuarios finales se les pidan credenciales de Active Directory antes de solicitar un nombre de usuario y código de acceso de autenticación RADIUS.

Preparar el servidor RADIUS

Prepare el servidor RADIUS y, a continuación, configúrelo para que acepte peticiones de RADIUS procedentes del servicio de Directories Management.

Consulte las guías de configuración del proveedor de RADIUS para obtener información sobre la configuración del servidor RADIUS. Tenga en cuenta que la información de configuración de RADIUS cuando la utilice para configurar RADIUS en el servicio. Para ver el tipo de información de RADIUS necesaria para configurar Directories Management, consulte [Configurar la autenticación RADIUS en Administración de directorios](#).

Puede configurar un servidor de autenticación de Radius secundario para los casos de alta disponibilidad. Si el servidor RADIUS principal no responde en el tiempo de espera del servidor configurado para la autenticación de RADIUS, la solicitud se enruta al servidor secundario. Cuando el servidor principal no responde, el segundo recibe todas las solicitudes de autenticación que llegan a continuación.

Configurar la autenticación RADIUS en Administración de directorios

El software RADIUS se habilita en un servidor del administrador de autenticación. Para la autenticación RADIUS, siga las instrucciones en la documentación de configuración del proveedor.

Requisitos previos

Instale y configure el software de RADIUS en un servidor de administrador de autenticación. Para la autenticación RADIUS, siga las instrucciones en la documentación de configuración del proveedor.

Necesita conocer la siguiente información del servidor RADIUS para configurar RADIUS en el servicio.

- Dirección IP o nombre DNS del servidor RADIUS.
- Números de puertos de autenticación. El puerto de autenticación suele ser el 1812.

- Tipo de autenticación. Entre los tipos de autenticación, se incluyen Protocolo de autenticación de contraseña (Password Authentication Protocol, PAP), Protocolo de autenticación por desafío mutuo (Challenge Handshake Authentication Protocol, CHAP) y Protocolo de autenticación por desafío mutuo de Microsoft, versiones 1 y 2 (Microsoft Challenge Handshake Authentication Protocol, versions 1 and 2; MSCHAP1 y MSCHAP2).
- Secreto compartido de RADIUS que se usa para el cifrado y descifrado en los mensajes del protocolo RADIUS.
- Valores específicos de tiempo de espera y reintento necesarios para la autenticación RADIUS.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Conectores**.
- 2 En la página Conectores, seleccione el vínculo Trabajo para el conector que se vaya a configurar para la autenticación RADIUS.
- 3 Haga clic en **Adaptadores de autenticación** y después en **RadiusAuthAdapter**.
Se le redirige a la página de inicio de sesión del administrador de identidades.
- 4 Haga clic en **Editar** para configurar estos campos en la página Adaptador de autenticación.

Opción	Acción
Nombre	Es necesario un nombre. El nombre predeterminado es RadiusAuthAdapter. Puede cambiarlo.
Habilitar adaptador de Radius	Active esta casilla para habilitar la autenticación RADIUS.
Número de intentos de autenticación permitidos	Escriba el número máximo de intentos de inicio de sesión fallidos cuando se usa RADIUS para iniciar sesión. El valor predeterminado es cinco intentos.
Número de intentos en el servidor Radius	Especifique el número total de reintentos. Si el servidor principal no responde, el servicio espera el tiempo configurado antes de volver a intentarlo.
Nombre del host/dirección del servidor Radius	Escriba el nombre del host o la dirección IP del servidor RADIUS.
Puerto de autenticación	Escriba el número de puerto para la autenticación RADIUS. Suele ser el 1812.
Puerto de cuentas	Escriba 0 como número de puerto. En estos momentos, no se usa el puerto de cuentas.
Tipo de autenticación	Indique el protocolo de autenticación compatible con el servidor RADIUS. Elija PAP, CHAP, MSCHAP1 o MSCHAP2.

Opción	Acción
Secreto compartido	Escriba el secreto compartido que se usa entre el servidor RADIUS y el servicio de VMware Identity Manager.
Tiempo de espera del servidor en segundos	Escriba el tiempo de espera del servidor RADIUS en segundos, después del cual se enviará un reintento si el servidor RADIUS no responde.
Prefijo de territorio	(Opcional) La ubicación de la cuenta de usuario se denomina territorio. Si especifica una cadena de prefijo de territorio, se coloca al principio del nombre de usuario cuando se envía al servidor RADIUS. Por ejemplo, si el nombre de usuario es jdoe y se especifica el prefijo de territorio DOMAIN-A\, se envía el nombre de usuario DOMAIN-A\jdoe al servidor RADIUS. Si no configura estos campos, solamente se envía el nombre de usuario que se indique.
Sufijo de territorio	(Opcional) Si especifica un sufijo de territorio, la cadena se coloca al final del nombre de usuario. Por ejemplo, si el sufijo es @myco.com, se envía el nombre de usuario jdoe@myco.com al servidor RADIUS.
Sugerencia de frase de contraseña de página de inicio de sesión	Escriba la cadena de texto que se mostrará en el mensaje de la página de inicio de sesión de usuario a los usuarios directos para que escriban el código de acceso de RADIUS correcto. Por ejemplo, si este campo está configurado con contraseña de AD primero y después el código de acceso SMS , el mensaje de la página de inicio de sesión sería Escriba su contraseña de AD primero y después el código de acceso SMS . La cadena de texto predeterminada es Código de acceso de RADIUS .

5 Puede habilitar un servidor RADIUS secundario para lograr una disponibilidad elevada.

Configure el servidor secundario tal como se describe en el paso 4.

6 Haga clic en **Guardar**.

Pasos siguientes

Añada el método de autenticación RADIUS a la política de acceso predeterminada. Seleccione **Administración > Administración de directorios > Políticas** y haga clic en **Editar política predeterminada** para editar las reglas de la política predeterminada con objeto de añadir el método de autenticación de RADIUS a la regla en el orden de autenticación correcto.

Configurar un certificado o adaptador de tarjeta inteligente para utilizarlo con Directories Management

Puede configurar la autenticación del certificado x509 para que los clientes puedan autenticar con certificados desde su escritorio o dispositivos móviles, o bien para utilizar un adaptador de tarjeta inteligente para la autenticación. La autenticación basada en certificados se basa en lo que tiene el usuario (la clave privada o tarjeta inteligente) y en lo que sabe la persona (la contraseña de la clave privada o el PIN de la tarjeta inteligente). Un certificado X.509 utiliza el estándar de infraestructura de clave pública (PKI) para comprobar que la clave pública que contiene el certificado pertenece al usuario. Gracias a la autenticación con tarjeta inteligente, los usuarios se conectan a esta con el equipo y escriben un PIN.

Los certificados de tarjeta inteligente se copian en el almacén de certificados local del equipo del usuario. Los certificados del almacén de certificados local están disponibles en todos los navegadores que se ejecuten en el equipo del usuario, excepto en algunos casos, y por lo tanto están disponibles para una instancia de Directories Management en el navegador.

- **Usar el nombre principal de usuario para la autenticación de certificado**

Puede usar la asignación de certificados en Active Directory. Los inicios de sesión con certificado y tarjeta inteligente usan el nombre principal de usuario (UPN) de Active Directory para validar las cuentas de usuario. Las cuentas de Active Directory de los usuarios que intentan autenticarse en el servicio Directories Management deben poseer un UPN válido que se corresponda con el UPN en el certificado.

- **Entidad de certificación necesaria para la autenticación**

Para habilitar el inicio de sesión mediante la autenticación de certificado, se deben cargar los certificados raíz e intermedios en el de Directories Management.

- **Usar la comprobación de revocación de certificados**

Puede configurar la comprobación de revocación de certificados para impedir la autenticación de los usuarios cuyos certificados de usuario se hayan revocado. Con frecuencia, los certificados se revocan cuando un usuario deja una organización, pierde una tarjeta inteligente o cambia de departamento.

- **Configurar la autenticación mediante certificado para la administración de directorios**

La autenticación mediante certificado se habilita y configura en la función de administración de directorios de la consola de administración de vRealize Automation.

Usar el nombre principal de usuario para la autenticación de certificado

Puede usar la asignación de certificados en Active Directory. Los inicios de sesión con certificado y tarjeta inteligente usan el nombre principal de usuario (UPN) de Active Directory para validar las cuentas de usuario. Las cuentas de Active Directory de los usuarios que intentan autenticarse en el servicio Directories Management deben poseer un UPN válido que se corresponda con el UPN en el certificado.

Puede configurar Directories Management para que use la dirección de correo electrónico para validar la cuenta de usuario si no existe un UPN en el certificado.

También puede habilitar un tipo de UPN alternativo para que se use.

Entidad de certificación necesaria para la autenticación

Para habilitar el inicio de sesión mediante la autenticación de certificado, se deben cargar los certificados raíz e intermedios en el de Directories Management.

Los certificados se copian en el almacén de certificados local del equipo del usuario. Los certificados del almacén de certificados local están disponibles en todos los navegadores que se ejecuten en el equipo del usuario, excepto en algunos casos, y por lo tanto están disponibles para una instancia de Directories Management en el navegador.

Para la autenticación de tarjeta inteligente, cuando un usuario inicia una conexión con la instancia de Directories Management, el servicio de Directories Management envía una lista de entidades de certificación (CA) de confianza al navegador. El navegador coteja la lista de CA de confianza con los certificados de usuario disponibles, selecciona uno adecuado y después solicita al usuario que proporcione un PIN de tarjeta inteligente. Si se dispone de varios certificados de usuario, el navegador solicita al usuario que seleccione uno.

Si un usuario no se puede autenticar, es posible que la CA raíz y las intermedias no estén configuradas correctamente, o bien que el servicio no se haya reiniciado después de que las CA raíz e intermedias se cargaran en el servidor. En estos casos, el navegador no puede mostrar los certificados instalados, el usuario no puede seleccionar el correcto y, por tanto, la autenticación de certificado genera un error.

Usar la comprobación de revocación de certificados

Puede configurar la comprobación de revocación de certificados para impedir la autenticación de los usuarios cuyos certificados de usuario se hayan revocado. Con frecuencia, los certificados se revocan cuando un usuario deja una organización, pierde una tarjeta inteligente o cambia de departamento.

Se admite la comprobación de revocación de certificados con listas de revocación de certificados (CRL) y con el Protocolo de estado de certificados en línea (Online Certificate Status Protocol, OCSP). Una CRL es una lista de certificados revocados publicada por la CA que emitió los certificados. OCSP es un protocolo de validación de certificados que se usa para obtener el estado de revocación de un certificado.

Puede configurar la comprobación de revocación de certificados en la consola de administración, en Conectores > Adaptadores de autenticación > página CertificateAuthAdapter, cuando configure la autenticación de certificado.

Puede definir tanto CRL como OCSP en la configuración del mismo adaptador de autenticación de certificado. Cuando se configuran ambos tipos de comprobación de revocación de certificados y la casilla Usar CRL en caso de error de OCSP está habilitada, se comprueba antes con OCSP y, si esto no funciona, la comprobación de revocación de certificados recae en la CRL. La comprobación de revocación no recae en OCSP si falla la CRL.

Iniciar sesión con la comprobación con CRL

Cuando habilita la revocación de certificados, el servidor del de Directories Management lee una CRL para determinar el estado de revocación de un certificado de usuario.

Si el certificado está revocado, la autenticación mediante él genera un error.

Iniciar sesión con la comprobación de certificado con OCSP

Cuando configura la comprobación de revocación con el protocolo OCSP de estado de certificado, el de Directories Management envía una solicitud a un respondedor OCSP para determinar el estado de revocación de un certificado de usuario concreto. El servidor del de Directories Management usa el certificado de firma de OCSP para comprobar que las respuestas que reciba del respondedor OCSP sean genuinas.

Si el certificado está revocado, la autenticación genera un error.

Puede configurar la autenticación para que recurra a la comprobación con CRL si no recibe respuesta del respondedor OCSP o si la respuesta no es válida.

Configurar la autenticación mediante certificado para la administración de directorios

La autenticación mediante certificado se habilita y configura en la función de administración de directorios de la consola de administración de vRealize Automation.

Requisitos previos

- Obtener el certificado raíz y los certificados intermedios de la CA que firmó los certificados presentados por sus usuarios.
- (Opcional) Lista de identificadores de objeto (OID) de políticas de certificados válidas para la autenticación de certificado.
- Para comprobar la revocación, la ubicación del archivo de la CRL, la dirección URL del servidor OCSP.
- (Opcional) Ubicación del archivo de certificado de firma para la respuesta OCSP.
- Contenido del formulario de consentimiento, si se va a habilitar un formulario de consentimiento para mostrarlo antes de la autenticación.

Procedimiento

- 1 Como administrador de tenants, navegue a **Administración > Administración de directorios > Conectores**
- 2 En la página Conectores, seleccione el vínculo Trabajo para el conector que se vaya a configurar.
- 3 Haga clic en **Adaptadores de autenticación** y después en **CertificateAuthAdapter**.
Se le redirige a la página de inicio de sesión del administrador de identidades.
- 4 En la fila de CertificateAuthAdapter, haga clic en **Editar**.
- 5 Configure la página Adaptador de autenticación de certificado.

Nota El asterisco indica que el campo es obligatorio. El resto de los campos son opcionales.

Opción	Descripción
*Nombre	Es necesario un nombre. El nombre predeterminado es CertificateAuthAdapter. Puede cambiarlo.
Habilitar adaptador de certificado	Active esta casilla para habilitar la autenticación de certificado.
*Certificados de CA raíz e intermedios	Seleccione los certificados que desee cargar. Puede seleccionar varios certificados de CA raíz e intermedios que estén codificados como DER o PEM.

Opción	Descripción
Certificados de CA cargados	<p>Los archivos de certificado cargados aparecen en la sección Certificados de CA cargados del formulario.</p> <p>Debe reiniciar el servicio para que los nuevos certificados estén disponibles. Haga clic en Reiniciar servicio web para reiniciar el servicio y añadir los certificados al servicio de confianza.</p> <p>Nota Cuando se reinicia el servicio, no se habilita la autenticación de certificado. Una vez reiniciado el servicio, proceda a configurar esta página. Si hace clic en Guardar al final de la página, se habilita la autenticación de certificado en el servicio.</p>
Usar correo electrónico si no hay UPN en el certificado	Si el nombre principal de usuario (UPN) no existe en el certificado, active esta casilla para usar el atributo emailAddress como extensión de nombre alternativo del firmante para validar las cuentas de usuario.
Políticas de certificados aceptadas	<p>Cree una lista de los identificadores de objeto que se aceptan en las extensiones de las políticas de certificados.</p> <p>Escriba los números de ID de objeto (OID) para la política de emisión de certificados. Haga clic en Añadir otro valor para añadir más OID.</p>
Habilitar revocación de certificados	Active esta casilla para habilitar la comprobación de revocación de certificados. Esto impide la autenticación de los usuarios con certificados de usuario revocados.
Usar CRL de certificados	Active esta casilla para usar la lista de revocación de certificados (CRL) publicada por la CA que emitió los certificados para validar el estado de un certificado, es decir, si está revocado o no.
Ubicación de la CRL	Escriba la ruta de archivo del servidor o local desde la que recuperar la CRL.
Habilitar revocación con OCSP	Active la casilla para usar el protocolo de validación de certificados Protocolo de estado de certificados en línea (Online Certificate Status Protocol, OCSP) para obtener el estado de revocación de un certificado.
Usar CRL en caso de error de OCSP	Si configura tanto CRL como OCSP, puede activar esta casilla para recurrir de nuevo a la CRL si la comprobación con OCSP no está disponible.
Enviar nonce de OCSP	Active esta casilla si desea que se envíe en la respuesta el identificador único de la solicitud de OCSP.
URL de OCSP	Si habilitó la revocación con OCSP, escriba la dirección del servidor OCSP para la comprobación de la revocación.
Certificado de firma del respondedor OCSP	Escriba la ruta del certificado OCSP para el respondedor, <i>/path/to/file.cer</i> .
Habilitar formulario de consentimiento antes de autenticación	Active esta casilla para incluir una página de formulario de consentimiento que aparezca antes de que los usuarios inicien sesión en su portal de Mis aplicaciones mediante la autenticación de certificado.
Contenido del formulario de consentimiento	Escriba el texto que aparece en el formulario de consentimiento en este cuadro de texto.

6 Haga clic en **Guardar**.

Pasos siguientes

- Añada el método de autenticación mediante certificado a la política de acceso predeterminada. Navegue a **Administración > Administración de directorios > Políticas** y haga clic en **Editar política predeterminada** para editar las reglas de la política predeterminada y añadir la opción de Certificado para convertirla en el primer método de autenticación de la política predeterminada. Los certificados deben ser el primer método de autenticación indicado en la regla de la política para que no se produzca ningún error en la autenticación de certificado.
- Cuando se configura la autenticación de certificado y el dispositivo del servicio esté configurado tras un equilibrador de carga, asegúrese de que el conector de Directories Management esté configurado con paso a través SSL en el equilibrador de carga y no para finalizar SSL en el equilibrador de carga. Esta configuración garantiza que el protocolo de enlace SSL se encuentre entre el conector y el cliente para pasar el certificado al conector.

Configurar una instancia de proveedor de identidades externo para autenticar usuarios

Puede configurar un proveedor de identidades externo que se use para autenticar usuarios en el servicio Directories Management.

Complete las siguientes tareas antes de usar la consola de administración para añadir la instancia de proveedor de identidades externo.

- Compruebe que las instancias externas cumplen con SAML 2.0 y que el servicio puede acceder a la instancia externa.
- Obtenga la información de metadatos externa adecuada para añadir cuando configure el proveedor de identidades en la consola de administración. La información de metadatos que obtenga de la instancia externa será la URL a los metadatos o los metadatos reales.

Configurar una conexión de proveedor de identidades de terceros

vRealize Automation se proporciona con una instancia de conexión de proveedor de identidades predeterminada. Es posible que los usuarios deseen crear conexiones de proveedor de identidades adicionales para admitir el aprovisionamiento de usuarios de Just-in-Time u otras configuraciones personalizadas.

vRealize Automation se proporciona con un proveedor de identidades predeterminado. En la mayoría de los casos, el proveedor predeterminado cumple con las necesidades del cliente. No obstante, si utiliza una solución de administración de identidades empresarial existente, puede configurar un proveedor de identidades personalizado para redirigir a los usuarios a su solución de identidades existente.

Cuando se utiliza un proveedor de identidades personalizado, la administración de directorios utiliza los metadatos de SAML de ese proveedor para establecer una relación de confianza con el proveedor. Una vez establecida esta relación, la administración de directorios asigna los usuarios de la aserción de SAML a la lista de usuarios internos de vRealize Automation según el identificador del nombre de asunto.

Requisitos previos

- Configure los rangos de redes que desea dirigir hacia esta instancia del proveedor de identidades para la autenticación. Consulte [Añadir o editar un rango de redes](#).
- Acceda al documento de metadatos de terceros. Puede ser la dirección URL de los metadatos o los propios metadatos.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Proveedores de identidades**.

En esta página se muestran los distintos proveedores de identidades configurados.

- 2 Haga clic en **Añadir proveedor de identidades**.

Aparecerá un menú con las opciones del proveedor de identidades.

- 3 Seleccione **Crear IDP de terceros**.

- 4 Introduzca la información apropiada para configurar el proveedor de identidades.

Opción	Descripción
Nombre de proveedor de identidades	Escriba un nombre para la instancia del proveedor de identidades.
Metadatos de SAML	<p>Añada el documento de metadatos basado en XML de IDP de terceros para establecer una relación de confianza con el proveedor de identidades.</p> <ol style="list-style-type: none"> 1 Escriba la dirección URL de los metadatos de SAML o bien el contenido xml en el cuadro de texto. 2 Haga clic en Procesar metadatos de IDP. Los formatos de ID de nombre compatibles con el IDP se extraen de los metadatos y se añaden a la tabla Formato de ID de nombre. 3 En la columna de valor de ID de nombre, seleccione el atributo de usuario del servicio para asignarlo a los formatos de ID que aparecen. Puede añadir formatos de ID de nombre personalizados de terceros y asignarlos a los valores de atributos de usuario del servicio. 4 (Opcional) Seleccione el formato de cadena de identificador de respuesta NameIDPolicy.
Usuarios	Seleccione los directorios de Directories Management de los usuarios que pueden autenticarse con este proveedor de identidades.
Aprovisionamiento de usuarios de Just-in-Time	<p>Seleccione las opciones adecuadas para admitir el aprovisionamiento de Just-in-Time mediante un proveedor de identidades de terceros apropiado.</p> <p>En Nombre de directorio, introduzca el nombre de directorio que se utilizará para el aprovisionamiento de Just-in-Time.</p> <p>En Dominios, especifique uno o varios dominios que existan en el proveedor de identidades externo que se va a utilizar para el aprovisionamiento de Just-in-Time.</p>
Red	<p>Incluye una lista de los rangos de redes existentes configurados en el servicio.</p> <p>Seleccione los rangos de redes para los usuarios, basados en sus direcciones IP, que desea dirigir hacia la instancia en cuestión del proveedor de identidades para la autenticación.</p>

Opción	Descripción
Métodos de autenticación	Añada los métodos de autenticación que admite el proveedor de identidades de terceros. Seleccione la clase de contexto de autenticación de SAML compatible con el método de autenticación.
Certificado de firma de SAML	Haga clic en Metadatos del proveedor de servicios (SP) para ver la dirección URL de los metadatos del proveedor de servicios de SAML de Directories Management. Copie la dirección URL y guárdela. Esta dirección URL se configura al editar la aserción de SAML en el proveedor de identidades de terceros para asignar usuarios de Directories Management.
Nombre de host	Si aparece el campo Hostname , escriba el nombre de host al que será redirigido el proveedor de identidades para la autenticación. Si utiliza un puerto no estándar distinto del 443, puede definirlo con el formato Nombredehost:Puerto. Por ejemplo, miemp.ejemplo.com:8443.

5 Haga clic en **Agregar**.

Pasos siguientes

- Copie y guarde los metadatos del proveedor de servicios de Directories Management necesarios para configurar la instancia del proveedor de identidades de terceros. Estos metadatos están disponibles en la sección Certificado de firma de SAML de la página Proveedor de identidades.
- Añada el método de autenticación del proveedor de identidades a la política predeterminada de servicios.

Consulte la guía de *Configuración de recursos en Directories Management* para obtener información sobre cómo añadir y personalizar los recursos que añade al catálogo.

Administrar métodos de autenticación para aplicar a usuarios

El servicio de Directories Management intenta autenticar a los usuarios basándose en los métodos de autenticación, la política de acceso predeterminada, los rangos de redes y las instancias de proveedor de identidades que configure.

Cuando los usuarios tratan de iniciar sesión, el servicio evalúa las reglas de la política de acceso predeterminada para seleccionar qué regla aplicar a la política. Los métodos de autenticación se aplican en el orden en que se muestran en la regla. Se selecciona la primera instancia de proveedor de identidades que reúna los requisitos de método de autenticación y rango de redes de la regla y la solicitud de autenticación de usuario se reenvía a la instancia de proveedor de identidades para su autenticación. En caso de error de autenticación, se aplicará el siguiente método de autenticación configurado en la regla.

Puede agregar reglas que especifiquen los métodos de autenticación que se usarán por tipo de dispositivo o por tipo de dispositivo y desde un rango de redes específico. Por ejemplo, podría configurar una regla que haga que los usuarios que inician sesión con un dispositivo iOS desde una red específica se autenticuen mediante RSA SecurID y otra regla que especifique que todos los tipos de dispositivo que inicien sesión desde la dirección IP de la red interna se autenticuen con su contraseña.

Añadir o editar un rango de redes

Es posible administrar los rangos de redes para definir las direcciones IP a partir de las cuales los usuarios pueden iniciar sesión a través de un vínculo de Active Directory. Los rangos de redes que cree se añaden a las instancias específicas de proveedor de identidades y a las reglas de políticas de acceso.

Defina rangos de redes para su implementación de Directories Management basándose en su topología de red.

Se crea un rango de redes denominado ALL RANGES, que pasa a ser el predeterminado. Este rango de redes incluye todas las direcciones IP disponibles en Internet, de 0.0.0.0 a 255.255.255.255. Aunque su implementación cuente con una única instancia de proveedor de identidades, puede cambiar el rango de direcciones IP y añadir otros rangos para excluir o incluir direcciones IP específicas en el rango de redes predeterminado. Puede crear otros rangos de redes con direcciones IP específicas que podrá aplicar para una finalidad concreta.

Nota El rango de redes predeterminado ALL RANGES y su descripción "a network for all ranges" son editables. Para editar el nombre y la descripción, incluido cambiar el texto a otro idioma, haga clic en el nombre del rango de redes en la página Rangos de redes.

Requisitos previos

- Deberá haber configurado tenants para su implementación de vRealize Automation y un vínculo adecuado de Active Directory que admita la autenticación básica mediante ID de usuario y contraseña de Active Directory.
- Active Directory deberá estar instalado y configurado para utilizarse en su red.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Rangos de redes**.
- 2 Edite un rango de redes existente o añada uno nuevo.

Opción	Descripción
Editar un rango existente	Haga clic en el nombre del rango de redes para editarlo.
Añadir un rango	Haga clic en Añadir rango de redes para añadir un nuevo rango.

- 3 Complete el formulario.

Elemento del formulario	Descripción
Nombre	Especifique un nombre para el rango de redes.
Descripción	Especifique una descripción para el rango de redes.

Elemento del formulario	Descripción
Ver Pods	<p>La opción Ver Pods solo aparece cuando está habilitado el módulo Ver.</p> <p>Host de URL de acceso de cliente. Escriba la URL de acceso de Horizon Client para el rango de redes.</p> <p>Puerto de acceso de cliente. Escriba el número de puerto de acceso de Horizon Client para el rango de redes.</p>
Rangos de IP	Edite o añada rangos de IP hasta que se hayan incluido todas las direcciones IP deseadas y excluido las no deseadas.

Pasos siguientes

- Asocie cada rango de redes con una instancia de proveedor de identidades.
- Asocie los rangos de redes con la regla de política de acceso según sea necesario. Consulte [Configurar la política de acceso](#).

Seleccionar atributos para sincronizar con el directorio

Cuando configura el directorio de Directories Management para que se sincronice con Active Directory, especifica los atributos de usuario que se sincronizan con el directorio. Antes de configurar el directorio, puede especificar en la página Atributos de usuario qué atributos predeterminados son necesarios y, si lo desea, añadir atributos adicionales que desee asignar a los atributos de Active Directory.

Cuando configura la página Atributos de usuario antes de que se cree el directorio, puede cambiar los atributos predeterminados de obligatorios a no obligatorios, marcar atributos como obligatorios y añadir atributos personalizados.

Para obtener una lista de los atributos asignados predeterminados, consulte [Administrar atributos de usuario que se sincronizan desde Active Directory](#).

Una vez creado el directorio, puede convertir un atributo obligatorio en no obligatorio, y puede eliminar atributos personalizados. No se puede convertir un atributo en atributo obligatorio.

Cuando añada otros atributos para que se sincronicen con el directorio, una vez creado el directorio, vaya a la página Atributos asignados del directorio para asignar estos atributos a atributos de Active Directory.

Procedimiento

- 1 Inicie sesión en vRealize Automation como administrador del sistema o administrador de tenants.
- 2 Haga clic en la pestaña Administración.
- 3 Seleccione **Administración de directorios > Atributos de usuario**
- 4 En la sección Atributos predeterminados, repase la lista de atributos obligatorios y realice los cambios necesarios para reflejar cuáles deben serlo.
- 5 En la sección Atributos, añada el nombre de atributo de directorio de Directories Management a la lista.

6 Haga clic en **Guardar**.

Se actualiza el estado de atributo predeterminado y los atributos que añadió se incorporan a la lista Atributos asignados del directorio.

7 Tras la creación del directorio, vaya a la página Almacenes de identidades y seleccione el directorio.**8** Haga clic en **Configuración de sincronización > Atributos asignados**.**9** En el menú desplegable de los atributos que haya añadido, seleccione el atributo de Active Directory al que realizar la asignación.**10** Haga clic en **Guardar**.**Resultados**

El directorio se actualizará la próxima vez que se sincronice con Active Directory.

Aplicar la política de acceso predeterminada

El servicio de Directories Management incluye una política de acceso predeterminada que controla el acceso de usuarios a sus portales de aplicaciones. Puede editar la política para cambiar sus reglas en caso necesario.

Al habilitar los métodos de autenticación distintos a la autenticación con contraseña, debe editar la política predeterminada para añadir el método de autenticación habilitado a las reglas de la política.

Todas las reglas de la política de acceso predeterminada deben reunir unos requisitos para permitir el acceso de usuarios al portal de aplicaciones. Se aplica un rango de redes, se selecciona el tipo de usuario que puede acceder a contenido y los métodos de autenticación que se deseen utilizar. Consulte [Administrar políticas de acceso](#).

El número de intentos que hace el servicio para iniciar la sesión de un usuario mediante un determinado método de autenticación varía. El servicio lleva a cabo una sola vez el intento de autenticación de Kerberos o de certificado. Si el intento de iniciar la sesión de un usuario no se lleva a cabo, se intenta con el siguiente método de autenticación de la regla. De manera predeterminada, está configurado en cinco el máximo número de intentos de inicio de sesión con errores para la contraseña Active Directory y la autenticación RSA SecurID. Cuando un usuario alcanza cinco intentos de inicio de sesión fallidos, el servicio trata de iniciar la sesión del usuario con el método de autenticación que aparece a continuación en la lista. Cuando se hayan agotado todos los métodos de autenticación, el servicio emitirá un mensaje de error.

Aplicar métodos de autenticación a reglas de políticas

El único método de autenticación configurado en las reglas de la política predeterminada es el de contraseña. Debe editar las reglas de la política para seleccionar los otros métodos de autenticación que configuró y establecer el orden en que se usan para la autenticación.

Requisitos previos

Habilite y configure los métodos de autenticación que su organización admita. Consulte [Integrar productos de autenticación de usuario alternativos con Administración de directorios](#)

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Políticas**
- 2 Haga clic en la política de acceso predeterminada para editarla.
- 3 Para editar una regla de la política, haga clic en el método de autenticación para editarlo en la columna Reglas de política, Método de autenticación.

Para añadir una nueva regla de política, haga clic en el icono +.

- 4 Haga clic en **Guardar** y de nuevo en **Guardar** en la página de la política.

Editar regla de directivas

- 5 Haga clic en **Guardar** y de nuevo en **Guardar** en la página de la política.

Configurar Kerberos para Directories Management

La autenticación de Kerberos provee a los usuarios que hayan iniciado sesión en su dominio de Active Directory correctamente de acceso a su portal de aplicaciones sin solicitudes adicionales de credenciales. Es necesario habilitar la autenticación de Windows para permitir que el protocolo Kerberos proteja las interacciones entre los exploradores de los usuarios y el servicio Directories Management. No es necesario configurar Active Directory directamente para que Kerberos funcione con la implementación existente.

Actualmente, Kerberos autentica las interacciones entre el explorador de un usuario y el servicio solo en sistemas operativos Windows. Si se accede al servicio desde otros sistemas operativos, no se utiliza la autenticación de Kerberos.

- **Configurar la autenticación de Kerberos**

Para configurar el servicio Directories Management para que proporcione autenticación de Kerberos, es necesario que se una al dominio y que habilite la autenticación de Kerberos en el conector Directories Management.

- **Configurar Internet Explorer para acceder a la interfaz web**

Debe configurar Internet Explorer si Kerberos está configurado para la implementación y si desea conceder a los usuarios acceso a la interfaz web mediante Internet Explorer.

- **Configurar Firefox para el acceso a la interfaz web**

Si configura Kerberos para su implementación y desea conceder a los usuarios acceso a la interfaz web mediante Firefox, deberá configurar el explorador Firefox.

■ Configurar el explorador Chrome para acceder a la interfaz web

Si configura Kerberos para su implementación y desea conceder a los usuarios acceso a la interfaz web mediante el explorador Chrome, deberá configurar el explorador Chrome.

Configurar la autenticación de Kerberos

Para configurar el servicio Directories Management para que proporcione autenticación de Kerberos, es necesario que se una al dominio y que habilite la autenticación de Kerberos en el conector Directories Management.

Procedimiento

- 1 Como administrador de tenants, navegue a **Administración > Administración de directorios > Conectores**
- 2 En la página Conectores, para el conector que se esté configurando para la autenticación Kerberos, haga clic en **Unirse a dominio**.
- 3 En la página Unirse a dominio, escriba la información del dominio de Active Directory.

Opción	Descripción
Dominio	Escriba el nombre de dominio completo de Active Directory. Este nombre de dominio debe coincidir con el dominio de Windows del servidor del conector.
Usuario de dominio	Escriba el nombre de usuario de una cuenta de Active Directory que posea permisos para unir sistemas a ese dominio de Active Directory.
Contraseña de dominio	Escriba la contraseña asociada al nombre de usuario de AD. Esta contraseña no se almacena en Directories Management.

Haga clic en **Guardar**.

Se actualiza la página Unirse a dominio y se muestra un mensaje que indica que está unido al dominio.

- 4 En la columna Trabajo del conector, haga clic en **Adaptadores de autenticación**.
- 5 Haga clic en **KerberosIdpAdapter**.
Se le redirige a la página de inicio de sesión del administrador de identidades.
- 6 Haga clic en **Editar** en la fila de KerberosIdpAdapter y configure la página de la autenticación Kerberos.

Opción	Descripción
Nombre	Es necesario un nombre. El nombre predeterminado es KerberosIdpAdapter. Puede cambiarlo.
Atributo de UID de directorio	Escriba el atributo de cuenta que contiene el nombre de usuario.
Habilitar autenticación de Windows	Seleccione esta opción para extender las interacciones de autenticación entre los navegadores de los usuarios y Directories Management.

Opción	Descripción
Habilitar NTLM	Seleccione esta opción para habilitar la autenticación basada en el protocolo NT LAN Manager (NTLM) únicamente si la infraestructura de su entorno de Active Directory emplea la autenticación NTLM.
Habilitar redireccionamiento	Seleccione esta opción si DNS de round robin y los equilibradores de carga no son compatibles con Kerberos. Las solicitudes de autenticación se redirigen al nombre del host de redireccionamiento. Si se selecciona esta opción, escriba el nombre del host de redireccionamiento en el cuadro de texto Nombre del host de redireccionamiento . Suele tratarse del nombre del host del servicio.

7 Haga clic en **Guardar**.

Pasos siguientes

Añada el método de autenticación a la política de acceso predeterminada. Navegue a **Administración > Administración de directorios > Políticas** y haga clic en **Editar política predeterminada** para editar las reglas de la política predeterminada con objeto de añadir el método de autenticación de Kerberos a la regla en el orden de autenticación correcto.

Configurar Internet Explorer para acceder a la interfaz web

Debe configurar Internet Explorer si Kerberos está configurado para la implementación y si desea conceder a los usuarios acceso a la interfaz web mediante Internet Explorer.

La autenticación de Kerberos opera conjuntamente con Directories Management en sistemas operativos Windows.

Nota No implemente estos pasos relacionados con Kerberos en otros sistemas operativos.

Requisitos previos

Configure Internet Explorer para cada usuario o envíe las instrucciones a los usuarios después de configurar Kerberos.

Procedimiento

- 1** Compruebe que ha iniciado sesión en Windows como usuario del dominio.
- 2** En Internet Explorer, habilite el inicio de sesión automático.
 - a Seleccione **Herramientas > Opciones de Internet > Seguridad**.
 - b Haga clic en **Nivel personalizado**.
 - c Seleccione **Inicio de sesión automático solo en la zona Intranet**.
 - d Haga clic en **Aceptar**.

- 3 Compruebe que esta instancia del dispositivo virtual del conector forma parte de la zona intranet local.
 - a Use Internet Explorer para acceder a la URL de inicio de sesión de Directories Management en *https://myconnectorhost.domain/authenticate/*.
 - b Busque la zona en la esquina inferior derecha de la barra de estado de la ventana del explorador.

Si la zona es Intranet local, se ha completado la configuración de Internet Explorer.
- 4 Si la zona no es Intranet local, añada la URL de inicio de sesión de Directories Management a la zona intranet.
 - a Seleccione **Herramientas > Opciones de Internet > Seguridad > Intranet local > Sitios**.
 - b Seleccione **Detectar redes intranet automáticamente**.

Si esta opción no estaba seleccionada, selecciónela para añadir el a la zona intranet.
 - c (Opcional) Si seleccionó **Detectar redes intranet automáticamente**, haga clic en **Aceptar** hasta que se cierren todos los cuadros de diálogo.
 - d En el cuadro de diálogo Intranet local, haga clic en **Opciones avanzadas**.

Aparece un segundo cuadro de diálogo denominado Intranet local.
 - e Escriba la URL de Directories Management en el cuadro de texto **Agregar este sitio web a la zona de**.

https://myconnectorhost.domain/authenticate/
 - f Haga clic en **Agregar > Cerrar > Aceptar**.
- 5 Compruebe que Internet Explorer tiene permiso para enviar la autenticación de Windows al sitio de confianza.
 - a En el cuadro de diálogo Opciones de Internet, haga clic en la pestaña **Opciones avanzadas**.
 - b Seleccione **Habilitar autenticación integrada de Windows**.

Esta opción solo surtirá efecto tras reiniciar Internet Explorer.
 - c Haga clic en **Aceptar**.
- 6 Inicie sesión en la interfaz web para comprobar el acceso.

Si la autenticación de Kerberos se realizó correctamente, la URL de prueba abre la interfaz web.

Resultados

El protocolo Kerberos protege todas las interacciones entre esta instancia de Internet Explorer y Directories Management. Ahora, los usuarios podrán usar Single Sign-On para acceder al portal Mis apps.

Configurar Firefox para el acceso a la interfaz web

Si configura Kerberos para su implementación y desea conceder a los usuarios acceso a la interfaz web mediante Firefox, deberá configurar el explorador Firefox.

La autenticación de Kerberos opera conjuntamente con Directories Management en sistemas operativos Windows.

Requisitos previos

Una vez que haya configurado Kerberos, configure el explorador Firefox para cada usuario o bien proporcione las instrucciones correspondientes a los usuarios.

Procedimiento

- 1 En el cuadro de texto de la dirección URL del explorador Firefox, escriba `about:config` para acceder a la configuración avanzada.
- 2 Haga clic en **¡Tendré cuidado, lo prometo!**
- 3 Haga doble clic en **network.negotiate-auth.trusted-uris** en la columna Nombre de la preferencia.
- 4 Escriba la dirección URL de Directories Management en el cuadro de texto.
`https://hostdemiconector.dominio.com`
- 5 Haga clic en **Aceptar**.
- 6 Haga doble clic en **network.negotiate-auth.delegation-uris** en la columna Nombre de la preferencia.
- 7 Escriba la dirección URL de Directories Management en el cuadro de texto.
`https://hostdemiconector.dominio.com/authenticate/`
- 8 Haga clic en **Aceptar**.
- 9 Utilice el explorador Firefox para iniciar sesión en la dirección URL de inicio de sesión de y comprobar así la funcionalidad de Kerberos. Por ejemplo, *`https://hostdemiconector.dominio.com/authenticate/`*.

Si la autenticación de Kerberos funciona correctamente, la dirección URL de prueba accederá a la interfaz web.

Resultados

El protocolo Kerberos protege cualquier interacción entre la instancia en cuestión del explorador Firefox y Directories Management. Ahora, los usuarios ya podrán utilizar Single Sign-On para acceder a su portal Mis apps.

Configurar el explorador Chrome para acceder a la interfaz web

Si configura Kerberos para su implementación y desea conceder a los usuarios acceso a la interfaz web mediante el explorador Chrome, deberá configurar el explorador Chrome.

La autenticación de Kerberos opera conjuntamente con Directories Management en sistemas operativos Windows.

Nota No implemente estos pasos relacionados con Kerberos en otros sistemas operativos.

Requisitos previos

- Configure Kerberos.
- Dado que Chrome utiliza la configuración de Internet Explorer para habilitar la autenticación de Kerberos, deberá configurar Internet Explorer para que permita a Chrome utilizar la configuración de Internet Explorer. Consulte la documentación de Google para obtener información sobre cómo configurar Chrome para la autenticación de Kerberos.

Procedimiento

- 1 Utilice el explorador Chrome para comprobar la funcionalidad de Kerberos.
- 2 Inicie sesión en Directories Management en la dirección *https://myconnectorhost.domain.com/authenticate/*.

Si la autenticación de Kerberos funciona correctamente, la dirección URL de prueba se conectará a la interfaz web.

Resultados

Si todas las configuraciones de Kerberos relacionadas son correctas, el protocolo relativo (Kerberos) protegerá cualquier interacción entre la instancia en cuestión del explorador Chrome y Directories Management. Los usuarios ya podrán utilizar Single Sign-On para acceder a su portal Mis apps.

Actualizar conectores externos para Administración de directorios

Si utiliza un conector externo con la configuración de Administración de directorios de vRealize Automation, puede que deba actualizar ese conector de vez en cuando.

Puede que deba actualizar un conector externo cuando actualice la versión de su implementación de vRealize Automation o si una nueva compilación de un conector ofrece una función que le interesa.

Esta documentación solo afecta a usuarios que han implementado dispositivos conectores externos independientes adicionales. En vRealize Automation, los dispositivos conectores externos se utilizan con autenticación de tarjeta inteligente, por ejemplo.

De forma predeterminada, el conector utiliza el sitio web de VMware para el procedimiento de actualización y, para ello, es necesario que el dispositivo del conector tenga conexión a Internet. También se debe configurar el servidor proxy para el dispositivo del conector, si corresponde.

Si la instancia del conector no dispone de conexión a Internet, se puede realizar la actualización sin conexión. Para realizar una actualización sin conexión, se debe descargar el paquete de actualización y configurar un servidor web local para alojar el archivo de actualización.

Público objetivo

Esta información va dirigida a las personas que instalan, actualizan y configuran Administración de directorios. La información está escrita para administradores de sistemas Windows o Linux con experiencia y que estén familiarizados con la tecnología de máquinas virtuales.

Preparativos para actualizar un conector externo

Para preparar la actualización de un conector, debe comprobar si existen actualizaciones disponibles y configurar los ajustes del servidor proxy del dispositivo, según corresponda.

■ [Comprobar en línea la disponibilidad de una actualización de un conector externo](#)

Si su dispositivo conector tiene conexión a Internet, puede comprobar la disponibilidad de actualizaciones en línea desde el dispositivo.

■ [Configurar las opciones del servidor proxy para el dispositivo conector externo](#)

El dispositivo conector accede a los servidores de actualización de VMware a través de Internet. Si su configuración de red proporciona acceso a Internet con un proxy HTTP, debe modificar la configuración del dispositivo.

Comprobar en línea la disponibilidad de una actualización de un conector externo

Si su dispositivo conector tiene conexión a Internet, puede comprobar la disponibilidad de actualizaciones en línea desde el dispositivo.

Procedimiento

1 Inicie sesión en el dispositivo conector como usuario raíz.

2 Ejecute el siguiente comando.

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

3 Ejecute el comando siguiente para comprobar si existe una actualización en línea.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

Configurar las opciones del servidor proxy para el dispositivo conector externo

El dispositivo conector accede a los servidores de actualización de VMware a través de Internet. Si su configuración de red proporciona acceso a Internet con un proxy HTTP, debe modificar la configuración del dispositivo.

Habilite su proxy para gestionar solo el tráfico de Internet. Para garantizar que el proxy se configura correctamente, establezca el parámetro del tráfico interno en la opción sin proxy en el dominio.

Nota Los servidores proxy que requieren autenticación no son compatibles.

Requisitos previos

- Compruebe que dispone de la contraseña raíz del dispositivo conector.
- Compruebe que dispone de la información del servidor proxy.

Procedimiento

- 1 Inicie sesión en el dispositivo conector como usuario raíz.
- 2 Introduzca YaST en la línea de comandos para ejecutar la utilidad YaST.
- 3 En el panel izquierdo, seleccione **Servicios de red** y, a continuación, **Proxy**.
- 4 Introduzca las URL del servidor proxy en los campos de **URL del proxy HTTP** y **URL del proxy HTTPS**.
- 5 Seleccione **Finalizar** y salga de la utilidad YaST.
- 6 Reinicie el servidor Tomcat en el dispositivo virtual conector para utilizar la nueva configuración del proxy.

```
service horizon-workspace restart
```

Resultados

Los servidores de actualización de VMware ya están disponibles para el dispositivo conector.

Actualizar un conector externo en línea

Si tiene una conexión apropiada, puede actualizar en línea un conector externo de Administración de directorios.

Requisitos previos

- Verifique que el dispositivo conector pueda resolver y acceder a la dirección `vapp-updates.vmware.com` en el puerto 80 mediante HTTP.
- Confirme que existe una actualización del conector. Ejecute el comando correspondiente para comprobar si hay actualizaciones. Consulte Comprobar la disponibilidad de una actualización en línea de un conector de Directories Management.
- Compruebe que dispone de al menos 2 GB de espacio en el disco en la partición raíz primaria del dispositivo.
- Compruebe que el conector está configurado correctamente.
- Realice una snapshot del dispositivo conector como copia de seguridad. Para obtener información sobre cómo realizar snapshots, consulte la documentación de vSphere.
- Si para el acceso HTTP saliente se necesita un servidor proxy HTTP, configure los valores del servidor proxy para el dispositivo conector. Consulte Configurar las opciones del servidor proxy para el dispositivo conector de Directories Management.

Procedimiento

- 1 Inicie sesión en el dispositivo conector como usuario raíz.

- 2 Ejecute el siguiente comando.

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

- 3 Ejecute el comando siguiente para comprobar si existe una actualización en línea.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- 4 Ejecute el comando siguiente para actualizar el dispositivo.

```
/usr/local/horizon/update/updatemgr.hznupdate
```

Los mensajes que se generen durante la actualización se guardan en el archivo `update.log` en `/opt/vmware/var/log/update.log`.

- 5 Vuelva a ejecutar el comando `updatemgr.hzn check` para comprobar que no existe ninguna actualización más reciente.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- 6 Compruebe la versión del dispositivo actualizado.

```
vamicli version --appliance
```

Se mostrará la nueva versión.

- 7 Reinicie el dispositivo conector.

```
reboot
```

Actualizar sin conexión un conector externo

Si el dispositivo conector de Administración de directorios de vRealize Automation existente no se puede conectar a Internet para realizar la actualización, puede ejecutarla sin conexión. Se debe configurar un directorio de actualización en un servidor web local y configurar el dispositivo conector para utilizarlo para la actualización.

Requisitos previos

- Confirme que existe una actualización del conector. Compruebe si hay actualizaciones en el sitio de descargas de My VMware en my.vmware.com.
- Compruebe que dispone de al menos 2 GB de espacio en el disco en la partición raíz primaria del dispositivo.
- Compruebe que el conector está configurado correctamente.

- Realice una snapshot del dispositivo conector como copia de seguridad. Para obtener información sobre cómo realizar snapshots, consulte la documentación de vSphere.
- Configure el dispositivo conector para usar un servidor web local que aloje el archivo de actualización. Consulte Preparar un servidor web local para la actualización sin conexión.

Procedimiento

1 Preparar un servidor web local para la actualización sin conexión

Antes de iniciar la actualización del conector sin conexión, se debe preparar el servidor web local creando una estructura de directorios que incluya un subdirectorio para el dispositivo conector.

2 Configurar el conector y realizar una actualización sin conexión

Configure el dispositivo conector para indicarle al servidor web local que realice una actualización sin conexión. A continuación, actualice el dispositivo.

Preparar un servidor web local para la actualización sin conexión

Antes de iniciar la actualización del conector sin conexión, se debe preparar el servidor web local creando una estructura de directorios que incluya un subdirectorio para el dispositivo conector.

Requisitos previos

- Descargue el archivo `identity-manager-connector-versionNumber-buildNumber-updaterepo.zip` desde My VMware. Acceda a my.vmware.com, diríjase a la página de descargas de VMware Identity Manager y descargue el archivo que aparece en la lista de la sección **Paquete de actualización sin conexión del conector de VMware Identity Manager**.
- Si utiliza un servidor web IIS, configúrelo para que admita caracteres especiales en los nombres de archivo. Para ello, acceda a la sección **Filtrado de solicitudes** y seleccione la opción **Permitir doble escape**.

Procedimiento

- 1 Cree un directorio en el servidor web en `http://SuServidorWeb/VM/` y copie en él el archivo descargado.

- 2 Verifique que el servidor web incluya los tipos mime para `.sig` (texto/simple) y `.sha256` (texto/simple).

Si estos tipos de mime, el servidor no podrá comprobar si hay actualizaciones.

- 3 Descomprima el archivo.

El contenido extraído del archivo ZIP será proporcionado por `http://SuServidorWeb/VM/`.

El contenido extraído del archivo contiene los siguientes subdirectorios `/manifest` y `/package-pool`.

- 4 Ejecute el comando siguiente `updatelocal.hzn` para comprobar que en la URL hay contenido de actualización válido.

```
/usr/local/horizon/update/updatelocal.hzn checkurl http://YourWebServer/VM
```

Configurar el conector y realizar una actualización sin conexión

Configure el dispositivo conector para indicarle al servidor web local que realice una actualización sin conexión. A continuación, actualice el dispositivo.

Requisitos previos

Prepare un servidor web local para la actualización sin conexión.

Procedimiento

- 1 Inicie sesión en el dispositivo conector como usuario raíz.
- 2 Ejecute el siguiente comando para configurar un repositorio de actualización que utilice un servidor web local.

```
/usr/local/horizon/update/updatelocal.hzn seturl http://YourWebServer/VM/
```

Nota Para deshacer los cambios de la configuración y restablecer la opción de realizar una actualización en línea, puede ejecutar el siguiente comando.

```
/usr/local/horizon/update/updatelocal.hzn setdefault
```

- 3 Realice la actualización.

- a Ejecute el siguiente comando.

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

- b Ejecute el comando siguiente para comprobar la versión de la actualización disponible.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- c Ejecute el comando siguiente para actualizar el conector.

```
/usr/local/horizon/update/updatemgr.hznupdate
```

Los mensajes que se generen durante la actualización se guardan en el archivo `update.log` en `/opt/vmware/var/log/update.log`.

- d Vuelva a ejecutar el comando `updatemgr.hzn check`.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- e Compruebe la versión del dispositivo actualizado.

```
vamcli version --appliance
```

El comando debe mostrar la nueva versión.

- f Reinicie el dispositivo conector.

Por ejemplo, desde la línea del comando, ejecute el siguiente comando.

```
reboot
```

Resultados

Se completó la actualización del conector.

Ajustar la configuración después de actualizar un conector externo

Después de actualizar al conector 2016.3.1.0 o posterior, puede que tenga que configurar algunas opciones.

Volver a acceder a un dominio con autenticación Kerberos

Si utiliza directorios de Active Directory (Autenticación de Windows integrada) o autenticación Kerberos, debe abandonar el dominio y, a continuación, volver a acceder a él. Este paso es obligatorio para todos los dispositivos virtuales conectores de su implementación.

- 1 Seleccione **Administración > Administración de directorios > Conectores**.
- 2 En la página Conectores, haga clic en **Dejar el dominio** en cada conector que se está utilizando en el directorio de Active Directory (Autenticación de Windows integrada) o la autenticación Kerberos.
- 3 Para unirse al dominio, necesita las credenciales de Active Directory con los privilegios para unirse. Consulte [Unir una máquina de conector a un dominio](#) para obtener más información.
- 4 Si utiliza la autenticación de Kerberos, vuelva a habilitar el adaptador de esta autenticación. Para acceder a la página Adaptadores de autenticación, haga clic en el vínculo adecuado en la columna **Trabajo** y seleccione la pestaña **Adaptadores de autenticación** en la página Conectores.
- 5 Compruebe que el resto de adaptadores de autenticación que está utilizando están habilitados.

Actualizar la página Dominios

Si utiliza Active Directory (Autenticación de Windows integrada) o Active Directory en LDAP con la opción **Este directorio admite la ubicación de servicio de DNS** activada, guarde la página Dominios del directorio.

- 1 Seleccione **Administración > Administración de directorios > Directorios**.
- 2 Seleccione el directorio aplicable para editarlo.

- 3 Proporcione la contraseña del usuario de DN de enlace y haga clic en **Guardar**.
- 4 Haga clic en **Configuración de sincronización** en la parte izquierda de la página y seleccione la pestaña **Dominios**.
- 5 Haga clic en **Guardar**.

Ubicación del servicio de DNS y controladores de dominio

Nota En la versión 2016.3.1.0 o versiones posteriores del conector, se crea automáticamente un archivo `domain_krb.properties` que se rellena de forma automática con controladores de dominio cuando se crea un directorio con la ubicación del servicio DNS habilitada. Cuando guarda la página Dominios tras realizar la actualización, si disponía de un archivo `domain_krb.properties` en su implementación original, el archivo se actualiza con los dominios que pudo agregar posteriormente y que no se encontraban en el archivo. Si no disponía de un archivo `domain_krb.properties` en su implementación original, se creará y rellenará de forma automática con controladores de dominio. Consulte [Acerca de la selección de controladoras de dominio](#) para obtener más información sobre el archivo `domain_krb.properties`.

Solucionar problemas de actualización de conectores externos

Para solucionar los problemas de actualización de los conectores externos de Administración de directorios de vRA, revise los logs de errores. Si el conector no se inicia, se puede restaurar una instancia anterior a partir de una snapshot.

- [Consultar los registros de errores de la actualización](#)
Revise los registros de errores ocurridos durante la actualización para resolverlos. Los archivos de registro de la actualización están en el directorio `/opt/vmware/var/log`.
- [Restaurar snapshots del conector](#)
Si el conector no se inicia correctamente después de una actualización y, además, no puede resolverse el problema revisando los logs de errores de actualización y ejecutando el comando de actualización de nuevo, es posible revertir a una instancia previa del conector.
- [Recopilar un paquete de archivos de registro](#)
Puede recopilar un paquete de archivos de registro para enviárselo al equipo de soporte técnico de VMware. El paquete se obtiene de la página de configuración del conector.

Consultar los registros de errores de la actualización

Revise los registros de errores ocurridos durante la actualización para resolverlos. Los archivos de registro de la actualización están en el directorio `/opt/vmware/var/log`.

Si se produjera algún error, puede que el conector no se inicie después de la actualización.

Procedimiento

- 1 Inicie sesión en el dispositivo del conector.
- 2 Acceda al directorio `/opt/vmware/var/log`.

- 3 Abra el archivo `update.log` y revise los mensajes de error.
- 4 Resuelva los errores y vuelva a ejecutar el comando de actualización. El comando de actualización continuará desde el punto en que se detuvo.

Nota También puede revertir a una snapshot y ejecutar de nuevo la actualización.

Restaurar snapshots del conector

Si el conector no se inicia correctamente después de una actualización y, además, no puede resolverse el problema revisando los logs de errores de actualización y ejecutando el comando de actualización de nuevo, es posible revertir a una instancia previa del conector.

Procedimiento

- ◆ Realice la restauración utilizando una de las snapshots realizadas como copia de seguridad de la instancia original del conector. Para obtener información, consulte la documentación de vSphere.

Recopilar un paquete de archivos de registro

Puede recopilar un paquete de archivos de registro para enviárselo al equipo de soporte técnico de VMware. El paquete se obtiene de la página de configuración del conector.

El paquete incluye los siguientes archivos de registro.

Tabla 2-9. Archivos de registro

Componente	Ubicación del archivo de registro	Descripción
Registros de Apache Tomcat (catalina.log)	/opt/vmware/horizon/workspace/logs/catalina.log	Apache Tomcat registra los mensajes que no se registran en otros archivos de registro.
Registros del configurador (configurator.log)	/opt/vmware/horizon/workspace/logs/configurator.log	Solicitudes que recibe el configurador del cliente REST y de la interfaz web.
Registros del conector (connector.log)	/opt/vmware/horizon/workspace/logs/connector.log	Un registro de cada solicitud recibida desde la interfaz web. Cada entrada del registro incluye también la URL, la marca de hora y las excepciones de la solicitud. No se registra ninguna acción de sincronización.

Procedimiento

- 1 Inicie la sesión en la página de configuración del conector en <https://connectorURL:8443/cfg/logs>.
- 2 Haga clic en **Preparar paquete de registro**.
- 3 Descargue el paquete y envíelo al equipo de soporte técnico de VMware.

Escenario: Configurar un vínculo de Active Directory para vRealize Automation de alta disponibilidad

Como administrador de tenant, desea configurar una conexión de directorio de Active Directory en LDAP para admitir la autenticación de usuarios para la implementación de vRealize Automation de alta disponibilidad.

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

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

Requisitos previos

- Instale una implementación de vRealize Automation distribuida con los equilibradores de carga adecuados. Consulte *Instalación de vRealize Automation*.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Directorios**.
- 2 Haga clic en **Añadir directorio**.
- 3 Escriba su configuración de cuenta específica de Active Directory y acepte las opciones predeterminadas.

Opción	Entrada de muestra
Nombre de directorio	Añada la dirección IP del nombre de dominio de Active Directory.
Conector de sincronización	Cada dispositivo de vRealize Automation contiene un conector. Use cualquiera de los conectores que hay disponibles.
DN de la base	Escriba el nombre distintivo (DN) del punto de inicio de las búsquedas en el servidor de directorios. Por ejemplo, cn=users,dc=corp,dc=local .

Opción	Entrada de muestra
DN de enlace	Escriba el nombre distintivo (DN) completo, incluido el nombre común (CN), de una cuenta de usuario de Active Directory que tenga privilegios para buscar usuarios. Por ejemplo, cn=config_admin infra,cn=users,dc=corp,dc=local.
Contraseña de DN de enlace	Escriba la contraseña de Active Directory para la cuenta que puede buscar usuarios.

- 4 Haga clic en **Probar conexión** para probar la conexión al directorio configurado.
Si la conexión no es correcta, compruebe los valores que ha introducido en todos los campos y, en caso necesario, consulte al administrador del sistema.
- 5 Haga clic en **Guardar y Siguiente**.
Aparece la página de selección de dominios, que contiene una lista de dominios.
- 6 Deje seleccionado el dominio predeterminado y haga clic en **Siguiente**.
- 7 Compruebe que los nombres de atributo estén asignados a los atributos de Active Directory correctos. Si no es así, seleccione el atributo de Active Directory correcto en el menú desplegable. Haga clic en **Siguiente**.
- 8 Seleccione los grupos y los usuarios que desea sincronizar.
 - a Haga clic en el icono **Añadir** (+).
 - b Escriba el dominio de usuario y haga clic en **Buscar grupos**.
Por ejemplo, **cn=users,dc=corp,dc=local**.
 - c Active la casilla **Seleccionar todo**.
 - d Haga clic en **Seleccionar**.
 - e Haga clic en **Siguiente**.
 - f Haga clic en **+** para añadir más usuarios. Por ejemplo, escriba **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.
Para excluir usuarios, haga clic en **+** para crear un filtro que excluya a algunos tipos de usuarios. Debe seleccionar el atributo de usuario por el que desea filtrar, la regla de consulta y el valor.
 - g Haga clic en **Siguiente**.
- 9 Revise la página para ver cuántos usuarios y grupos se han sincronizado en el directorio y haga clic en **Sincronizar directorio**.
El proceso de sincronización del directorio tarda un poco pero se ejecuta en segundo plano, lo que le permite seguir trabajando.

10 Configure un segundo conector para admitir la alta disponibilidad.

- a Inicie sesión en el equilibrador de carga de la implementación de vRealize Automation como administrador de tenants.

La URL del equilibrador de carga es *dirección de equilibrador de carga/vcac/org/nombre de tenant*.

- b Seleccione **Administración > Administración de directorios > Proveedores de identidades**.
- c Haga clic en el proveedor de identidades que está en uso en su sistema actualmente.
Se muestran el directorio y el conector existentes responsables de la administración de identidades básica en el sistema.
- d Haga clic en la lista desplegable **Añadir conector** y seleccione el conector que corresponda al dispositivo de vRealize Automation secundario.
- e Escriba la contraseña adecuada en el cuadro de texto **Enlazar contraseña de DN** que aparece al seleccionar el conector.
- f Haga clic en **Añadir conector**.
- g Edite el nombre de host para que apunte al equilibrador de carga.

Resultados

Previamente conectó el Active Directory corporativo a vRealize Automation y configuró la administración de directorios para la alta disponibilidad.

Pasos siguientes

Para proporcionar una mayor seguridad, puede configurar una confianza bidireccional entre el proveedor de identidades y Active Directory. Consulte [Configurar una relación de confianza bidireccional entre vRealize Automation y Active Directory](#).

Configurar conectores externos para la autenticación del proveedor de identidades de terceros y la tarjeta inteligente en vRealize Automation

Un administrador del sistema debe configurar un conector externo para la implementación de vRealize Automation mediante la administración de directorios si usa proveedores de identidades de terceros, como la autenticación Kerberos o de tarjetas inteligentes.

La administración de directorios admite varios proveedores de identidades y clústeres de conectores para cada Active Directory configurado. Para usar la autenticación de tarjetas inteligentes o de proveedor de identidades, puede configurar un solo conector externo o un clúster de conectores con un proveedor de identidades apropiado tras un equilibrador de carga que admita acceso directo a SSL. Consulte [Administración de conectores y clústeres de conectores](#) para obtener más información.

Consulte [Actualizar conectores externos para Administración de directorios](#) para obtener información sobre cómo se actualiza un conector externo.

Hay varias opciones de configuración de certificado disponibles para usar con la autenticación de tarjetas inteligentes. Consulte [Configurar un certificado o adaptador de tarjeta inteligente para utilizarlo con Directories Management](#).

Requisitos previos

- Configure una conexión de Active Directory apropiada para usarla con la implementación de vRealize Automation.
- Descargue el archivo OVA necesario para configurar un conector de [Herramientas y SDK de VMware vRealize Automation](#).
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

1 [Generar un token de activación del conector](#)

Antes de implementar el dispositivo virtual del conector para usarlo en la autenticación de tarjetas inteligentes, genere un código de activación para el nuevo conector desde la consola de vRealize Automation. El código de activación se usa para establecer la comunicación entre la administración de directorios y el conector.

2 [Implementar el archivo OVA del conector](#)

Tras descargar un archivo OVA del conector, puede implementarlo mediante VMware vSphere Client o vSphere Web Client.

3 [Configurar los ajustes del conector](#)

Tras implementar el archivo OVA del conector, debe ejecutar el asistente de configuración para activar el dispositivo y configurar las contraseñas de administrador.

4 [Aplicar la entidad de certificación pública](#)

Cuando se instala la administración de directorios, se genera un certificado SSL predeterminado. Puede usar el certificado predeterminado con propósitos de prueba, pero debería generar e instalar certificados SSL comerciales para los entornos de producción.

5 [Crear un proveedor de identidades de área de trabajo](#)

Debe crear un proveedor de identidades de área de trabajo para usarlo con un conector externo.

6 [Configurar la autenticación mediante certificado y las reglas de la política de acceso predeterminada](#)

Debe configurar el conector externo para usarlo con el dominio y Active Directory de vRealize Automation.

Generar un token de activación del conector

Antes de implementar el dispositivo virtual del conector para usarlo en la autenticación de tarjetas inteligentes, genere un código de activación para el nuevo conector desde la consola de vRealize Automation. El código de activación se usa para establecer la comunicación entre la administración de directorios y el conector.

Puede configurar un solo conector o un clúster de conectores. Si desea usar un clúster de conectores, repita este procedimiento para cada conector que necesite.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Conectores**.
- 2 Escriba un nombre para el nuevo conector en el cuadro de texto **Nombre del ID de conector**.
- 3 Pulse **Intro**.
El código de activación del conector se mostrará en el cuadro **Código de activación del conector**.
- 4 Copie el código de activación para usarlo en la configuración del conector mediante el archivo OVA.

Implementar el archivo OVA del conector

Tras descargar un archivo OVA del conector, puede implementarlo mediante VMware vSphere Client o vSphere Web Client.

Implemente el archivo OVA mediante vSphere Client o vSphere Web Client.

Requisitos previos

- Identifique los registros de DNS y el nombre de host que usará la implementación del archivo OVA del conector.
- Si usa vSphere Web Client, emplee los navegadores Firefox o Chrome. No use Internet Explorer para implementar el archivo OVA.
- Descargue el archivo OVA necesario para configurar un conector de [Herramientas y SDK de VMware vRealize Automation](#).

Procedimiento

- 1 En vSphere Client o vSphere Web Client, seleccione **Archivo > Implementar plantilla de OVF**.

- 2 En las páginas para Implementar plantilla de OVF, introduzca la información específica de la implementación del conector.

Página	Descripción
Origen	Vaya a la ubicación del paquete OVA o escriba una URL determinada.
Información de la plantilla de OVA	Compruebe que ha seleccionado la versión correcta.
Licencia	Lea el Contrato de licencia para el usuario final y haga clic en Aceptar .
Nombre y ubicación	<p>Escriba un nombre para el dispositivo virtual. El nombre debe ser exclusivo en la carpeta del inventario y puede contener hasta 80 caracteres. Los nombres distinguen mayúsculas de minúsculas.</p> <p>Seleccione una ubicación para el dispositivo virtual.</p>
Host/Clúster	Seleccione el host o el clúster donde se ejecutará la plantilla implementada.
Grupo de recursos	Seleccione el grupo de recursos.
Almacenamiento	Seleccione la ubicación donde se almacenarán los archivos de las máquinas virtuales.
Formato de disco	Seleccione el formato de disco de los archivos. En el caso de entornos de producción, seleccione el formato Aprovisionamiento grueso . Use el formato Aprovisionamiento fino para la evaluación y las pruebas.
Asignación de redes	Asigne las redes del entorno a las redes de la plantilla de OVF.
Propiedades	<p>a En el campo Configuración de zona horaria, seleccione la zona horaria correcta.</p> <p>b La casilla del Programa de mejora de la experiencia del cliente está activada de forma predeterminada. VMware recopila datos anónimos acerca de la implementación para mejorar la manera en que VMware responde a las necesidades de los usuarios. Desactive la casilla si no desea que se recopilen datos.</p> <p>c En el cuadro de texto Nombre del host, escriba el nombre del host que se usará. Si se deja en blanco, se usará un DNS inverso para buscar el nombre del host.</p> <p>d Para configurar la dirección IP estática del conector, escriba una dirección para cada uno de los siguientes elementos: puerta de enlace predeterminada, DNS, dirección IP y máscara de red.</p> <p>Importante Si se deja en blanco cualquiera de los cuatro campos de dirección, incluido Nombre del host, se usará DHCP.</p> <p>Para configurar DHCP, deje los campos de dirección en blanco.</p>
Listo para completar	Revise sus selecciones y haga clic en Finalizar .

En función de la velocidad de la red, la implementación podría tardar varios minutos. Puede seguir el progreso en el cuadro de diálogo de progreso.

- 3 Cuando se complete la implementación, seleccione el dispositivo del , haga clic con el botón derecho en él y seleccione **Energía > Encender**.

El dispositivo del se inicializará. Puede ir a la pestaña **Consola** para consultar la información. Cuando finalice la inicialización del dispositivo virtual, la pantalla de la consola mostrará la versión del y las URL para iniciar sesión en el asistente de configuración del para completar la configuración.

Pasos siguientes

Use el asistente de configuración para añadir el código de activación y las contraseñas de administración.

Configurar los ajustes del conector

Tras implementar el archivo OVA del conector, debe ejecutar el asistente de configuración para activar el dispositivo y configurar las contraseñas de administrador.

Requisitos previos

- Ha generado un código de activación del conector.
- Asegúrese de que el dispositivo del conector está encendido y de que conoce la URL del conector.
- Recopile una lista de contraseñas para el administrador del conector, la cuenta raíz y la cuenta de usuario SSH.

Procedimiento

- 1 Para ejecutar el asistente de configuración, escriba la URL del conector que se encontraba en la pestaña Consola tras la implementación del archivo OVA.
- 2 En la página de bienvenida, haga clic en **Continuar**.

- 3** Cree contraseñas seguras para las siguientes cuentas de administrador del dispositivo virtual del conector.

Las contraseñas seguras deben tener ocho caracteres de longitud como mínimo y deben incluir caracteres en mayúsculas y minúsculas y al menos un número o un carácter especial.

Opción	Descripción
Administrador del dispositivo	Cree la contraseña del administrador del dispositivo. El nombre de usuario es admin y no se puede cambiar. Debe utilizar esta cuenta y esta contraseña para iniciar sesión en los servicios del conector y administrar certificados, contraseñas del dispositivo y la configuración de syslog. Importante La contraseña del usuario admin debe tener una longitud de seis caracteres como mínimo.
Cuenta raíz	Se ha usado una contraseña raíz de VMware predeterminada para instalar el dispositivo del conector. Cree una contraseña raíz nueva.
Cuenta del usuario SSH	Cree la contraseña que se usará para acceder de forma remota al dispositivo del conector.

- 4** Haga clic en **Continuar**.
- 5** En la página de activación del conector, pegue el código de activación y haga clic en **Continuar**.
- 6** Si utiliza un certificado autofirmado en el conector interno de vRealize Automation, puede obtener el certificado adecuado ejecutando el comando siguiente en el dispositivo de vRealize Automation: `cat /etc/apache2/server-cert.pem`.

Seleccione la pestaña **Finalizar SSL en un equilibrador de carga** y, a continuación, haga clic en el vínculo de `/horizon_workspace_rootca.pem`.

Se comprobará el código de activación y se establecerá la comunicación entre el servicio y la instancia del conector para completar la configuración del conector.

Pasos siguientes

En el servicio, configure el entorno en función de sus necesidades. Por ejemplo, si ha añadido un conector adicional debido a que dese sincronizar dos directorios de autenticación integrada de Windows, cree el directorio y asócielo al nuevo conector.

Aplicar la entidad de certificación pública

Cuando se instala la administración de directorios, se genera un certificado SSL predeterminado. Puede usar el certificado predeterminado con propósitos de prueba, pero debería generar e instalar certificados SSL comerciales para los entornos de producción.

Si la administración de directorios apunta a un equilibrador de carga, a este se le aplica el certificado SSL.

Debe activar la opción **Marcar esta clave como exportable** al importar un certificado.

Solo debe especificar el CN o el nombre de dominio del sitio de la entidad de certificación si desea generar un CSR para un certificado personalizado.

Requisitos previos

Genere una solicitud de firma de certificado (CSR) y obtenga un certificado válido y firmado de una CA. Si la organización proporciona certificados SSL firmados por una CA, puede usar dichos certificados. El certificado debe tener el formato PEM.

Procedimiento

- 1 Inicie sesión en la página de administración del dispositivo del conector como usuario administrador en la siguiente ubicación:
`https://myconnector.mycompany:8443/cfg`
- 2 En la consola del administrador, haga clic en **Configuración del dispositivo**.
La configuración del dispositivo virtual se selecciona de forma predeterminada.
- 3 Haga clic en **Administrar configuraciones**.
- 4 Introduzca la contraseña del usuario administrador del servidor de VMware Identity Manager.
- 5 Seleccione **Instalar certificado**.
- 6 En la pestaña Finalizar SSL en el dispositivo de **Identity Manager Appliance**, seleccione **Certificado personalizado**.
- 7 En el cuadro de texto **Cadena de certificados SSL**, pegue los certificados host, intermedio y raíz, en este mismo orden.

El certificado SSL solo funciona si se incluye la cadena de certificados completa en el orden correcto. Para cada certificado, copie todo el contenido que se encuentre entre las líneas -----BEGIN CERTIFICATE----- y -----END CERTIFICATE-----, ambas incluidas.

Asegúrese de que el certificado contiene el nombre de host de FQDN.
- 8 Pegue la clave privada en el cuadro de texto Clave privada. Copie todo el contenido que haya entre -----BEGIN RSA PRIVATE KEY----- y -----END RSA PRIVATE KEY-----.
- 9 Haga clic en **Guardar**.

Ejemplo: Ejemplos de certificados

Ejemplo de cadena de certificados

```
-----BEGIN CERTIFICATE-----
jIQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+
...
...
W53+O05j5xsxzDJfWr1qBIFf/OkIYCPcyK1
-----END CERTIFICATE-----
```

Ejemplo de cadena de certificados

```
-----BEGIN CERTIFICATE-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjIQvt90+
...
...
O05j5xsxzDJfWr1lqBIFF/OkiYCPW53+cyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
dR9Vpg3WQTjIQvt9W5+C3HU17bUOwvhp/r0+
...
...
5j5xsxzDJfWr1lqW53+O0BIFF/OkiYCPcyK1
-----END CERTIFICATE-----
```

Ejemplo de clave privada

```
-----BEGIN RSA PRIVATE KEY-----
jIQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+
...
...
1lqBIFFW53+O05j5xsxzDJfWr/OkiYCPcyK1
-----END RSA PRIVATE KEY-----
```

Crear un proveedor de identidades de área de trabajo

Debe crear un proveedor de identidades de área de trabajo para usarlo con un conector externo.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Proveedores de identidades**.
- 2 Seleccione **Añadir proveedor de identidades**.
- 3 Seleccione **Crear proveedor de identidades de área de trabajo** en el menú que se muestra.
- 4 Escriba un nombre para el proveedor de identidades en el campo **Nombre de proveedor de identidades**.

- 5 Seleccione el directorio que corresponda a los usuarios que utilizarán este proveedor de identidades.

El directorio seleccionado determina los conectores que se mostrarán para su selección en este proveedor de identidades.

- 6 Seleccione el conector o los conectores externos que haya configurado para la autenticación de tarjetas inteligentes.

Nota Si la implementación se encuentra tras un equilibrador de carga, escriba la URL de este.

- 7 Seleccione la red para acceder a este proveedor de identidades.

- 8 Haga clic en **Agregar**.

Configurar la autenticación mediante certificado y las reglas de la política de acceso predeterminada

Debe configurar el conector externo para usarlo con el dominio y Active Directory de vRealize Automation.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Conectores**.

- 2 Seleccione el conector que desee en la columna **Trabajo**.

El trabajo seleccionado se muestra en el cuadro de texto **Nombre de trabajo** de la pestaña **Detalles** del conector y la información sobre el tipo de conector aparece en el cuadro de texto **Tipo de conector**.

- 3 Asegúrese de que el conector está vinculado con el Active Directory que desee indicando dicho directorio en el cuadro de texto **Directorio asociado**.

- 4 Escriba el nombre de dominio apropiado en el cuadro de texto **Dominios asociados**.

- 5 Seleccione la pestaña **AuthAdapters** y habilite CertificateAuthAdapter.

- 6 Configure la autenticación mediante certificado según corresponda a su implementación.

Consulte [Configurar la autenticación mediante certificado para la administración de directorios](#).

- 7 Seleccione **Administración > Administración de directorios > Políticas**.

- 8 Haga clic en **Editar política predeterminada**.

- 9 Añada el certificado a las reglas de la política y establézcalo como primer método de autenticación.

El certificado debe ser el primer método de autenticación indicado en la regla de la política para que no se produzca ningún error en la autenticación mediante certificado.

Crear un vínculo de Active Directory con varios dominios o bosques

Como administrador del sistema, necesita configurar un vínculo de Active Directory con varios dominios o bosques.

El procedimiento para configurar un vínculo de Active Directory con varios dominios o bosques es esencialmente el mismo. Para un vínculo de varios bosques, se requiere una confianza bidireccional entre todos los dominios aplicables.

Requisitos previos

- Instale una implementación de vRealize Automation distribuida con los equilibradores de carga adecuados. Consulte *Instalación de vRealize Automation*.
- Inicie sesión en vRealize Automation como **administrador de tenants**.
- Configure los dominios adecuados y los bosques de Active Directory para su implementación.

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Directorios**.
- 2 Haga clic en **Añadir directorio**.
- 3 En la página Añadir directorio, especifique un nombre para el servidor de Active Directory en el cuadro de texto **Nombre del directorio**.
- 4 Seleccione **Active Directory (autenticación integrada de Windows)** bajo el encabezado **Nombre del directorio**.
- 5 Configure el conector que sincroniza usuarios desde Active Directory hacia el directorio de VMware Directories Management en la sección de sincronización y autenticación del directorio.

Opción	Descripción
Conector de sincronización	Seleccione el conector apropiado que ha de usarse para su sistema. Cada Dispositivo de vRealize Automation incluye un conector predeterminado. Consulte con el administrador del sistema en el caso de que necesite ayuda para elegir el conector apropiado.
Autenticación	Haga clic en el botón de opciones apropiado para indicar si el conector seleccionado también realiza la autenticación.
Atributo de búsqueda directa	Seleccione el atributo de cuenta apropiado que contiene el nombre de usuario.

Según cuál sea la configuración de su implementación, tendrá uno o más conectores disponibles para su uso.

- 6 Escriba las credenciales de unión a dominio apropiadas en los cuadros de texto **Nombre de dominio**, **Nombre de usuario administrador del dominio** y **Contraseña del administrador del dominio**.

Como ejemplo, podría escribir algo parecido a lo siguiente: **Nombre de dominio:** hs.trcint.com, **Nombre de usuario administrador del dominio:** devadmin, **Contraseña del administrador del dominio:** xxxx.

- 7 En la sección **Detalles del usuario de enlace**, introduzca las credenciales de Active Directory (autenticación integrada de Windows) apropiadas para facilitar la sincronización de directorios.

Opción	Descripción
UPN del usuario de enlace	Escriba el nombre principal del usuario que puede autenticar con el dominio. Por ejemplo, NombreDeUsuario@ejemplo.com.
Contraseña de DN de enlace	Escriba la contraseña del usuario de enlace.

- 8 Haga clic en **Guardar y Siguiente**.

Aparece la página Seleccione los dominios con la lista de dominios.


- 9 Haga clic en las casillas de verificación adecuadas para seleccionar los dominios deseados para su implementación del sistema.

- 10 Haga clic en **Siguiente**.

- 11 Compruebe que los nombres de atributos del directorio de Directories Management estén asignados a los atributos correctos de Active Directory.

Si los nombres de atributos del directorio se asignan incorrectamente, seleccione el atributo correcto de Active Directory en el menú desplegable.


- 12 Haga clic en **Siguiente**.


- 13** Haga clic en  para seleccionar los grupos que desea sincronizar entre Active Directory y el directorio.

Cuando se añade un grupo de Active Directory, si los miembros de ese grupo no están incluidos en la lista de usuarios, entonces se añaden.

Nota El sistema de autenticación de usuarios de Directories Management importa los datos de Active Directory al añadir grupos y usuarios, y la velocidad del sistema quedará limitada por las prestaciones de Active Directory. En consecuencia, las operaciones de importación podrían tardar mucho tiempo en completarse en función del número de grupos y usuarios que se añada. Para minimizar la posibilidad de retrasos o problemas, limite el número de grupos y usuarios a únicamente los necesarios para el funcionamiento de vRealize Automation. Si el rendimiento del sistema se degrada o si se producen errores, cierre las aplicaciones que no sean necesarias y asegúrese de que su sistema tenga asignada a Active Directory la memoria adecuada. Si los problemas persisten, aumente la asignación de memoria a Active Directory según sea necesario. En el caso de sistemas con una gran cantidad de usuarios y grupos, es posible que deba aumentar la asignación de memoria a Active Directory hasta los 24 GB.

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

- 15** Haga clic en  para añadir más usuarios. Por ejemplo, escriba **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.

Para excluir a usuarios, haga clic en  para crear un filtro de exclusión de determinados tipos de usuarios. Debe seleccionar el atributo de usuario por el que desea filtrar, la regla de consulta y el valor.

- 16** Haga clic en **Siguiente**.

- 17** Revise la página para ver cuántos usuarios y grupos se han sincronizado en el directorio.

Si desea realizar cambios en los usuarios y grupos, haga clic en los vínculos Editar.

- 18** Haga clic en **Mover a Workspace** para iniciar la sincronización con el directorio.

Pasos siguientes

Configurar funciones de usuarios y grupos

Los administradores de tenants crean grupos empresariales y grupos personalizados, y conceden a los usuarios derechos de acceso a la consola de vRealize Automation.

Asignar funciones a usuarios o grupos de directorios

Los administradores de tenants conceden a los usuarios derechos de acceso mediante la asignación de funciones a usuarios o grupos.

Para permitir que los usuarios o grupos modifiquen y activen una canalización, debe asignar permisos a esos usuarios y grupos. Cuando se asigna a los usuarios y grupos la función de administrador de versiones, pueden modificar y activar la canalización. Cuando se asigna a los usuarios y grupos la función de ingeniero de versiones, pueden activar la canalización. Para obtener más información, consulte la guía *Uso de vRealize Code Stream*.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Usuarios y grupos > Usuarios y grupos de directorios**.
- 2 Escriba el nombre de un usuario o grupo en el cuadro **Buscar** y presione Entrar.
No utilice el signo de arroba (@), la barra diagonal inversa (\) ni la barra diagonal (/) en el nombre. Para optimizar la búsqueda, escriba el nombre completo del usuario o grupo con el formato usuario@dominio.
- 3 Haga clic en el nombre del usuario o grupo al que desea asignar funciones.
- 4 Seleccione una o más funciones de la lista Añadir funciones a este usuario.
La lista Autorizaciones concedidas por funciones seleccionadas indica las autorizaciones específicas que se conceden.
- 5 (opcional) Haga clic en **Siguiente** para ver más información sobre el usuario o grupo.
- 6 En la página **Detalles de usuarios**, en la pestaña **General**, desplácese por la lista de funciones para agregar el usuario.
 - a Para asignar permisos al usuario para que pueda modificar y activar una canalización, seleccione la casilla de verificación **Release Manager** (Administrador de versiones).
 - b Para asignar permisos al usuario para que pueda activar una canalización, seleccione la casilla de verificación **Release Engineer** (Ingeniero de versiones).
- 7 Haga clic en **Actualizar**.

Resultados

Los usuarios que han iniciado sesión en vRealize Automation deben cerrar la sesión de vRealize Automation y volver a iniciarla antes de poder desplazarse hasta las páginas a las que se les ha concedido acceso.

Pasos siguientes

Si lo desea, también puede crear sus propios grupos personalizados a partir de los usuarios y grupos de sus conexiones de Active Directory. Consulte [Crear un grupo personalizado](#).

Crear un grupo personalizado

Los administradores de tenant pueden crear grupos personalizados combinando otros grupos personalizados, grupos de almacén de identidades y usuarios de almacén de identidades

individuales. Los grupos personalizados proporcionan un control más granular sobre el acceso dentro de vRealize Automation que el que se tiene en los grupos empresariales que corresponden a una línea de negocios, un departamento u otra unidad organizativa.

Con los grupos personalizados se pueden conceder derechos de acceso para las tareas de una forma más precisa que las asignaciones de grupos de vRealize Automation estándar. Por ejemplo, es posible que quiera crear un grupo personalizado para permitir que los administradores de tenants controlen quién tiene permisos específicos en el tenant.

Se pueden asignar funciones a un grupo personalizado, si bien esto no es necesario en todos los casos. Por ejemplo, puede crear un grupo personalizado llamado Aprobadores de especificaciones de máquina para usarlo en todas las aprobaciones previas de máquina. También puede crear grupos personalizados para asignarlos a sus grupos empresariales y, así, poder administrar todos los grupos desde un único sitio. En ninguno de estos casos es necesario asignar funciones.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

1 Seleccione **Administración > Usuarios y grupos > Grupos personalizados**.

2 Haga clic en el icono **Añadir** (+).

3 Escriba un nombre de grupo en el cuadro de texto **Nombre de grupo nuevo**.

Los nombres de los grupos personalizados no pueden contener la combinación de punto y coma (;) seguido del signo igual (=).

4 (opcional) Escriba una descripción en el cuadro de texto **Descripción de grupo nuevo**.

5 Seleccione una o más funciones de la lista **Añadir funciones a este grupo**.

La lista **Autorizaciones concedidas por funciones seleccionadas** indica las autorizaciones específicas que se conceden.

6 Haga clic en **Siguiente**.

7 Añada usuarios y grupos para crear el grupo personalizado.

a Escriba el nombre de un usuario o grupo en el cuadro **Buscar** y presione **Entrar**.

No utilice el signo de arroba (@), la barra diagonal inversa (\) ni la barra diagonal (/) en el nombre. Para optimizar la búsqueda, escriba el nombre completo del usuario o grupo con el formato **usuario@dominio**.

b Seleccione el usuario o grupo que quiera añadir al grupo personalizado.

8 Haga clic en **Agregar**.

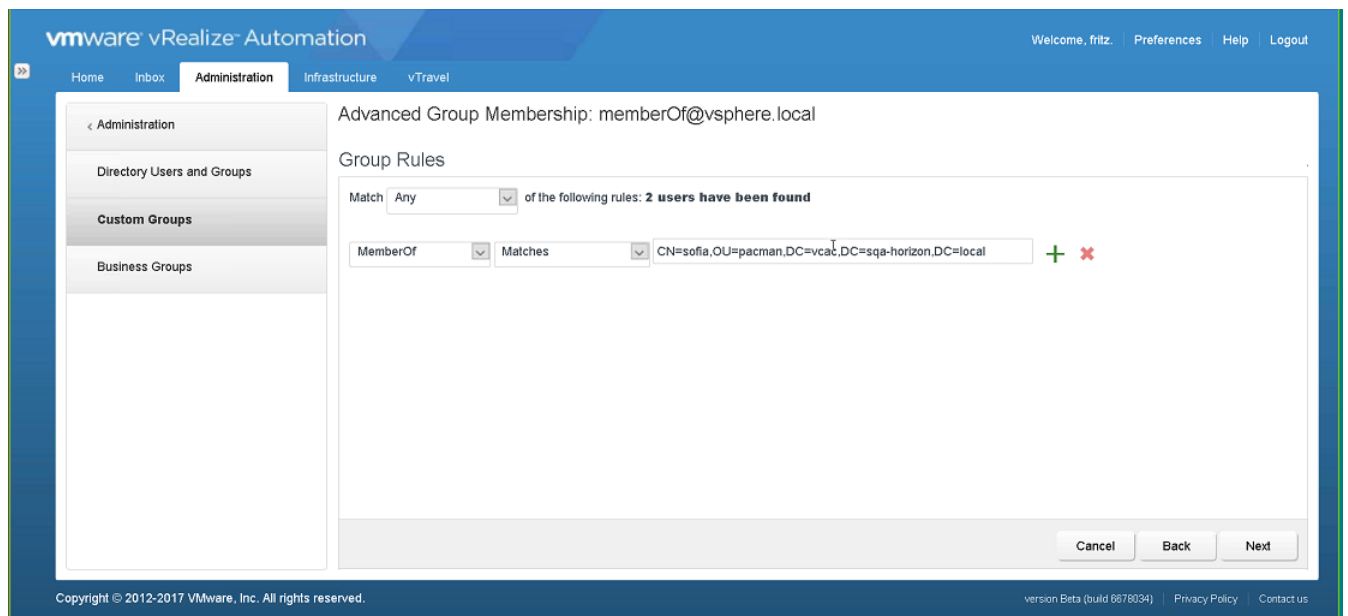
Resultados

Los usuarios que han iniciado sesión en vRealize Automation deben cerrar la sesión de vRealize Automation y volver a iniciarla antes de poder desplazarse hasta las páginas a las que se les ha concedido acceso.

Agregar usuarios de Just-in-Time con reglas y grupos personalizados

Puede agregar usuarios de vRealize Automation a una implementación sin acceso a Active Directory mediante el aprovisionamiento de usuarios de Just-in-Time. Si desea invocar el aprovisionamiento de Just-in-Time para usuarios nuevos, debe crear reglas para rellenar el grupo personalizado correspondiente.

La primera vez que inician sesión, a los usuarios de Just-in-Time se les asigna pertenencia a grupos de forma dinámica según las reglas que se crean en la página del asistente Pertenencia a grupo avanzada. Después de iniciar sesión por primera vez, puede asignar la pertenencia al grupo siguiendo el procedimiento habitual. La segunda página del asistente contiene cuatro cuadros de selección para crear reglas basadas en una serie de criterios que definen los usuarios de Just-in-Time.



Por ejemplo, en el primer cuadro de selección de regla, puede seleccionar Dominio como un criterio y, a continuación, seleccionar Coincidencias en el segundo cuadro. Después, en el tercer cuadro de regla, podrá especificar un dominio. Estas selecciones crean una regla que define los usuarios basados en pertenencia de Just-in-Time que están asociados al dominio especificado. El tercer cuadro de selección es un cuadro de entrada de forma libre y en él puede introducir cualquier información que esté relacionada lógicamente con las selecciones de los dos primeros cuadros de selección.

Nota Puede crear varias reglas para rellenar usuarios de Just-in-Time en función de diversos de criterios. Si crea varias reglas, puede utilizar el cuadro de selección de regla **Coincidencia**, el cual se encuentra sobre los cuadros de regla principales, para indicar si vRealize Automation debe coincidir con alguna de las reglas o con todas ellas al rellenar usuarios de Just-in-Time.

Procedimiento

- 1 Seleccione **Administración > Usuarios y grupos > Grupos personalizados**, y cree o busque un grupo personalizado adecuado para los usuarios de Just-in-Time.
Consulte [Crear un grupo personalizado](#) para obtener más información.
- 2 Haga clic en el botón **Pertenencia avanzada**.
Si lo desea, puede agregar usuarios individuales en la página.
- 3 Haga clic en **Siguiente** para ver la página de reglas de grupo.
- 4 En los tres cuadros de selección de regla principales que se sitúan debajo del cuadro de selección de regla **Coincidencia**, haga clic en las flechas que apuntan hacia abajo e introduzca información para activar los menús desplegables que le permiten crear la regla deseada.
- 5 Utilice los cuadros de selección de regla para crear una o más reglas según corresponda a su configuración de usuario.
- 6 (opcional) Si crea varias reglas, se puede usar el cuadro de selección de regla **Coincidencia** para designar la forma en que vRealize Automation controla las reglas.
- 7 Haga clic en **Siguiente**.
- 8 Si desea excluir a usuarios del grupo, busque dichos usuarios y añádalos en la página Excluir usuarios del grupo.
- 9 Haga clic en **Siguiente**.
- 10 Revise la configuración del grupo en la página Revisar y, a continuación, haga clic en **Guardar** para guardar e implementar las reglas y la configuración.

Resultados

Los usuarios de Just-in-time se agregan de acuerdo con las reglas que ha creado.

Crear un grupo empresarial

Los grupos empresariales sirven para asociar un conjunto de servicios y recursos a un conjunto de usuarios. Estos grupos suelen corresponder a una línea de negocios, un departamento o a otra unidad organizativa. Crea un grupo empresarial para poder configurar reservas y autorizar a los usuarios a aprovisionar elementos del catálogo de servicios para los miembros del grupo empresarial.

Para añadir varios usuarios a una función de grupo empresarial, puede añadir varios usuarios individuales o bien varios usuarios simultáneamente, añadiendo un grupo de almacén de identidades o un grupo personalizado a una función. Por ejemplo, puede crear un grupo personalizado Equipo de soporte de ventas y añadir el grupo a la función de soporte. También puede usar grupos de usuarios del almacén de identidades existente. Los usuarios y grupos que elija deben ser válidos en el almacén de identidades.

Para admitir la integración de vCloud Director, los mismos miembros del grupo empresarial del grupo empresarial de vRealize Automation también deben ser miembros de la organización vCloud Director.

Tras la creación de un grupo empresarial por parte de un tenant, el administrador de ese grupo tendrá permiso para modificar la dirección de correo electrónico del administrador, así como sus miembros. El administrador de tenants puede modificar todas las opciones.

Este procedimiento da por hecho que IaaS está instalado y configurado.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants**.
- Si quiere añadir máquinas creadas por miembros del grupo empresarial a una unidad organizativa particular de Active Directory, configure la política de Active Directory. Consulte [Crear una política de Active Directory](#). Puede aplicar la política cuando cree el grupo empresarial o puede hacerlo más adelante.
- Si desea tener un prefijo de máquina predeterminado de grupo que se anteponga a los nombres de las máquinas aprovisionadas, solicite un prefijo a un administrador de tejidos. Consulte [Configurar prefijos de máquina](#). Los prefijos de máquinas no se aplican a solicitudes de XaaS.

Procedimiento

- 1 Seleccione **Administración > Usuarios y grupos > Grupos empresariales**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Configure los detalles del grupo empresarial.

Opción	Descripción
Nombre	Escriba el nombre del grupo empresarial.
Descripción	Escriba la descripción.

Opción	Descripción
Enviar correos electrónicos del administrador a	Introduzca una o varias direcciones de correo electrónico de los usuarios que deben recibir notificaciones de alerta de capacidad. No se admiten direcciones de correo electrónico de alias; cada dirección de correo electrónico debe corresponder a un usuario específico. Separe varias entradas con una coma. Por ejemplo, JoeAdmin@miempresa.com,WeiMgr@miempresa.com.
Política de Active Directory	Seleccione la política de Active Directory predeterminada del grupo empresarial.

4 Añada propiedades personalizadas.

5 Escriba un nombre de usuario o un nombre de grupo de usuarios personalizados y pulse Entrar.

Puede añadir uno o varios usuarios individuales o grupos de usuarios personalizados al grupo empresarial. Puede especificar los usuarios ahora, o bien crear grupos empresariales vacíos y rellenarlos más tarde.

Opción	Descripción
Función de administrador de grupo	Puede crear autorizaciones y asignar políticas de aprobación para el grupo.
Función de soporte	Puede solicitar y administrar elementos del catálogo de servicios en nombre de otros miembros del grupo empresarial.
Función de acceso compartido	Puede utilizar y ejecutar acciones en los recursos que implementan otros miembros del grupo empresarial.
Función de usuario	Puede solicitar elementos del catálogo de servicios para los que está autorizado.

6 Haga clic en **Siguiente**.

7 Configure opciones de infraestructura predeterminada.

Opción	Descripción
Prefijo de máquina predeterminado	Seleccione un prefijo de máquina preconfigurado para el grupo empresarial. Este prefijo lo utilizan blueprints de máquina. Si el blueprint utiliza el prefijo predeterminado y no está indicado aquí, se crea un prefijo de máquina basado en el nombre del grupo empresarial. El procedimiento recomendado es facilitar un prefijo predeterminado. Podrá seguir configurando blueprints con prefijos específicos, así como permitir a los usuarios del catálogo de servicios que lo reemplacen cuando soliciten un blueprint. Los blueprints de XaaS no utilizan prefijos de máquina predeterminados. Si configura aquí un prefijo y autoriza a un blueprint de XaaS para este grupo empresarial, esto no afecta al aprovisionamiento de una máquina de XaaS.
Contenedor de Active Directory	Especifique un contenedor de Active Directory. Esta opción solo se aplica al aprovisionamiento de WIM. Otros métodos de aprovisionamiento precisan de más configuración para unir las máquinas aprovisionadas a un contenedor de AD.

8 Haga clic en **Agregar**.

Resultados

Los administradores de tejidos pueden asignar recursos a su grupo empresarial mediante la creación de una reserva. Los administradores de los grupos empresariales pueden crear autorizaciones para miembros del grupo empresarial.

Pasos siguientes

- Cree una reserva para su grupo empresarial basada en el lugar en que el grupo empresarial aprovisiona máquinas. Consulte [Elegir un escenario de reserva](#).
- Si los elementos del catálogo se publican y existen los servicios, podrá crear una autorización para los miembros del grupo empresarial. Consulte [Autorizar usuarios a servicios, elementos de catálogo y acciones](#).

Solucionar problemas de rendimiento lento al mostrar miembros de grupos

Los miembros de grupos empresariales o personalizados se muestran con lentitud al consultar los detalles de un grupo.

Problema

Al consultar la información de usuarios en entornos con un gran número de usuarios, los nombres de estos últimos se cargan con gran lentitud en la interfaz de usuario.

Causa

Este tiempo adicional necesario para cargar los nombres tiene lugar en entornos con un entorno de Active Directory de gran tamaño.

Solución

- ◆ Para reducir la carga de trabajo de recuperación, utilice siempre que sea posible grupos o grupos personalizados de Active Directory en lugar de añadir a cientos de miembros individuales por el nombre.

Crear tenants adicionales

Como administrador del sistema, puede crear tenants de vRealize Automation adicionales para que los usuarios puedan acceder a las aplicaciones y recursos adecuados necesarios para completar sus asignaciones de trabajo.

Un tenant es un grupo de usuarios con privilegios específicos que trabaja en una instancia de software. Normalmente, un tenant de vRealize Automation predeterminado se crea durante la instalación y configuración inicial del sistema. A continuación, los administradores pueden crear tenants adicionales para que los usuarios puedan iniciar la sesión y completar sus asignaciones de trabajo. Los administradores pueden crear tantos tenants como sea necesario para la operación del sistema. Al crear tenants, los administradores deben especificar detalles de configuración básicos como nombre, URL de inicio de sesión, usuarios locales y administradores.

Tras configurar la información básica de los tenants, el administrador debe iniciar la sesión y configurar la conexión de Active Directory adecuada mediante la función Administración de directorios de la pestaña de administración de la consola de vRealize Automation. Además, los administradores de tenants puede aplicar a los tenants propiedades personalizadas.

Requisitos previos

Inicie sesión en la consola de vRealize Automation como **administrador del sistema**.

Procedimiento

1 (opcional) Especificar la información de tenant

El primer paso para configurar un tenant es asignarle un nombre, añadirlo a vRealize Automation y crear la URL de acceso específica del tenant.

2 (opcional) Configurar usuarios locales

El administrador del sistema de vRealize Automation debe configurar usuarios locales para cada tenant aplicable.

3 (opcional) Asignar administradores

Puede asignar uno o varios administradores de tenants y administradores de IaaS desde los almacenes de identidades que haya configurado para un tenant.

Especificar la información de tenant

El primer paso para configurar un tenant es asignarle un nombre, añadirlo a vRealize Automation y crear la URL de acceso específica del tenant.

Requisitos previos

Inicie sesión en la consola de vRealize Automation como **administrador del sistema**.

Procedimiento

- 1 Seleccione **Administración > Tenants**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Escriba un nombre en el cuadro de texto **Nombre**.
- 4 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 5 Escriba un identificador único para el tenant en el cuadro de texto **Nombre de URL**.

Este token de URL se usa para anexar un identificador específico del tenant a la URL de la consola de vRealize Automation.

Por ejemplo, escriba **mytenant** para crear la URL `https://vrealize-appliance-hostname.domain.name/vcac/org/mytenant`.

Nota La URL del tenant puede tener únicamente caracteres en minúsculas en vRealize Automation 7.0 y 7.1.

6 (opcional) Escriba una dirección de correo electrónico en el cuadro de texto **Correo electrónico de contacto**.

7 Haga clic en **Enviar y siguiente**.

Configurar usuarios locales

El administrador del sistema de vRealize Automation debe configurar usuarios locales para cada tenant aplicable.

Después de que un administrador cree la información general para un tenant, se activa la pestaña Usuarios locales y el administrador podrá designar a los usuarios que pueden acceder al tenant. Cuando se complete la configuración del tenant, los usuarios locales de tenants podrán iniciar sesión en sus respectivos tenants para completar asignaciones de trabajos.

Nota Después de añadir un usuario, no podrá cambiar su configuración. Si necesita cambiar algún aspecto de la configuración de usuario, tendrá que eliminar el usuario y volver a crearlo.

Procedimiento

- 1** Haga clic en el botón **Añadir** en la pestaña Usuarios locales.
- 2** Escriba los nombres y apellidos de los usuarios en los campos **Nombre** y **Apellidos** en el cuadro de diálogo Detalles de usuarios.
- 3** Escriba la dirección de correo electrónico del usuario en el campo **Correo electrónico**.
- 4** Escriba el ID de usuario y la contraseña para el usuario en los campos **Nombre de usuario** y **Contraseña**.
- 5** Haga clic en el botón **Añadir**.
- 6** Repita estos pasos según corresponda para todos los usuarios locales del tenant.

Resultados

Se han creado los usuarios locales especificados para el tenant.

Asignar administradores

Puede asignar uno o varios administradores de tenants y administradores de IaaS desde los almacenes de identidades que haya configurado para un tenant.

Los administradores de tenants son responsables de configurar la personalización de marca específica del tenant, así como de administrar los almacenes de identidades, usuarios, grupos, autorizaciones y blueprints compartidos en el contexto del tenant. Los administradores de IaaS son responsables de configurar los endpoints de origen de infraestructuras en IaaS, asignar administradores de tejido y supervisar los logs de IaaS.

Requisitos previos

- Para poder asignar administradores de IaaS, debe instalar IaaS. Para obtener más información sobre cómo instalar IaaS, consulte *Instalación de vRealize Automation*.

Procedimiento

- 1 Escriba el nombre de un usuario o grupo en el cuadro de búsqueda **Administradores de tenants** y presione Entrar.

Para obtener resultados más rápidos, escriba el nombre completo del grupo o usuario; por ejemplo, myAdmins@mycompany.domain. Repita este paso para asignar administradores de tenants adicionales.

- 2 Si ha instalado IaaS, escriba el nombre de un usuario o grupo en el cuadro de búsqueda **Administradores de IaaS** y presione Entrar.

Para obtener resultados más rápidos, escriba el nombre completo del grupo o usuario; por ejemplo, IaaSAdmins@mycompany.domain. Repita este paso para asignar administradores de infraestructura adicionales.

- 3 Haga clic en **Agregar**.

Eliminar un tenant

Un administrador del sistema puede eliminar tenants no deseados de vRealize Automation.

Si se elimina un tenant, este se quitará de la interfaz de vRealize Automation inmediatamente, pero puede que tarde varias horas en quitarse por completo de la implementación. Si elimina un tenant y desea crear otro con la misma URL, espere a que transcurran varias horas para que se complete la eliminación antes de crear el nuevo tenant.

Requisitos previos

Inicie sesión en la consola de vRealize Automation como **administrador del sistema**.

Procedimiento

- 1 Seleccione **Administración > Tenants**.
- 2 Seleccione el tenant que quiera eliminar.

No haga clic en el nombre real para seleccionar el tenant. Si lo hace, se abrirá el tenant para su edición.

- 3 Haga clic en **Eliminar**.

Resultados

El tenant se eliminará de la implementación de vRealize Automation.

Configurar los ajustes de seguridad para varios tenants

En un entorno de varios tenants, puede controlar la disponibilidad de los objetos de seguridad de NSX en todos los tenants.

Cuando se crea un objeto de seguridad de NSX en vRealize Automation, su disponibilidad predeterminada puede ser global, lo que significa que está disponible en todos los tenants para los que el endpoint asociado tenga una reserva, o bien puede estar oculto para todos los usuarios, salvo el administrador.

La disponibilidad de objetos de seguridad en todos los tenants también está relacionada con el hecho de que el endpoint asociado tenga o no una reserva o una política de reserva en el tenant.

En el tema relacionado [Controlar el acceso a tenants de los objetos de seguridad](#) se resume cómo puede controlarse la disponibilidad de los nuevos objetos de seguridad en todos los tenants, así como el comportamiento que se aprecia en los objetos de seguridad existentes en relación con una estructura de varios tenants, después de actualizar a esta versión de vRealize Automation.

Configurar la personalización de marca

vRealize Automation permite aplicar personalización de marca a las páginas de inicio de sesión de tenant y de aplicación.

La personalización de marca puede incluir los colores del texto y del fondo, logotipos empresariales, el nombre de la compañía, políticas de privacidad, declaraciones de derechos de autor y otra información relevante que desee que aparezca en las páginas de inicio de sesión de tenant o de aplicación.

Personalización de marca en la página de inicio de sesión de tenant

Utilice la página Personalización de marca de pantalla de inicio de sesión para aplicar personalización de marca a las páginas de inicio de sesión del tenant de vRealize Automation.

Puede usar la personalización de marca de vRealize Automation predeterminada en las páginas de inicio de sesión de tenant, o bien puede configurar la personalización de marca mediante la página Personalización de marca de pantalla de inicio de sesión. Tenga en cuenta que la personalización de marca se aplica del mismo modo a todas las aplicaciones de tenant.

Esta página permite configurar la personalización de marca en todas las páginas de inicio de sesión de tenant.

La página Personalización de marca de pantalla de inicio de sesión muestra la personalización de marca de inicio de sesión de tenant implementada actualmente en el panel Vista previa.

Nota Después de guardar la nueva personalización de marca de la página de inicio de sesión de tenant, es probable que se presente una demora de hasta cinco minutos antes de que pueda verse en todas las páginas de inicio de sesión.

Requisitos previos

Para poder utilizar un logotipo personalizado u otra imagen con su personalización de marca, debe disponer de los archivos adecuados.

Procedimiento

- 1 Inicie sesión en vRealize Automation como administrador del sistema o administrador de tenants.
- 2 Haga clic en la pestaña **Administración**.
- 3 Seleccione los efectos visuales que desee marcando las casillas correspondientes del encabezado Efectos.

Todos los efectos son opcionales.
- 4 Seleccione **Personalización de marca > Personalización de marca de pantalla de inicio de sesión**
- 5 Haga clic en **Cargar** en el campo Logotipo, navegue a la carpeta adecuada y seleccione un archivo de imagen de logotipo.
- 6 Si lo desea, haga clic en **Cargar** en el campo Imagen (opcional), navegue a la carpeta adecuada y seleccione un archivo de imagen adicional.
- 7 Si lo desea, introduzca los códigos de color hexadecimal correspondientes en los campos **Color del fondo**, **Color de la cabecera**, **Color de fondo del botón de inicio de sesión** y **Color de primer plano del botón de inicio de sesión**.

Si es necesario, busque en Internet la lista de códigos de color hexadecimal.
- 8 Haga clic en **Guardar** para aplicar la configuración.

Resultados

Los usuarios del tenant verán la personalización de marca en sus páginas de inicio de sesión.

Personalización de marca en aplicaciones de tenant

Utilice la página Personalización de marca de aplicación para aplicar la personalización de marca a las aplicaciones de tenant de vRealize Automation.

Puede usar la personalización de marca de vRealize Automation predeterminada en las aplicaciones de usuario, o bien puede configurar la personalización de marca mediante la página Personalización de marca de aplicación. Esta página permite configurar la personalización de marca en el encabezado y el pie de página de las páginas de aplicación. Tenga en cuenta que la personalización de marca se aplica del mismo modo a todas las aplicaciones de usuario.

En la parte inferior de la página Personalización de marca de aplicación se muestra la personalización de marca implementada actualmente en el encabezado o el pie de página.

Requisitos previos

Si desea usar un logotipo personalizado con su personalización de marca, debe tener un archivo de imagen del logotipo.

Procedimiento

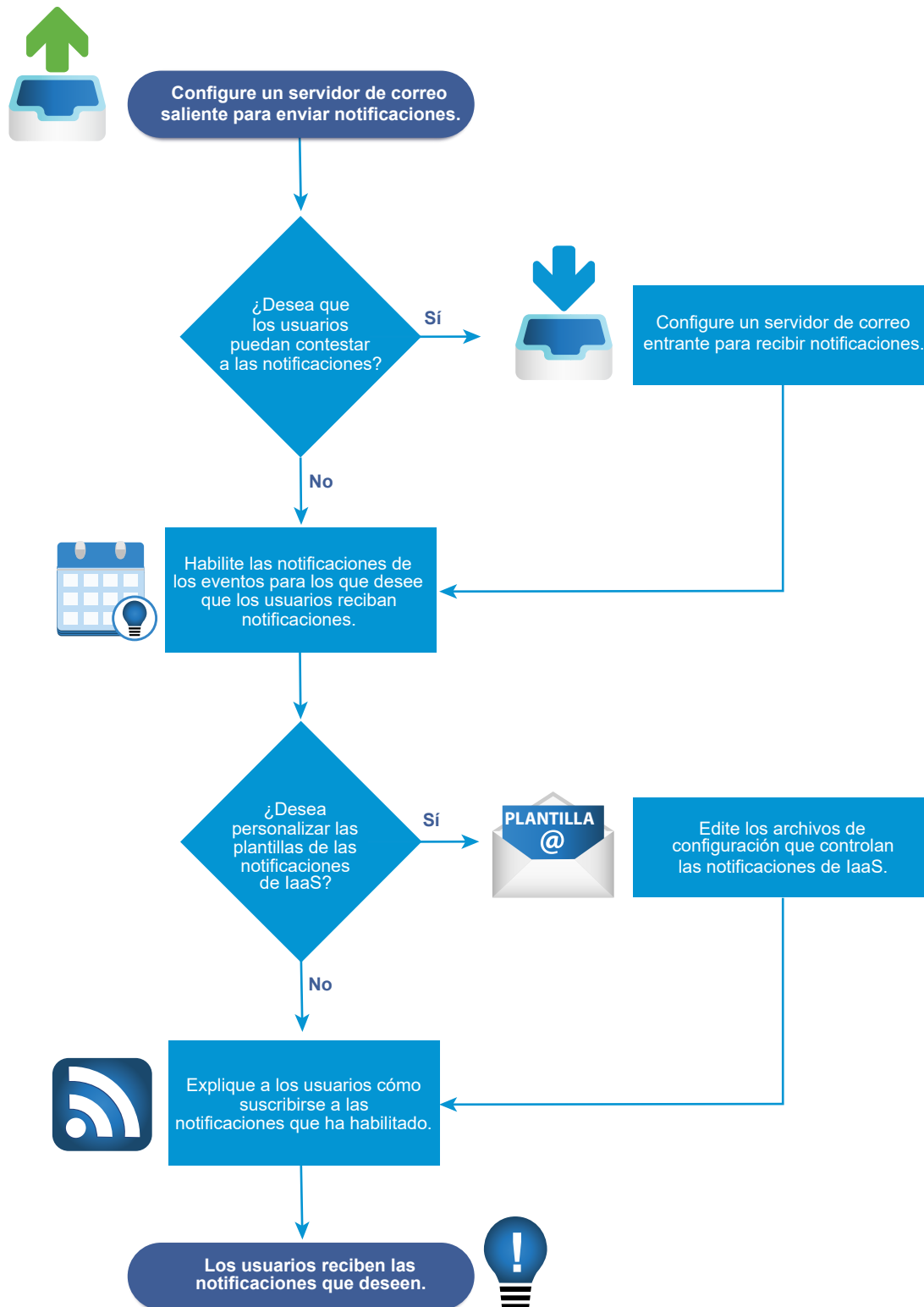
- 1 Inicie sesión en vRealize Automation como administrador del sistema o administrador de tenants.
- 2 Haga clic en la pestaña **Administración**.
- 3 Seleccione **Personalización de marca > Personalización de marca de aplicación**
- 4 Haga clic en la pestaña **Encabezado** si no está activa.
- 5 Si desea usar la personalización de marca de vRealize Automation predeterminada, haga clic en la casilla **Usar predeterminado**.
- 6 Para implementar la personalización de marca, seleccione las opciones adecuadas en los campos de las pestañas **Encabezado** y **Pie de página**.
 - a Haga clic en el botón **Examinar** en el campo **Logotipo de encabezado**, navegue a la carpeta adecuada y seleccione un archivo de imagen de logotipo.
 - b Escriba el nombre de la compañía correspondiente en el campo **Nombre de la compañía**.
El nombre especificado aparece cuando un usuario pasa el mouse por encima del logotipo.
 - c Escriba el nombre correspondiente en el campo **Nombre del producto**.
El nombre especificado aquí aparece en el encabezado de la aplicación, junto al logotipo.
 - d Escriba el código de color hexadecimal correspondiente al color de fondo del perímetro de la aplicación en el campo **Color hexadecimal del fondo**.
Si es necesario, busque en Internet la lista de códigos de color hexadecimal.
 - e Escriba el código de color hexadecimal correspondiente al color de texto en el campo **Color hexadecimal del texto**.
Si es necesario, busque en Internet la lista de códigos de color del texto.
 - f Haga clic en **Siguiente** para activar el campo Pie de página.
 - g Escriba la frase que desee en el campo **Aviso de derechos de autor**.
 - h Inserte el vínculo a la declaración de política de privacidad de su compañía en el campo **Vínculo de política de privacidad**.
 - i Especifique la información de contacto de la compañía que desee en el campo **Vínculo del contacto**.
- 7 Haga clic en **Actualizar** para implementar su configuración de personalización de marca.

Resultados

Los usuarios del tenant verán la personalización de marca en sus páginas de aplicación.

Lista de comprobación para la configuración de notificaciones

Puede configurar vRealize Automation para enviar notificaciones a los usuarios cuando se produzcan determinados eventos. Los usuarios pueden elegir las notificaciones a las que desean suscribirse, pero solo pueden seleccionar los eventos que se hayan habilitado como desencadenadores de notificaciones.



La Lista de comprobación para la configuración de notificaciones proporciona una descripción general de la secuencia de pasos necesarios para configurar notificaciones y proporciona vínculos a puntos decisivos o instrucciones detalladas de cada paso.

Tabla 2-10. Lista de comprobación para la configuración de notificaciones

Tarea	Función necesaria	Detalles
<input type="checkbox"/> Configurar un servidor de correo electrónico saliente para enviar notificaciones.	<ul style="list-style-type: none"> Los administradores del sistema configuran servidores globales predeterminados. Los administradores de tenants configuran servidores para sus tenants. 	<p>Para configurar un servidor para su tenant por primera vez, consulte Añadir un servidor de correo electrónico saliente específico del tenant. Si necesita reemplazar un servidor global predeterminado, consulte Reemplazar un servidor de correo electrónico saliente predeterminado de sistema.</p> <p>Para configurar servidores globales predeterminados para todos los tenants, consulte Crear un servidor de correo electrónico saliente global.</p>
<input type="checkbox"/> (Opcional) Configurar un servidor de correo electrónico saliente para que los usuarios puedan completar tareas respondiendo a las notificaciones.	<ul style="list-style-type: none"> Los administradores del sistema configuran servidores globales predeterminados. Los administradores de tenants configuran servidores para sus tenants. 	<p>Para configurar un servidor para su tenant por primera vez, consulte Añadir un servidor de correo electrónico entrante específico del tenant.</p> <p>Si necesita reemplazar un servidor global predeterminado, consulte Reemplazar un servidor de correo electrónico entrante predeterminado de sistema.</p> <p>Para configurar un servidor global predeterminado para todos los tenants, consulte Crear un servidor de correo electrónico entrante global.</p>
<input type="checkbox"/> (Opcional) Especifique cuándo enviar una notificación de correo electrónico antes de la fecha de caducidad de una máquina.	Administrador del sistema	Consulte Personalizar la fecha de notificación de correo electrónico de caducidad de máquina .
<input type="checkbox"/> Seleccionar los eventos de vRealize Automation que desencadenan notificaciones de usuario. Los usuarios solo pueden suscribirse a las notificaciones de los eventos que se hayan habilitado como desencadenadores de notificaciones.	Administrador de tenants	Consulte Configurar notificaciones .

Tabla 2-10. Lista de comprobación para la configuración de notificaciones (continuación)

Tarea	Función necesaria	Detalles
<input type="checkbox"/> (Opcional) Configurar las plantillas de las notificaciones que se envían a los propietarios de máquinas respecto de eventos relacionados con sus máquinas, por ejemplo, la caducidad de concesiones.	Todo aquel que tenga acceso al directorio \Templates del directorio de instalación del servidor de vRealize Automation (que suele estar en %SystemDrive%\Archivos de programa x86\VMware\VCAC\Server) puede configurar las plantillas de estas notificaciones de correo electrónico.	Consulte Configurar plantillas para correos electrónicos de IaaS automáticos .
<input type="checkbox"/> Sus usuarios se suscriben automáticamente a las notificaciones configuradas. Si es necesario, proporcione a los usuarios instrucciones sobre cómo suscribirse a las notificaciones habilitadas. Pueden optar por suscribirse únicamente a las notificaciones relevantes para sus funciones.	Todos los usuarios	Consulte Suscribirse a notificaciones .

Configurar servidores de correo electrónico globales para notificaciones

Los administradores de tenant pueden añadir servidores de correo electrónico como parte de la configuración de las notificaciones para sus propios tenants. Por su parte, los administradores del sistema pueden configurar servidores de correo electrónico entrante y saliente, que se muestran a todos los tenants como valores predeterminados del sistema. Si los administradores de tenant no sobrescriben estos valores antes de habilitar las notificaciones, vRealize Automation usa los servidores de correo electrónico configurados globalmente.

Crear un servidor de correo electrónico entrante global

Los administradores del sistema pueden crear un servidor de correo electrónico entrante global para controlar las notificaciones de correo electrónico entrantes (como, por ejemplo, las respuestas de aprobación). Solamente se puede crear un servidor entrante, que aparecerá como servidor predeterminado para todos los tenants. Si los administradores de tenant no sobrescriben estos valores antes de habilitar las notificaciones, vRealize Automation usa el servidor de correo electrónico configurado globalmente.

Requisitos previos

Inicie sesión en la consola de vRealize Automation como **administrador del sistema**.

Procedimiento

- 1 Seleccione **Administración > Servidores de correo electrónico**.
- 2 Haga clic en el icono **Añadir** (+).
- 3 Seleccione **Correo electrónico: entrante**.
- 4 Haga clic en **Aceptar**.
- 5 Escriba un nombre en el cuadro de texto **Nombre**.
- 6 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 7 (opcional) Active la casilla **SSL** para usar SSL para la seguridad.
- 8 Elija un protocolo de servidor.
- 9 Escriba el nombre del servidor en el cuadro de texto **Nombre del servidor**.
- 10 Escriba el número de puerto del servidor en el cuadro de texto **Puerto del servidor**.
- 11 Escriba el nombre de la carpeta de los correos electrónicos en el cuadro de texto **Nombre de la carpeta**.
Esta opción solo es obligatoria si se selecciona el protocolo de servidor IMAP.
- 12 Escriba un nombre de usuario en el cuadro de texto **Nombre de usuario**.
- 13 Escriba una contraseña en el cuadro de texto **Contraseña**.
- 14 Escriba la dirección de correo electrónico a la que los usuarios de vRealize Automation pueden responder en el cuadro de texto **Dirección de correo electrónico**.
- 15 (opcional) Seleccione **Eliminar del servidor** para eliminar del servidor todos los correos electrónicos procesados que recupere el servicio de notificaciones.
- 16 Elija si vRealize Automation puede aceptar certificados autofirmados del servidor de correo electrónico.
- 17 Haga clic en **Probar conexión**.
- 18 Haga clic en **Agregar**.

Crear un servidor de correo electrónico saliente global

Los administradores del sistema pueden crear un servidor de correo electrónico saliente global para controlar las notificaciones de correo electrónico salientes. Solamente se puede crear un servidor saliente, que aparecerá como servidor predeterminado para todos los tenants. Si los administradores de tenant no sobrescriben estos valores antes de habilitar las notificaciones, vRealize Automation usa el servidor de correo electrónico configurado globalmente.

Requisitos previos

Inicie sesión en la consola de vRealize Automation como **administrador del sistema**.

Procedimiento

- 1 Seleccione **Administración > Servidores de correo electrónico**.
- 2 Haga clic en el icono **Añadir** (+).
- 3 Seleccione **Correo electrónico: saliente**.
- 4 Haga clic en **Aceptar**.
- 5 Escriba un nombre en el cuadro de texto **Nombre**.
- 6 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 7 Escriba el nombre del servidor en el cuadro de texto **Nombre del servidor**.
- 8 Elija un método de cifrado.
 - Haga clic en **Usar SSL**.
 - Haga clic en **Usar TLS**.
 - Haga clic en **Ninguno** para enviar comunicaciones sin cifrar.
- 9 Escriba el número de puerto del servidor en el cuadro de texto **Puerto del servidor**.
- 10 (opcional) Active la casilla de verificación **Obligatorio** si el servidor requiere autenticación.
 - a Escriba un nombre de usuario en el cuadro de texto **Nombre de usuario**.
 - b Escriba una contraseña en el cuadro de texto **Contraseña**.
- 11 Escriba la dirección de correo electrónico desde la que parecerá que se originan los correos electrónicos de vRealize Automation en el cuadro de texto **Dirección del remitente**.
 Esta dirección de correo electrónico se corresponde con el nombre de usuario y la contraseña que ha indicado.
- 12 Elija si vRealize Automation puede aceptar certificados autofirmados del servidor de correo electrónico.
- 13 Haga clic en **Probar conexión**.
- 14 Haga clic en **Agregar**.

Añadir un servidor de correo electrónico saliente específico del tenant

Los administradores de tenants pueden añadir un servidor de correo electrónico saliente para enviar notificaciones para completar los elementos de trabajo tales como las aprobaciones.

Cada tenant solo puede tener un servidor de correo electrónico saliente. Si el administrador del sistema ya ha configurado un servidor de correo electrónico saliente global, consulte [Reemplazar un servidor de correo electrónico saliente predeterminado de sistema](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants**.

- Si el correo electrónico requiere autenticación, el usuario especificado debe estar en un almacén de identidades y en el grupo empresarial.

Procedimiento

- 1 Seleccione **Administración > Notificaciones > Servidores de correo electrónico**.
- 2 Haga clic en el icono **Añadir (+)**.
- 3 Seleccione **Correo electrónico: saliente**.
- 4 Haga clic en **Aceptar**.
- 5 Escriba un nombre en el cuadro de texto **Nombre**.
- 6 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 7 Escriba el nombre del servidor en el cuadro de texto **Nombre del servidor**.
- 8 Elija un método de cifrado.
 - Haga clic en **Usar SSL**.
 - Haga clic en **Usar TLS**.
 - Haga clic en **Ninguno** para enviar comunicaciones sin cifrar.
- 9 Escriba el número de puerto del servidor en el cuadro de texto **Puerto del servidor**.
- 10 (opcional) Active la casilla de verificación **Obligatorio** si el servidor requiere autenticación.
 - a Escriba un nombre de usuario en el cuadro de texto **Nombre de usuario**.
 - b Escriba una contraseña en el cuadro de texto **Contraseña**.
- 11 Escriba la dirección de correo electrónico desde la que parecerá que se originan los correos electrónicos de vRealize Automation en el cuadro de texto **Dirección del remitente**.
Esta dirección de correo electrónico se corresponde con el nombre de usuario y la contraseña que ha indicado.
- 12 Elija si vRealize Automation puede aceptar certificados autofirmados del servidor de correo electrónico.
Esta opción solo está disponible si habilita el cifrado.
 - Haga clic en **Sí** para aceptar los certificados autofirmados.
 - Haga clic en **No** para rechazar los certificados autofirmados.
- 13 Haga clic en **Probar conexión**.
- 14 Haga clic en **Agregar**.

Añadir un servidor de correo electrónico entrante específico del tenant

Los administradores de tenants pueden añadir un servidor de correo electrónico entrante para que los usuarios puedan responder a las notificaciones para completar los elementos de trabajo tales como las aprobaciones.

Cada tenant solo puede tener un servidor de correo electrónico entrante. Si el administrador del sistema ya ha configurado un servidor de correo electrónico entrante global, consulte [Reemplazar un servidor de correo electrónico entrante predeterminado de sistema](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants**.
- Compruebe que el usuario especificado está en un almacén de identidades y en el grupo empresarial.

Procedimiento

- 1 Seleccione **Administración > Notificaciones > Servidores de correo electrónico**.
- 2 Haga clic en el icono **Añadir** (+).
- 3 Seleccione **Correo electrónico - Entrante** y haga clic en **Aceptar**.
- 4 Configure las siguientes opciones del servidor de correo electrónico entrante.

Opción	Acción
Nombre	Escriba un nombre para el servidor de correo electrónico entrante.
Descripción	Escriba una descripción del servidor de correo electrónico entrante.
Seguridad	Active la casilla Usar SSL .
Protocolo	Elija un protocolo de servidor.
Nombre del servidor	Escriba el nombre del servidor.
Puerto del servidor	Escriba el número de puerto del servidor.

- 5 Escriba el nombre de la carpeta de los correos electrónicos en el cuadro de texto **Nombre de la carpeta**.

Esta opción solo es obligatoria si se selecciona el protocolo de servidor IMAP.

- 6 Escriba un nombre de usuario en el cuadro de texto **Nombre de usuario**.
- 7 Escriba una contraseña en el cuadro de texto **Contraseña**.
- 8 Escriba la dirección de correo electrónico a la que los usuarios de vRealize Automation pueden responder en el cuadro de texto **Dirección de correo electrónico**.
- 9 (opcional) Seleccione **Eliminar del servidor** para eliminar del servidor todos los correos electrónicos procesados que recupere el servicio de notificaciones.
- 10 Elija si vRealize Automation puede aceptar certificados autofirmados del servidor de correo electrónico.

Esta opción solo está disponible si habilita el cifrado.

- Haga clic en **Sí** para aceptar los certificados autofirmados.
- Haga clic en **No** para rechazar los certificados autofirmados.

11 Haga clic en **Probar conexión**.

12 Haga clic en **Agregar**.

Reemplazar un servidor de correo electrónico saliente predeterminado de sistema

Si el administrador del sistema ha configurado un servidor de correo electrónico saliente predeterminado de sistema, el administrador de tenant puede reemplazar esta configuración global.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Notificaciones > Servidores de correo electrónico**.
- 2 Seleccione el servidor de correo electrónico saliente.
- 3 Haga clic en **Reemplazar el valor global**.
- 4 Escriba un nombre en el cuadro de texto **Nombre**.
- 5 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 6 Escriba el nombre del servidor en el cuadro de texto **Nombre del servidor**.
- 7 Elija un método de cifrado.
 - Haga clic en **Usar SSL**.
 - Haga clic en **Usar TLS**.
 - Haga clic en **Ninguno** para enviar comunicaciones sin cifrar.
- 8 Escriba el número de puerto del servidor en el cuadro de texto **Puerto del servidor**.
- 9 (opcional) Active la casilla de verificación **Obligatorio** si el servidor requiere autenticación.
 - a Escriba un nombre de usuario en el cuadro de texto **Nombre de usuario**.
 - b Escriba una contraseña en el cuadro de texto **Contraseña**.
- 10 Escriba la dirección de correo electrónico desde la que parecerá que se originan los correos electrónicos de vRealize Automation en el cuadro de texto **Dirección del remitente**.
 Esta dirección de correo electrónico se corresponde con el nombre de usuario y la contraseña que ha indicado.
- 11 Elija si vRealize Automation puede aceptar certificados autofirmados del servidor de correo electrónico.
 Esta opción solo está disponible si habilita el cifrado.
 - Haga clic en **Sí** para aceptar los certificados autofirmados.
 - Haga clic en **No** para rechazar los certificados autofirmados.

12 Haga clic en **Probar conexión**.

13 Haga clic en **Agregar**.

Reemplazar un servidor de correo electrónico entrante predeterminado de sistema

Si el administrador del sistema ha configurado un servidor de correo electrónico entrante predeterminado de sistema, los administradores de tenant pueden reemplazar esta configuración global.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1** Seleccione **Administración > Notificaciones > Servidores de correo electrónico**.
- 2** Seleccione el servidor de correo electrónico entrante en la tabla Servidores de correo electrónico.
- 3** Haga clic en **Reemplazar el valor global**.
- 4** Especifique las siguientes opciones de servidor de correo electrónico entrante.

Opción	Acción
Nombre	Escriba el nombre del servidor de correo electrónico entrante.
Descripción	Escriba una descripción del servidor de correo electrónico entrante.
Seguridad	Active la casilla SSL para usar SSL para la seguridad.
Protocolo	Elija un protocolo de servidor.
Nombre del servidor	Escriba el nombre del servidor.
Puerto del servidor	Escriba el número de puerto del servidor.

- 5** Escriba el nombre de la carpeta de los correos electrónicos en el cuadro de texto **Nombre de la carpeta**.

Esta opción solo es obligatoria si se selecciona el protocolo de servidor IMAP.

- 6** Escriba un nombre de usuario en el cuadro de texto **Nombre de usuario**.
- 7** Escriba una contraseña en el cuadro de texto **Contraseña**.
- 8** Escriba la dirección de correo electrónico a la que los usuarios de vRealize Automation pueden responder en el cuadro de texto **Dirección de correo electrónico**.
- 9** (opcional) Seleccione **Eliminar del servidor** para eliminar del servidor todos los correos electrónicos procesados que recupere el servicio de notificaciones.

- 10 Elija si vRealize Automation puede aceptar certificados autofirmados del servidor de correo electrónico.

Esta opción solo está disponible si habilita el cifrado.

- Haga clic en **Sí** para aceptar los certificados autofirmados.
- Haga clic en **No** para rechazar los certificados autofirmados.

- 11 Haga clic en **Probar conexión**.

- 12 Haga clic en **Agregar**.

Revertir a los servidores de correo electrónico predeterminados del sistema

Los administradores de tenant que reemplacen los servidores predeterminados del sistema podrán revertir la configuración a los ajustes generales.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Notificaciones > Servidores de correo electrónico**.
- 2 Seleccione el servidor de correo electrónico que desea revertir.
- 3 Haga clic en **Restaurar el valor global**.
- 4 Haga clic en **Sí**.

Configurar notificaciones

Cada usuario decide si desea recibir notificaciones, pero es el administrador de tenant quien decide qué eventos desencadenan notificaciones.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants**.
- Confirme que un administrador de tenant o administrador del sistema ha configurado un servidor de correo electrónico saliente. Consulte [Añadir un servidor de correo electrónico saliente específico del tenant](#).

Procedimiento

- 1 Seleccione **Administración > Notificaciones > Escenarios**.
- 2 Seleccione una o varias notificaciones.
- 3 Haga clic en **Activar**.

Resultados

De este modo, los usuarios que estén suscritos a las notificaciones en la configuración de sus preferencias recibirán notificaciones.

Personalizar la fecha de notificación de correo electrónico de caducidad de máquina

Puede especificar cuándo enviar una notificación de correo electrónico antes de la fecha de caducidad de una máquina.

Puede cambiar la configuración que define la cantidad de días de anticipación a la fecha de caducidad de una máquina con el que vRealize Automation envía un mensaje de correo electrónico de notificación de caducidad. El mensaje de correo electrónico informa a los usuarios de la fecha de caducidad de una máquina. De forma predeterminada, la configuración se establece como siete días antes de la caducidad de la máquina.

Procedimiento

- 1 Inicie sesión en el servidor de vRealize Automation con credenciales que tengan acceso administrativo.
- 2 Desplácese al archivo `/etc/vcac/setenv-user` y ábralo.
- 3 Agregue la siguiente línea al archivo para especificar la cantidad de días de anticipación a la fecha de caducidad de la máquina, donde 3 en este ejemplo especifica tres días antes de la caducidad de la máquina.

```
VCAC_OPTS="$VCAC_OPTS -Dlease.enforcement.prearchive.notification.days=3"
```

- 4 Ejecute el siguiente comando para reiniciar los servicios vCAC en el dispositivo virtual:

```
service vcac-server restart
```

Pasos siguientes

Si está trabajando en un entorno de equilibrador de carga de alta disponibilidad, repita este procedimiento para todos los dispositivos virtuales del entorno de alta disponibilidad.

Configurar plantillas para correos electrónicos de IaaS automáticos

Puede configurar el envío de correos electrónicos de notificación a los propietarios de máquinas para comunicarles eventos de vRealize Automation relativos a sus máquinas.

Entre los eventos que desencadenan estas notificaciones están la caducidad o proximidad de caducidad de los períodos de archivado y de las concesiones de máquina virtual.

Para obtener información sobre cómo configurar, habilitar o deshabilitar las notificaciones de correo electrónico de vRealize Automation, consulte el siguiente artículo de blog y los siguientes artículos de la base de conocimientos:

- [Personalización de correo electrónico en vRealize Automation](#)
- [Personalización de plantillas de correo electrónico en vRealize Automation \(2088805\)](#) (en inglés)
- [Ejemplos de la personalización de plantillas de correo electrónico en vRealize Automation \(2102019\)](#) (en inglés)

Suscribirse a notificaciones

Si los administradores configuraron notificaciones, la suscripción es automática. Los eventos de notificaciones pueden ser la finalización correcta de una solicitud del catálogo o una aprobación necesaria.

Si debe suscribirse manualmente, puede habilitar las notificaciones.

Requisitos previos

Inicie sesión en vRealize Automation.

Procedimiento

- 1 Haga clic en **Preferencias**.
- 2 Active la casilla de verificación **Habilitado** del protocolo Correo electrónico en la tabla Notificaciones.
- 3 Haga clic en **Aplicar**.
- 4 Haga clic en **Cerrar**.

Crear un archivo RDP personalizado para admitir conexiones RDP para máquinas aprovisionadas

Los administradores del sistema crean un archivo de protocolo de escritorio remoto personalizado que los arquitectos de IaaS usan en blueprints para configurar las opciones de RDP. Puede crear el archivo RDP y ofrecer a los arquitectos el nombre completo de la ruta al archivo para que puedan incluirlo en blueprints. Después, un administrador del catálogo autoriza a los usuarios para la acción de RDP.

Nota Si usa Internet Explorer con la configuración de seguridad mejorada habilitada, no puede descargar archivos `.rdp`.

Requisitos previos

Inicie sesión en IaaS Manager Service como administrador.

Procedimiento

- 1 Establezca el directorio actual en `<vra_installation_dir>\Rdp`.
- 2 Copie el archivo `Default.rdp` y cambie su nombre por `Console.rdp` en el mismo directorio.
- 3 Abra el archivo `Console.rdp` en un editor.
- 4 Añada la configuración de RDP al archivo.

Por ejemplo, **connect to console:i:1**.

- 5 Si trabaja en un entorno distribuido, inicie sesión como usuario con privilegios administrativos en la máquina host de IaaS donde esté instalado el componente de sitio web de Model Manager.

- 6 Copie el archivo `Console.rdp` en el directorio `vRA_installation_dir\Server\Website\Rdp`.
- 7 Añada la propiedad personalizada `VirtualMachine.Rdp.File` al blueprint.

Los arquitectos de IaaS pueden añadir propiedades personalizadas de RDP a los blueprints de la máquina virtual de Windows y, después, los administradores del catálogo pueden autorizar a los usuarios para la acción Conectar mediante RDP. Consulte [Añadir soporte para la conexión RDP a los blueprints de máquina de Windows](#).

Escenario: Añadir ubicaciones de centros de datos para implementaciones en varias regiones

Como administrador del sistema, desea definir ubicaciones para los centros de datos de Boston y Londres, de modo que los administradores de tejido puedan aplicar las ubicaciones adecuadas para calcular los recursos de cada centro de datos. Cuando los arquitectos de blueprint crean blueprints, pueden habilitar la característica de ubicaciones para que los usuarios puedan optar por aprovisionar máquinas en Boston o Londres cuando rellenen sus formularios de solicitud de elementos del catálogo.

Tiene un centro de datos en Londres y otro en Boston, y no quiere que los usuarios de Boston aprovisionen máquinas en la infraestructura de Londres y viceversa. Para asegurarse de que los usuarios de Boston aprovisionan en la infraestructura de Boston, y los usuarios de Londres aprovisionan en la infraestructura de Londres, le interesa permitir a los usuarios que seleccionen una ubicación adecuada para el aprovisionamiento cuando estos soliciten máquinas.



No se pueden filtrar las ubicaciones de centro de datos en el archivo xml basado en el tenant o el grupo empresarial. Cuando trabaje en un entorno de varios tenants, puede usar las definiciones de propiedad para filtrar en función del tenant o el grupo empresarial. Para obtener información sobre el uso de las definiciones de propiedad, consulte la publicación del blog sobre [cómo usar las definiciones de propiedad dinámica](#).

Procedimiento

- 1 Inicie sesión en el host del servidor web de IaaS a través de las credenciales de administrador.

Esta es la máquina en la que instaló el componente del sitio web de IaaS.

- 2 Edite el archivo `WebSite\XmlData\DataCenterLocations.xml` en el directorio de instalación del servidor Windows (normalmente `%SystemDrive%\Archivos de programa x86\VMware\vCAC\Server`).
- 3 Edite la sección `CustomDataType` del archivo para crear entradas de nombre de datos para cada ubicación.

```
<CustomDataType>
  <Data Name="London" Description="London datacenter" />
  <Data Name="Boston" Description="Boston datacenter" />
</CustomDataType>
```

- 4 Guarde y cierre el archivo.
- 5 Reinicie Manager Service.
- 6 Si tiene más de un host de servidor web de IaaS, repita este procedimiento en cada instancia redundante.

Resultados

El administrador de tejido puede aplicar la ubicación adecuada para computar los recursos ubicados en cada centro de datos. Consulte [Escenario: Aplicar una ubicación a un recurso informático para implementaciones entre regiones](#).

Pasos siguientes

Para que el usuario deba indicar una ubicación de centro de datos al solicitar un aprovisionamiento de máquinas, puede añadir la propiedad `Vrm.DataCenter.Location` a un blueprint o activar la opción **Mostrar ubicación al solicitar** en el blueprint.

Configurar vRealize Orchestrator

vRealize Orchestrator es un motor de automatización y administración que amplía las opciones de vRealize Automation para prestar soporte a XaaS, además de otras opciones de extensibilidad. Puede configurar y usar el servidor de vRealize Orchestrator que viene preconfigurado en el dispositivo de vRealize Automation, o bien implementar vRealize Orchestrator como una instancia de servidor externo y asociar esa instancia externa a vRealize Automation.

vRealize Orchestrator permite a administradores y arquitectos desarrollar complejas tareas de automatización mediante el uso del diseñador de flujo de trabajo y, a continuación, acceder y ejecutar los flujos de trabajo desde vRealize Automation.

vRealize Orchestrator puede acceder y controlar tecnologías y aplicaciones externas mediante el uso de complementos vRealize Orchestrator.

Configurar vRealize Automation para que use vRealize Orchestrator permite publicar flujos de trabajo de Orchestrator en el catálogo de servicios vRealize Orchestrator como parte de la administración de blueprints de XaaS.

Si quiere ejecutar flujos de trabajo de Orchestrator para ampliar la administración de máquinas IaaS, debe configurar vRealize Orchestrator como un endpoint.

Privilegios de configuración

Los administradores del sistema y de tenants pueden configurar vRealize Automation para que use un servidor externo de vRealize Orchestrator.

Además, los administradores del sistema también pueden determinar las carpetas de flujo de trabajo disponibles para cada tenant.

Los administradores de tenants pueden configurar los complementos de vRealize Orchestrator como endpoints.

Función	Privilegios de configuración relacionados con vRealize Orchestrator
Administradores del sistema	<ul style="list-style-type: none"> ■ Configurar el servidor de vRealize Orchestrator para todos los tenants. ■ Definir las carpetas predeterminadas de flujo de trabajo de vRealize Orchestrator por tenant.
Administradores de tenants	<ul style="list-style-type: none"> ■ Configurar el servidor de vRealize Orchestrator para su propio tenant. ■ Añadir complementos de vRealize Orchestrator como endpoints.

Configure el servidor de vRealize Orchestrator integrado

El dispositivo de vRealize Automation incluye una instancia preconfigurada de vRealize Orchestrator. El servicio del servidor de vRealize Orchestrator se ejecuta de manera predeterminada, pero es necesario iniciar el servicio de configuración manualmente para acceder al centro de control.

Requisitos previos

Implementar el dispositivo de vRealize Automation. Para obtener detalles, consulte *Implementar el dispositivo de vRealize Automation* en *Instalación de vRealize Automation*.

Procedimiento

- 1 Inicie sesión en la consola de vRealize Automation como **administrador del sistema** o **administrador de tenants**.
- 2 Seleccione **Administración > Configuración de vRO > Configuración del servidor**.
- 3 Haga clic en **Usar el servidor predeterminado de Orchestrator**.

Resultados

Las conexiones con el servidor de vRealize Orchestrator integrado ya están configuradas. La carpeta de flujos de trabajo de **VCAC** y las acciones de utilidad relacionadas se importan automáticamente. La carpeta de flujos de trabajo **VCAC > ASD** contiene flujos de trabajo para la configuración de endpoints y la creación de asignaciones de recursos.

Configurar la carpeta de flujo de trabajo predeterminada de un tenant

Los administradores del sistema pueden agrupar flujos de trabajo en diversas carpetas y, después, definir categorías de flujo de trabajo por tenant. Gracias a esto, pueden proveer a usuarios de diferentes tenants de acceso a carpetas de flujo de trabajo distintas en el mismo servidor de vRealize Orchestrator.

Requisitos previos

Inicie sesión en la consola de vRealize Automation como **administrador del sistema**.

Procedimiento

- 1 Seleccione **Administración > Servicios avanzados > Carpeta de vRO predeterminada**.
- 2 Haga clic en el nombre del tenant que desee editar.
- 3 Vaya a la biblioteca de flujos de trabajo de vRealize Orchestrator y seleccione una carpeta.
- 4 Haga clic en **Agregar**.

Resultados

De este modo, ha definido la carpeta predeterminada de flujo de trabajo de vRealize Orchestrator de un tenant.

Pasos siguientes

Repita este procedimiento con todos los tenants para los que quiera definir una carpeta de flujo de trabajo predeterminada.

Iniciar sesión en la interfaz de configuración de vRealize Orchestrator

Para editar la configuración de la instancia de vRealize Orchestrator predeterminada incrustada en vRealize Automation, debe iniciar el servicio de configuración de vRealize Orchestrator e iniciar sesión en la interfaz de configuración de vRealize Orchestrator.

El servicio de configuración de vRealize Orchestrator no se inicia de forma predeterminada en el dispositivo de vRealize Automation. Debe iniciar el servicio de configuración de vRealize Orchestrator para poder acceder a la interfaz de configuración de vRealize Orchestrator.

Procedimiento

- 1 Inicie el servicio de configuración de vRealize Orchestrator.
 - a Inicie sesión en la consola de Linux del dispositivo de vRealize Automation como raíz.
 - b Escriba **service vco-configurator start** y presione Entrar.
- 2 Conéctese a la URL de vRealize Automation en un navegador web.
- 3 Haga clic en **Centro de control de vRealize Orchestrator**.

Se le redirigirá a https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter.

4 Inicie sesión en el centro de control de vRealize Orchestrator.

El nombre de usuario viene configurado por el administrador del dispositivo de vRealize Automation.

Iniciar sesión en el cliente de vRealize Orchestrator

Para realizar tareas generales de administración o editar y crear flujos de trabajo en la instancia de vRealize Orchestrator predeterminada, es necesario iniciar sesión en el cliente de vRealize Orchestrator.

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

Procedimiento

1 Conéctese a la URL de vRealize Automation en un navegador web.

2 Haga clic en **Cliente de vRealize Orchestrator**.

El archivo del cliente se ha descargado.

3 Haga clic en la descarga y siga las indicaciones.

4 En la página de inicio de sesión de vRealize Orchestrator, escriba la dirección IP o el nombre de dominio del dispositivo de vRealize Automation en el cuadro de texto **Nombre de host** y **443** como número de puerto predeterminado.

Por ejemplo, escriba *vrealize_automation_appliance_ip:443*.

5 Inicie sesión utilizando el nombre de usuario y la contraseña del cliente de vRealize Orchestrator.

Las credenciales son el nombre de usuario y la contraseña predeterminados del administrador de tenants.

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

El cliente de vRealize Orchestrator se comunica con el servidor de vRealize 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 vRealize 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 vRealize Orchestrator o cuando trate de sincronizar un flujo de trabajo con un servidor de vRealize 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 de *instalación y configuración de VMware vRealize Orchestrator*.

Pasos siguientes

Puede importar un paquete, desarrollar flujos de trabajo o establecer derechos de acceso raíz en el sistema. Consulte los temas de *uso del cliente de VMware vRealize Orchestrator* y *desarrollo con VMware vRealize Orchestrator*.

Configurar un servidor de vRealize Orchestrator externo

Puede configurar vRealize Automation para que utilice un servidor de vRealize Orchestrator externo.

Los administradores de sistemas pueden configurar el servidor de vRealize Orchestrator predeterminado de forma global para todos los tenants. Los administradores de tenants pueden configurar el servidor de vRealize Orchestrator solo para sus tenants.

Las conexiones a instancias externas de servidor de vRealize Orchestrator requieren que la cuenta de usuario disponga de permisos de visualización y ejecución en vRealize Orchestrator.

- **Autenticación Single Sign-On.** La información del usuario se transmite a vRealize Orchestrator con la solicitud de XaaS, y se conceden al usuario permisos de visualización y ejecución para el flujo de trabajo solicitado.
- **Autenticación básica.** La cuenta de usuario indicada debe ser miembro de un grupo de vRealize Orchestrator con permisos de visualización y ejecución, o bien miembro del grupo vcoadmins.

Requisitos previos

- Instalar y configurar un servidor de dispositivo de vRealize Orchestrator externo. Consulte *Instalación y configuración de vRealize Orchestrator* en el centro de información de vRealize Orchestrator en https://www.vmware.com/support/pubs/orchestrator_pubs.html.
- Inicie sesión en la consola de vRealize Automation como **administrador del sistema** o **administrador de tenants**.
- Configurar la carpeta de flujo de trabajo predeterminada. Consulte [Configurar la carpeta de flujo de trabajo predeterminada de un tenant](#).

Procedimiento

- 1 Seleccione **Administración > Configuración de vRO > Configuración del servidor**.
- 2 Haga clic en **Usar un servidor externo de Orchestrator**.
- 3 Especifique un nombre y, opcionalmente, una descripción.
- 4 Escriba la dirección IP o el nombre de DNS de la máquina en la que se ejecutará el servidor de vRealize Orchestrator en el cuadro de texto **Host**.

Nota Si el Orchestrator externo está configurado para funcionar en modo de clúster, introduzca el nombre de host o la dirección IP del servidor virtual del equilibrador de carga que distribuye las solicitudes del cliente entre los servidores de Orchestrator del clúster.

- 5 Escriba el número de puerto para la comunicación con el servidor de vRealize Orchestrator externo en el cuadro de texto **Puerto**.

El número de puerto predeterminado para vRealize Orchestrator es 8281.

- 6 Seleccione el tipo de autenticación.

Opción	Descripción
Single Sign-On	Realiza la conexión al servidor de vRealize Orchestrator mediante vCenter Single Sign-On. Esta opción solo es válida si se configuraron vRealize Orchestrator y vRealize Automation para utilizar una instancia común de vCenter Single Sign-On.
Básico	Realiza la conexión con el servidor de vRealize Orchestrator mediante el nombre de usuario y la contraseña especificados en los cuadros de texto Nombre de usuario y Contraseña . La cuenta que indique deberá ser miembro del grupo vcoadmins de vRealize Orchestrator o miembro de un grupo con permisos de visualización y ejecución.

- 7 Haga clic en **Probar conexión**.
- 8 Haga clic en **Aceptar**.

Resultados

La conexión con el servidor de vRealize Orchestrator externo queda configurada, y se importan automáticamente la carpeta de flujos de trabajo **VCAC** y las acciones de utilidades relacionadas. La carpeta de flujos de trabajo **VCAC > ASD** contiene flujos de trabajo para la configuración de endpoints y la creación de asignaciones de recursos.

Pasos siguientes

[Iniciar sesión en el cliente de vRealize Orchestrator](#)

Configurar recursos

Puede configurar recursos como endpoints, reservas y perfiles de red, e incluirlos en la definición de blueprints de vRealize Automation y en el aprovisionamiento de máquinas.

Lista de comprobación para la configuración de recursos de IaaS

Los administradores de IaaS y los administradores de tejido configuran recursos de IaaS para integrar la infraestructura existente en vRealize Automation y para asignar recursos de infraestructura a grupos empresariales de vRealize Automation.

Puede utilizar la Lista de comprobación para la configuración de recursos de IaaS para ver una descripción general de la secuencia de pasos necesarios para configurar recursos de IaaS.



Tabla 2-11. Lista de comprobación para la configuración de recursos de IaaS

Tarea	Función de vRealize Automation	Detalles
<input type="checkbox"/> Crear endpoints para la infraestructura para que los recursos sean administrados por vRealize Automation.	Administrador de IaaS	Elegir un escenario de endpoint.
<input type="checkbox"/> Crear un grupo de tejidos para organizar recursos de infraestructura en grupos y asignar uno o varios administradores para administrar dichos recursos como administradores de tejido de vRealize Automation.	Administrador de IaaS	Crear un grupo de tejidos.

Tabla 2-11. Lista de comprobación para la configuración de recursos de IaaS (continuación)

Tarea	Función de vRealize Automation	Detalles
❑ Configurar prefijos de máquina utilizados para crear nombres para las máquinas aprovisionadas a través de vRealize Automation.	Administrador de tejido	Configurar prefijos de máquina.
❑ (Opcional) Crear perfiles de red para configurar opciones de red para las máquinas aprovisionadas.	Administrador de tejido	Crear un perfil de red.
❑ Asignar recursos de infraestructura a grupos empresariales mediante la creación de reservas y, opcionalmente, perfiles de reserva y de reserva de almacenamiento.	<ul style="list-style-type: none"> ■ Administrador de IaaS si también está configurado como administrador de tejido ■ Administrador de tejido 	Configurar las reservas y las políticas de reserva.

Configurar endpoints

Los endpoints se crean y se configuran para hacer posible la comunicación de vRealize Automation con su infraestructura.

Las definiciones de los endpoints se clasifican en función del tipo:

- Nube

La categoría de nube contiene los tipos de endpoints vCloud Air, vCloud Director, Amazon EC2 y OpenStack

- IPAM

Esta categoría solo está visible si ha registrado un tipo de endpoint de IPAM de terceros, como Infoblox IPAM en un flujo de trabajo de vRealize Orchestrator.

- Administración

Esta categoría solo contiene el endpoint de vRealize Operations Manager.

- Redes y seguridad

Esta categoría contiene los tipos de endpoints de Proxy y NSX.

Un endpoint de Proxy se puede asociar a un endpoint de Amazon, vCloud Air o vCloud Director.

Un endpoint de NSX se puede asociar a un endpoint de vSphere.

- Orquestación

Esta categoría solo contiene el endpoint de vRealize Orchestrator.

- Almacenamiento

Esta categoría contiene el endpoint de NetApp ONTAP.

■ Virtual

La categoría virtual contiene los tipos de endpoints de vSphere, Hyper-V (SCVMM) y KVM (RHEV).

Puede configurar tipos de endpoints adicionales en vRealize Orchestrator y usarlos con tipos de endpoints compatibles en vRealize Automation. También puede importar y exportar endpoints mediante programación.

Para obtener información sobre cómo trabajar con endpoints después de la actualización o la migración, consulte [Consideraciones al trabajar con endpoints actualizados o migrados](#).

Elegir un escenario de endpoint

Elija un escenario de endpoint en función del tipo de endpoint de destino.

Para obtener información sobre la configuración de endpoint disponible, consulte [Referencia de la configuración de un endpoint](#).

Tabla 2-12. Elegir un escenario de endpoint

Endpoint	Más información
vSphere	Crear un endpoint de vSphere
NSX	Crear un endpoint de NSX y asociarlo a un endpoint de vSphere
vCloud Air (Suscripción o a petición)	Crear un endpoint de vCloud Air
vCloud Director	Crear un endpoint de vCloud Director
vRealize Orchestrator	Crear un endpoint de vRealize Orchestrator
vRealize Operations	Crear un endpoint de vRealize Operations Manager
Proveedor de IPAM de terceros	Crear un endpoint de proveedor de IPAM de terceros
Microsoft Azure	Crear un endpoint de Microsoft Azure
Puppet	Crear un endpoint de Puppet
Amazon	<ul style="list-style-type: none"> ■ Crear un endpoint de Amazon ■ (Opcional) Añadir un tipo de instancia de Amazon
OpenStack	Crear un endpoint de OpenStack
Proxy	Crear un endpoint de proxy y asociar a un endpoint de nube
Hyper-V (SCVMM)	Crear un endpoint de Hyper-V (SCVMM)
KVM (RHEV)	Referencia de la configuración de un endpoint
NetApp ONTAP	<ul style="list-style-type: none"> ■ Almacenamiento con un uso eficaz del espacio para el aprovisionamiento virtual ■ Referencia de la configuración de un endpoint

Tabla 2-12. Elegir un escenario de endpoint (continuación)

Endpoint	Más información
Hyper-V (independiente), XenServer o máster de grupo de Xen	Crear un endpoint de Hyper-V, XenServer o grupo de Xen
Importar endpoints	Importar o exportar endpoints mediante programación

Referencia de la configuración de un endpoint

Utilice la configuración del endpoint para definir la ubicación y las credenciales de acceso para la implementación del catálogo de servicios y la recopilación de datos.

Pestaña General

La mayoría de los endpoints de vRealize Automation contiene las siguientes opciones. Se indican las opciones que son únicas para un tipo de endpoint en concreto.

Tabla 2-13. Configuración de la pestaña **General**

Configuración	Descripción
Nombre	Escriba el nombre del endpoint.
Descripción	Escriba la descripción del endpoint.
Dirección	<p>Introduzca la dirección del endpoint con el formato de dirección de endpoint específico.</p> <ul style="list-style-type: none"> ■ Para un endpoint de KVM (RHEV) o NetApp ONTAP, la dirección debe tener uno de los formatos siguientes: <ul style="list-style-type: none"> ■ <code>https://FQDN</code> ■ <code>https://dirección_IP</code> <p>Por ejemplo: <code>https://mycompany-kvmrhev1.mycompany.local</code> o <code>netapp-1.mycompany.local</code>.</p> ■ Para un endpoint de OpenStack, la dirección debe tener el formato <code>https:// FQDN/powervc/openstack/ service</code>. Por ejemplo: <code>https://openstack.mycompany.com/powervc/openstack/admin</code>. ■ Para un endpoint de OpenStack, la dirección tener uno de los formatos siguientes: <ul style="list-style-type: none"> ■ <code>https://FQDN:500</code> ■ <code>https://dirección_IP:500</code> ■ Para un endpoint de vSphere, la dirección debe tener el formato <code>https://host/sdk</code>. ■ Para un endpoint de NSX, la dirección debe tener el formato <code>https://host</code>. ■ Para un endpoint de vRealize Orchestrator, la dirección debe tener el protocolo <code>https</code> e incluir el nombre completo o la dirección IP del servidor de vRealize Orchestrator y el número de puerto de vRealize Orchestrator; por ejemplo, <code>https://vrealize-automation-appliance-hostname:443/vco</code>. ■ Para un endpoint de vRealize Operations, la dirección debe tener el formato <code>https://host/suite-api</code>.

Tabla 2-13. Configuración de la pestaña **General** (continuación)

Configuración	Descripción
Credenciales integradas	Si decide utilizar sus credenciales integradas de vSphere, no necesita especificar un nombre de usuario ni una contraseña. Esta opción solo se aplica a los endpoints de vSphere.
Nombre de usuario	Escriba el nombre de usuario de nivel de administrador que guardó en relación con el endpoint en el formato específico del endpoint, como se sugiere en la interfaz de usuario.
Contraseña	Introduzca la contraseña de nivel de administrador que ha almacenado para el endpoint.
Proyecto de OpenStack	Introduzca un nombre de tenant de OpenStack. Esta configuración solo se aplica a los endpoints de OpenStack.
Organización	Si es el administrador de una organización, puede introducir un nombre de organización de vCloud Director. Esta opción solo se aplica a vCloud Director.
ID de clave de acceso	Introduzca el ID de clave AWS de Amazon. Esta opción solo se aplica a los endpoints de Amazon.
Clave de acceso secreta	Introduzca su clave de acceso secreta AWS de Amazon. Esta opción solo se aplica a los endpoints de Amazon.
Puerto	Escriba el valor de puerto para conectarse a la dirección de endpoint de proxy. Esta opción solo se aplica a los endpoints de proxy.
Prioridad	Introduzca un valor de prioridad como un número entero mayor o igual que 1. El valor más bajo especifica una prioridad más alta. El valor de prioridad está asociado a la propiedad personalizada integrada VMware.VCenterOrchestrator.Priority . Esta opción solo se aplica a los endpoints de vRealize Orchestrator.

Pestaña Propiedades

Todos los tipos de endpoints utilizan una pestaña de propiedades para capturar las propiedades o grupos de propiedades y configuración personalizados. Para ver ejemplos de propiedades personalizadas de determinados tipos de endpoints, consulte *Referencia de propiedades personalizadas*.

Pestaña Asociación

Puede crear una asociación a un endpoint de NSX o un endpoint de proxy, según el endpoint del que parte la asociación. Puede asociar un endpoint de vSphere a un endpoint de NSX para asignar opciones de NSX al endpoint de vSphere. También puede asociar un endpoint de vCloud Air, de vCloud Director o de Amazon a un endpoint de proxy para asignar la configuración del proxy a un endpoint de vCloud Air, de vCloud Director o de Amazon.

Probar conexión

Puede utilizar una acción de conexión de prueba para validar las credenciales, la dirección del endpoint del host y el certificado de un endpoint de vSphere, NSX o vRealize Operations Manager. Consulte [Consideraciones sobre el uso de la conexión de prueba](#).

Crear un endpoint de vSphere

Se pueden crear endpoints para que vRealize Automation pueda comunicarse con el entorno de vSphere con el fin de detectar recursos informáticos, recopilar datos y aprovisionar máquinas. También puede asociar la configuración de NSX al endpoint de vSphere al asociar a un endpoint de NSX.

Si ha actualizado o migrado un endpoint de vSphere que usaba una instancia de NSX Manager, tras la actualización se crea un endpoint de NSX que contiene una asociación entre el endpoint de vSphere de origen y un nuevo endpoint de NSX.

Si su entorno de vSphere está integrado con NSX, consulte [Crear un endpoint de NSX y asociarlo a un endpoint de vSphere](#).

Para obtener más información sobre cómo validar la conexión y la confianza del certificado, consulte [Consideraciones sobre el uso de la conexión de prueba](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.
- Debe instalar un agente de proxy de vSphere para administrar su endpoint de vSphere, y debe usar exactamente el mismo nombre para el endpoint y el agente. Para obtener información sobre la instalación del agente, consulte *Instalación de vRealize Automation*.
- Si desea usar un endpoint de vSphere para implementar máquinas virtuales a partir de plantillas de OVF, compruebe que las credenciales incluyan el privilegio de vSphereVApp.Import en la instancia de vCenter asociada con el endpoint.

El privilegio VApp.Import permite implementar una máquina de vSphere mediante la configuración importada de un OVF. Los detalles sobre este privilegio de vSphere están disponibles en la [documentación de vSphere SDK](#).

Si el OVF está alojado en un sitio web, consulte [Crear un endpoint de proxy para el sitio web de host de OVF](#).

- Si desea configurar otras opciones de red y seguridad de NSX para el endpoint de vSphere, cree un endpoint de NSX. Puede asociar al endpoint de NSX a medida que crea el endpoint de vSphere. Consulte [Crear un endpoint de NSX y asociarlo a un endpoint de vSphere](#).

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Virtual > vSphere**.
- 3 Escriba un nombre en el cuadro de texto **Nombre**.

El nombre debe coincidir con el nombre de endpoint que se proporcionó al agente de proxy de vSphere durante la instalación o, de lo contrario, se producirá un error en la recopilación de datos.

- 4 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.

- 5 Escriba la URL de la instancia de vCenter Server en el cuadro de texto **Dirección**.

Esta URL debe ser del tipo: **https://hostname/sdk** o **https://IP_address/sdk**.

Por ejemplo, **https://vsphereA/sdk**.

- 6 Introduzca su nombre de usuario y contraseña de nivel de administrador de vSphere o, en su lugar, utilice sus credenciales integradas de vSphere.

Proporcione las credenciales con permiso para modificar los atributos personalizados.

El formato del nombre de usuario es *dominio\nombre de usuario*.

Seleccione **Usar credenciales integradas** para utilizar la cuenta del servicio del agente de proxy de vSphere para conectarse a vCenter Server.

Si decide utilizar sus credenciales integradas de vSphere, no necesita especificar un nombre de usuario ni una contraseña.

- 7 (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades para el endpoint.
- 8 (opcional) Para configurar los ajustes de red y seguridad de NSX del endpoint, haga clic en **Asociaciones** y cree una asociación con un endpoint de NSX existente.

Debe tener al menos un endpoint de NSX para crear una asociación.

- 9 (opcional) Haga clic en **Probar conexión** para validar las credenciales, la dirección de endpoint de host y la confianza del certificado. Esta acción también comprueba que el agente y el servicio del administrador estén en ejecución para que se puedan recopilar datos del endpoint. La acción **Aceptar** comprueba las mismas condiciones.

La acción **Probar conexión** devuelve información acerca de cualquiera de las siguientes condiciones:

- Error de certificado

Si el certificado no se encuentra o no es de confianza, o si este ha caducado, se le solicitará que acepte una huella digital de certificado. Si no la acepta, puede seguir guardando el endpoint, pero el aprovisionamiento de máquinas podría generar errores.

- Error de agente

No se encuentra el agente de vSphere asociado. El agente debe estar en ejecución para que la prueba se realice correctamente.

- Error de host

No se puede acceder a la dirección de endpoint especificada o el servicio de administrador asociado no está en ejecución. El servicio de administrador debe estar en ejecución para que la prueba se realice correctamente.

- Error de credenciales

La combinación especificada de nombre de usuario y contraseña no es válida para el endpoint en la dirección determinada.

- Tiempo de espera

No se ha podido completar la acción de prueba en el plazo de dos minutos permitido.

Si se produce un error en la acción **Probar conexión**, puede seguir guardando el endpoint, pero el aprovisionamiento de máquinas podría generar errores.

Si hay un problema con el certificado de confianza (por ejemplo, el certificado ha caducado), se le solicitará que acepte una huella digital de certificado.

10 Haga clic en **Aceptar** para guardar el endpoint.

La acción **Aceptar** comprueba las mismas condiciones que la acción **Probar conexión**. Si encuentra cualquiera de las condiciones anteriores, devuelve un mensaje. Si se puede guardar, el error se sigue mostrando en pantalla para que pueda revisarlo.

Resultados

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Nota No cambie el nombre de los centros de datos de vSphere después de la recopilación de datos inicial. De lo contrario, se puede producir un error de aprovisionamiento.

Pasos siguientes

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [Crear un grupo de tejidos](#).

Crear un endpoint de NSX y asociarlo a un endpoint de vSphere

Puede crear un endpoint de NSX y asociar su configuración de NSX a un endpoint de vSphere existente.

Si ha actualizado o migrado un endpoint de vSphere que usaba una instancia de NSX Manager, tras la actualización se crea un endpoint de NSX que contiene una asociación entre el endpoint de vSphere de origen y un nuevo endpoint de NSX.

Para obtener información sobre la validación de la conexión de NSX y el certificado de confianza, consulte [Consideraciones sobre el uso de la conexión de prueba](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.
- Debe instalar un agente de proxy de vSphere para administrar su endpoint de vSphere, y debe usar exactamente el mismo nombre para el endpoint y el agente. Para obtener información sobre la instalación del agente, consulte *Instalación de vRealize Automation*.
- Configure las opciones de red de NSX. Consulte [Configurar opciones del componente de red y seguridad](#).
- [Crear un endpoint de vSphere](#).

Para usar las capacidades del equilibrador de carga, la seguridad y la red de NSX en vRealize Automation, cuando se utilizan las credenciales de NSX Manager debe utilizar la cuenta de administrador de NSX Manager.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Red y seguridad > NSX**.
- 3 Escriba un nombre en el cuadro de texto **Nombre**.
- 4 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 5 Escriba la URL de la instancia de NSX en el cuadro de texto **Dirección**.
Esta URL debe ser del tipo: **https://hostname** o **https://IP_address**.
Por ejemplo, **https://nsx-manager.local**.
- 6 Introduzca el nombre de usuario y la contraseña de nivel de administrador de NSX almacenados para el endpoint de NSX.
- 7 (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades para el endpoint.
- 8 Para asociar la configuración de red y seguridad de NSX con un endpoint de vSphere existente, haga clic en **Asociaciones** y seleccione un endpoint de vSphere existente.
Para poder crear la asociación, primero debe crear el endpoint de vSphere.
Un endpoint de NSX solo puede asociarse con un endpoint de vSphere. Esta restricción de asociación significa que no se puede aprovisionar una red a petición universal y asociarla a máquinas vSphere que se aprovisionan en diferentes instancias de vCenter.
- 9 (opcional) Haga clic en **Probar conexión** para validar las credenciales, la dirección de endpoint de host y la confianza del certificado. Esta acción también comprueba que el agente y el servicio del administrador estén en ejecución para que se puedan recopilar datos del endpoint. La acción **Aceptar** comprueba las mismas condiciones.

La acción **Probar conexión** devuelve información acerca de cualquiera de las siguientes condiciones:

- Error de certificado

Si el certificado no se encuentra o no es de confianza, o si este ha caducado, se le solicitará que acepte una huella digital de certificado. Si no la acepta, puede seguir guardando el endpoint, pero el aprovisionamiento de máquinas podría generar errores.

- Error de agente

No se encuentra el agente de vSphere asociado. El agente debe estar en ejecución para que la prueba se realice correctamente.

- Error de host

No se puede acceder a la dirección de endpoint especificada o el servicio de administrador asociado no está en ejecución. El servicio de administrador debe estar en ejecución para que la prueba se realice correctamente.

- Error de credenciales

La combinación especificada de nombre de usuario y contraseña no es válida para el endpoint en la dirección determinada.

- Tiempo de espera

No se ha podido completar la acción de prueba en el plazo de dos minutos permitido.

Si se produce un error en la acción **Probar conexión**, puede seguir guardando el endpoint, pero el aprovisionamiento de máquinas podría generar errores.

Si hay un problema con el certificado de confianza (por ejemplo, el certificado ha caducado), se le solicitará que acepte una huella digital de certificado.

10 Haga clic en **Aceptar** para guardar el endpoint.

La acción **Aceptar** comprueba las mismas condiciones que la acción **Probar conexión**. Si encuentra cualquiera de las condiciones anteriores, devuelve un mensaje. Si se puede guardar, el error se sigue mostrando en pantalla para que pueda revisarlo.

Resultados

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Pasos siguientes

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [Crear un grupo de tejidos](#).

Crear un endpoint de vCloud Air

Puede crear un endpoint de vCloud Air para un servicio de suscripción u OnDemand. Opcionalmente, puede asociar la configuración de proxy con el endpoint de vCloud Director creando una asociación con un endpoint de proxy.

Para obtener información sobre la consola de administración de vCloud Air, consulte la documentación de vCloud Air.

Nota Las reservas definidas para los endpoints de vCloud Air y los endpoints de vCloud Director no admiten el uso de perfiles de red para aprovisionar máquinas.

Para endpoints de vCloud Air, el nombre de organización y el nombre de vDC deben ser idénticos para una instancia de suscripción de vCloud Air.

Para obtener información acerca de cómo asociar la configuración del proxy al endpoint, consulte [Crear un endpoint de proxy y asociar a un endpoint de nube](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.

- Compruebe que tiene autorización del **administrador de infraestructura virtual** para la cuenta de OnDemand o el servicio de suscripción de vCloud Air.
- Si desea configurar una mayor seguridad y obligar a las conexiones a que atraviesen un servidor proxy, cree un endpoint de proxy. Puede crear una asociación con el endpoint de proxy mientras crea el endpoint de vCloud Director. Consulte [Crear un endpoint de proxy y asociar a un endpoint de nube](#).

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Nube > vCloud Air**.
- 3 Especifique un nombre y, opcionalmente, una descripción.
- 4 Acepte la dirección de endpoint de vCloud Air predeterminada reflejada en el cuadro de texto **Dirección** o escriba otra.

La dirección de endpoint de vCloud Air predeterminada es `https://vca.vmware.com`, según se especifica en la propiedad global `Default URL for vCloud Air endpoint`.

- 5 Escriba el nombre de usuario y la contraseña de nivel de administrador.

Las credenciales deben ser las del administrador de cuenta de OnDemand o del servicio de suscripción de vCloud Air.

El formato del nombre de usuario es *dominio\nombre de usuario*.

Proporcione las credenciales de un administrador de la organización con autorización para conectarse mediante VMware Remote Console.

- 6 (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades para el endpoint.
- 7 (opcional) Para configurar un nivel de seguridad adicional y hacer que las conexiones atraviesen un servidor proxy, haga clic en **Asociaciones** y cree una asociación con un endpoint de proxy existente.

Debe tener al menos un endpoint de proxy para crear una asociación.

- 8 Haga clic en **Aceptar**.

Pasos siguientes

[Crear un grupo de tejidos](#).

Crear un endpoint de vCloud Director

Puede crear un endpoint de vCloud Director para administrar todos los centros de datos virtuales (vDC) de vCloud Director de su entorno, o bien crear endpoints separados para administrar cada organización de vCloud Director. Opcionalmente, puede asociar la configuración de proxy con el endpoint de vCloud Director creando una asociación con un endpoint de proxy.

Para obtener información sobre los vDC de organización, consulte la documentación de vCloud Director.

No cree un solo endpoint y varios endpoints de organización individuales para la misma instancia de vCloud Director.

vRealize Automation usa un agente de para administrar los recursos de vSphere.

Nota Las reservas definidas para los endpoints de vCloud Air y los endpoints de vCloud Director no admiten el uso de perfiles de red para aprovisionar máquinas.

Para obtener información acerca de cómo asociar la configuración del proxy al endpoint, consulte [Crear un endpoint de proxy y asociar a un endpoint de nube](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.
- Si desea configurar una mayor seguridad y obligar a las conexiones a que atraviesen un servidor proxy, cree un endpoint de proxy. Puede crear una asociación con el endpoint de proxy mientras crea el endpoint de vCloud Director. Consulte [Crear un endpoint de proxy y asociar a un endpoint de nube](#).

Procedimiento

1 Seleccione **Infraestructura > Endpoint > Endpoint**.

2 Seleccione **Nuevo > Nube > vCloud Director**.

3 Especifique un nombre y, opcionalmente, una descripción.

4 Escriba la URL del servidor de vCloud Director en el cuadro de texto **Dirección**.

Esta URL debe ser del tipo *FQDN* o *IP_address*.

Por ejemplo, <https://mycompany.com>.

5 Escriba el nombre de usuario y la contraseña de nivel de administrador.

- Utilice credenciales de administrador de organización para conectarse al servidor de vCloud Director y especificar la organización en la que el usuario tiene la función de administrador. Con estas credenciales, el endpoint puede acceder únicamente a los vDC de la organización asociados. Puede añadir endpoints por cada organización adicional en la instancia de vCloud Director que se vaya a integrar con vRealize Automation.
- Para permitir el acceso a todos los vDC en la instancia de vCloud Director, utilice las credenciales de administrador del sistema de un vCloud Director y deje el cuadro de texto **Organización** vacío.

- 6 Si es un administrador de la organización, puede especificar un nombre de organización de vCloud Director en el cuadro de texto **Organización**.

Opción	Descripción
Detectar todos los vCD de organización	Si ha implementado vCloud Director en una nube privada, puede dejar el cuadro de texto Organización vacío y, así, dejar que la aplicación detecte todos los vCD de organización disponibles.
Endpoints independientes para cada vCD de organización	Escriba un nombre de organización de vCloud Director en el cuadro de texto Organización .

El nombre en **Organización** coincide con el nombre de organización de su vCloud Director, que puede aparecer también como el nombre del centro de datos virtual (vDC). Si utiliza una Virtual Private Cloud, este nombre será un identificador único con el formato M123456789-12345. En una nube dedicada, se trata del nombre que se le da al vDC de destino.

Si se conecta directamente a vCloud Director a nivel del sistema (por ejemplo, si deja vacío el campo Organización), necesitará credenciales de administrador del sistema. Si introduce una organización en el endpoint, necesitará un usuario que tenga credenciales de administrador de la organización en dicha organización.

Proporcione las credenciales con autorización para conectarse mediante VMware Remote Console.

- Para administrar todas las organizaciones con un solo endpoint, proporcione las credenciales de un administrador del sistema.
- Para administrar cada centro de datos virtual (vDC) de la organización con un endpoint independiente, cree credenciales de administrador de la organización independientes para cada vDC.

No cree un solo endpoint a nivel del sistema y varios endpoints de organización individuales para la misma instancia de vCloud Director.

- 7 (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades para el endpoint.
- 8 (opcional) Para configurar un nivel de seguridad adicional y hacer que las conexiones atraviesen un servidor proxy, haga clic en **Asociaciones** y cree una asociación con un endpoint de proxy existente.

Debe tener al menos un endpoint de proxy para crear una asociación.

- 9 Haga clic en **Aceptar**.

Pasos siguientes

[Crear un grupo de tejidos.](#)

Crear un endpoint de Amazon

Puede crear un endpoint para que se conecte a una instancia de Amazon. También puede asociar de manera opcional la configuración de proxy al endpoint de Amazon mediante la asociación a un endpoint de proxy.

vRealize Automation ofrece varios tipos de instancia de Amazon para que los use al crear blueprints, pero, si desea importar sus propios tipos de instancia, consulte [Añadir un tipo de instancia de Amazon](#).

Para obtener información acerca de cómo asociar la configuración del proxy al endpoint, consulte [Crear un endpoint de proxy y asociar a un endpoint de nube](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.
- Si desea configurar una mayor seguridad y obligar a las conexiones a que atraviesen un servidor proxy, cree un endpoint de proxy. Puede asociar el endpoint de proxy al crear el endpoint de Amazon. Consulte [Crear un endpoint de proxy y asociar a un endpoint de nube](#).

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Nube > Amazon EC2**.
- 3 Especifique un nombre y, opcionalmente, una descripción.
Este nombre suele indicar la cuenta de Amazon que se corresponde con este endpoint.
- 4 Introduzca el ID de clave de acceso de nivel administrativo para el endpoint de Amazon.
Solamente se puede asociar un endpoint con un ID de clave de acceso de Amazon.
Para obtener la clave de acceso necesaria para crear el endpoint de Amazon, debe solicitar una clave de un usuario que tenga credenciales de Administrador de acceso completo de AWS o tener configurada la política Administrador de acceso completo de AWS. Consulte la documentación de Amazon para obtener detalles.
- 5 Introduzca la clave de acceso secreta para el endpoint de Amazon.
- 6 (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades para el endpoint.
- 7 (opcional) Para configurar un nivel de seguridad adicional y hacer que las conexiones atraviesen un servidor proxy, haga clic en **Asociaciones** y cree una asociación con un endpoint de proxy existente.
Debe tener al menos un endpoint de proxy para crear una asociación.
- 8 Haga clic en **Aceptar**.

Resultados

Después de crear el endpoint, vRealize Automation empieza a recopilar datos de las regiones de Amazon Web Services.

Pasos siguientes

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [Crear un grupo de tejidos](#).

Añadir un tipo de instancia de Amazon

Hay varios tipos de instancia que se suministran con vRealize Automation y que pueden usarse con blueprints de Amazon. Un administrador puede añadir y quitar tipos de instancia.

Los tipos de instancia de máquina que administran los administradores de IaaS pueden ser utilizados por los arquitectos de blueprints para crear o editar un blueprint de Amazon. Los tipos de instancia y las imágenes de máquina de Amazon se encuentran disponibles a través del producto Amazon Web Services.

Requisitos previos


Inicie sesión en vRealize Automation como **administrador de IaaS**.

Procedimiento

- 1 Haga clic en **Infraestructura > Administración > Tipos de instancia**.
- 2 Haga clic en **Nuevo**.
- 3 Añada un nuevo tipo de instancia y especifique los siguientes parámetros.

La información relativa a los tipos de instancia de Amazon disponibles y a los valores de configuración que pueden especificarse para estos parámetros se encuentra disponible en la documentación de Amazon Web Services: *EC2 Instance Types - Amazon Web Services (AWS)* en aws.amazon.com/ec2 e *Instance Types* en docs.aws.amazon.com.

- Name
- Nombre de API
- Nombre de tipo
- Nombre de rendimiento de E/S
- CPU
- Memoria (GB)
- Almacenamiento (GB)
- Unidades informáticas

- 4 Haga clic en el icono **Guardar** (.

Resultados

Cuando los arquitectos de IaaS creen blueprints de Amazon Web Services, podrán usar los tipos de instancia que usted haya personalizado.

Pasos siguientes

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [Crear un grupo de tejidos](#).

Crear un endpoint de proxy y asociar a un endpoint de nube

Puede crear un endpoint de proxy y asociar su configuración de proxy a un endpoint de vCloud Air, vCloud Director o Amazon.

Si ha actualizado o migrado un endpoint de vCloud Air, de vCloud Director o de Amazon que usaba un administrador de proxy, se crea un endpoint de vCloud Air, de vCloud Director o de Amazon que contiene una asociación entre el endpoint de vCloud Air, de vCloud Director o de Amazon y un nuevo endpoint de proxy.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.
- Cree uno de los siguientes tipos de endpoint:
 - [Crear un endpoint de vCloud Air](#)
 - [Crear un endpoint de Amazon](#)
 - [Crear un endpoint de vCloud Director](#)

Debe tener al menos un endpoint de vCloud Air, vCloud Director o Amazon para crear una asociación del endpoint de proxy.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Red y seguridad > Proxy**.
- 3 Escriba un nombre en el cuadro de texto **Nombre**.
- 4 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 5 Escriba la URL del agente proxy instalado en el cuadro de texto **Dirección**.
- 6 Escriba el número de puerto que se va a usar para conectarse al servidor proxy en el cuadro de texto **Puerto**.
- 7 Escriba el nombre de usuario y la contraseña de nivel de administrador.
- 8 (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades para el endpoint.

- 9 Para asociar la configuración de proxy con un endpoint de vCloud Air, de vCloud Director o de Amazon, haga clic en **Associations** y seleccione uno o varios endpoints.

Debe tener al menos un endpoint de vCloud Air, de vCloud Director o de Amazon para crear una asociación.

Puede asociar el endpoint de proxy con más de un endpoint.

- 10 Haga clic en **Aceptar**.

Resultados

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Pasos siguientes

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [Crear un grupo de tejidos](#).

Crear un endpoint de proxy para el sitio web de host de OVF

Puede crear un endpoint de proxy que se utilizará al importar un OVF a un componente de máquina de vSphere en un blueprint, o bien como un conjunto de valores para un perfil de componente de imagen cuando el OVF esté alojado en un sitio web.

Para obtener información sobre la configuración de la implementación de OVF, consulte [Crear un endpoint de vSphere](#) y [Configurar un blueprint para aprovisionar desde un OVF](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Red y seguridad > Proxy**.
- 3 Escriba un nombre en el cuadro de texto **Nombre**.
- 4 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 5 Introduzca la dirección URL del sitio web que aloja el OVF en el cuadro de texto **Dirección**.
- 6 Escriba el número de puerto que se usará para conectarse al servidor proxy de sitio web en el cuadro de texto **Puerto**.
- 7 Escriba el nombre de usuario y la contraseña de nivel de administrador.
- 8 (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades para el endpoint.
- 9 Haga clic en **Aceptar**.

Resultados

Ahora puede utilizar el endpoint para definir el sitio web en el que se obtiene el OVF. Para obtener información detallada, consulte [Definir la configuración del blueprint para un componente de vSphere a través de un OVF](#) y [Definir un conjunto de valores de imagen para un perfil de componente mediante un OVF](#).

Crear un endpoint de vRealize Orchestrator

Puede crear un endpoint de vRealize Orchestrator para establecer una conexión con un servidor de vRealize Orchestrator.

Se pueden configurar varios endpoints que se conecten a diferentes servidores de vRealize Orchestrator, si bien en este sentido hay que establecer una prioridad en cada endpoint.

Durante la ejecución de flujos de trabajo de vRealize Orchestrator, vRealize Automation intenta acceder en primer lugar al endpoint de vRealize Orchestrator con la prioridad más alta. Si no puede conectar con ese endpoint, continúa con el siguiente endpoint en orden de prioridad, hasta que haya un servidor de vRealize Orchestrator disponible para ejecutar el flujo de trabajo.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Orquestación > vRealize Orchestrator**.
- 3 Especifique un nombre y, opcionalmente, una descripción.
- 4 Escriba una URL con el nombre completo o la dirección IP de servidor de vRealize Orchestrator y el número de puerto de vRealize Orchestrator.

El protocolo de transporte debe ser HTTPS. Si no se especifica ningún puerto, se utiliza el puerto predeterminado 443.

Para utilizar la instancia predeterminada de vRealize Orchestrator incrustada en el dispositivo de vRealize Automation, escriba

`https://vrealize-automation-appliance-hostname:443/vco`.

- 5 Proporcione las credenciales de vRealize Orchestrator en los cuadros de texto **Nombre de usuario** y **Contraseña** para conectarse al endpoint de vRealize Orchestrator.

Las credenciales que utilice deben tener permisos de ejecución en todos los flujos de trabajo de vRealize Orchestrator que se van a llamar desde IaaS.

Si desea utilizar la instancia predeterminada de vRealize Orchestrator incrustada en el dispositivo de vRealize Automation, el nombre de usuario es **administrator@vsphere.local** y la contraseña es la contraseña de administrador que se especificó al configurar SSO.

- 6 Escriba un entero mayor o igual que 1 en el cuadro de texto **Prioridad**.

Cuanto menor sea el valor, mayor será la prioridad.

7 (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades para el endpoint.

8 Haga clic en **Aceptar**.

Configurar endpoints de vRealize Orchestrator para redes

Si utiliza flujos de trabajo de vRealize Automation para llamar a flujos de trabajo de vRealize Orchestrator, deberá configurar el servidor o la instancia de vRealize Orchestrator como endpoint.

Para obtener información sobre cómo añadir un endpoint de vRealize Orchestrator, consulte [Crear un endpoint de vRealize Orchestrator](#).

Puede asociar un endpoint de vRealize Orchestrator a un blueprint de máquina para asegurarse de que todos los flujos de trabajo de vRealize Orchestrator para las máquinas aprovisionadas desde ese blueprint se ejecuten con dicho endpoint.

De forma predeterminada, vRealize Automation incluye una instancia de vRealize Orchestrator incrustada. Se recomienda utilizar la instancia integrada como endpoint de vRealize Orchestrator para ejecutar flujos de trabajo de vRealize Automation en un entorno de producción o prueba, o bien para crear una prueba de concepto.

Se recomienda utilizar este endpoint de vRealize Orchestrator para ejecutar flujos de trabajo de vRealize Automation en entornos de producción.

El complemento de vRealize Orchestrator se instala automáticamente con vRealize Orchestrator 7.1 y versiones posteriores. No hay ningún complemento independiente de vRealize Orchestrator para instalar.

Crear un endpoint de vRealize Operations Manager

Puede crear un endpoint de vRealize Operations Manager para establecer una conexión con una API de conjunto de hosts de vRealize Operations Manager.

Para obtener información sobre la validación de la conexión de vRealize Operations Manager y el certificado de confianza, consulte [Consideraciones sobre el uso de la conexión de prueba](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.

Procedimiento

- 1** Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2** Seleccione **Nuevo > Administración > vRealize Operations Manager**.
- 3** Especifique un nombre y, opcionalmente, una descripción.
- 4** Escriba la URL del servidor de vRealize Operations Manager en el cuadro de texto **Dirección**.
La dirección URL debe tener el formato: **https://hostname/suite-api**.
- 5** Escriba las credenciales de nombre de usuario y contraseña de vRealize Operations Manager.

- 6 (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades para el endpoint.
- 7 (opcional) Haga clic en **Probar conexión** para validar las credenciales, la dirección de endpoint de host y la confianza del certificado. Esta acción también comprueba que el agente y el servicio del administrador estén en ejecución para que se puedan recopilar datos del endpoint. La acción **Aceptar** comprueba las mismas condiciones.

La acción **Probar conexión** devuelve información acerca de cualquiera de las siguientes condiciones:

- Error de certificado

Si el certificado no se encuentra o no es de confianza, o si este ha caducado, se le solicitará que acepte una huella digital de certificado. Si no la acepta, puede seguir guardando el endpoint, pero el aprovisionamiento de máquinas podría generar errores.

- Error de agente

No se encuentra el agente de vSphere asociado. El agente debe estar en ejecución para que la prueba se realice correctamente.

- Error de host

No se puede acceder a la dirección de endpoint especificada o el servicio de administrador asociado no está en ejecución. El servicio de administrador debe estar en ejecución para que la prueba se realice correctamente.

- Error de credenciales

La combinación especificada de nombre de usuario y contraseña no es válida para el endpoint en la dirección determinada.

- Tiempo de espera

No se ha podido completar la acción de prueba en el plazo de dos minutos permitido.

Si se produce un error en la acción **Probar conexión**, puede seguir guardando el endpoint, pero el aprovisionamiento de máquinas podría generar errores.

Si hay un problema con el certificado de confianza (por ejemplo, el certificado ha caducado), se le solicitará que acepte una huella digital de certificado.

- 8 Haga clic en **Aceptar**.

Crear un endpoint de proveedor de IPAM de terceros

Si registró y configuró un tipo de endpoint de IPAM de terceros en vRealize Orchestrator, puede crear un endpoint para ese proveedor de solución de IPAM en vRealize Automation.

Si importó un paquete de vRealize Orchestrator para proporcionar una solución de IPAM externa y registró el tipo de endpoint de IPAM en vRealize Orchestrator, puede seleccionar ese tipo de endpoint de IPAM cuando cree un endpoint de vRealize Automation.

Nota Este ejemplo se basa en el uso del complemento Infoblox IPAM, que está disponible para descargar en VMware Solution Exchange. También puede usar este procedimiento si creó su propio paquete del proveedor de IPAM con el SDK de la solución IPAM que proporciona VMware. El procedimiento para importar y configurar su propio paquete de solución IPAM de terceros es el mismo que se describe en los requisitos previos.

El primer endpoint de IPAM de vRealize Automation se crea cuando se registra el tipo de endpoint para el complemento del proveedor de soluciones de IPAM en vRealize Orchestrator.

Requisitos previos

- [Obtención e importación de un paquete de proveedores de IPAM de terceros en vRealize Orchestrator.](#)
- [Ejecutar el flujo de trabajo para registrar un tipo de endpoint de IPAM de terceros en vRealize Orchestrator.](#)
- Inicie sesión en vRealize Automation como **administrador de IaaS**.

En este ejemplo, cree un endpoint de IPAM Infoblox usando un tipo de endpoint que haya registrado en vRealize Orchestrator en relación con el complemento o el paquete de proveedor de IPAM de terceros.

Procedimiento

- 1** Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2** Seleccione **Nuevo > IPAM > Tipo de endpoint de IPAM**.

Seleccione un tipo de endpoint de proveedor de IPAM externo registrado como, por ejemplo, Infoblox. Los endpoints de proveedores de IPAM externos solo están disponibles si se ha importado un paquete de vRealize Orchestrator de terceros y se han ejecutado los flujos de trabajo del paquete para registrar el tipo de endpoint.

En Infoblox IPAM, solo se enumeran los tipos de endpoint de IPAM principales. Puede utilizar propiedades personalizadas para especificar tipos de endpoint de IPAM secundarios.

En este ejemplo, seleccione un tipo de endpoint de IPAM externo registrado; por ejemplo, **Infoblox NIOS**.

- 3** Especifique un nombre y, opcionalmente, una descripción.

- 4 Introduzca la ubicación del endpoint de IPAM registrado en el cuadro de texto **Dirección**, con el formato de URL específico del proveedor (por ejemplo, `https://nombre_host/nombre`).

Por ejemplo, podría crear varios endpoints de IPAM, como `https://nsx62-scale-infoblox` y `https://nsx62-scale-infoblox2`, al registrar el tipo de endpoint de IPAM en vRealize Orchestrator. Introduzca un tipo de endpoint registrado principal. Para especificar además uno o varios endpoints de IPAM secundarios, puede usar propiedades personalizadas para emular los atributos extensibles que son específicos del proveedor de soluciones de IPAM.

- 5 Introduzca el nombre de usuario y la contraseña que son necesarios para acceder a la cuenta del proveedor de soluciones de IPAM.

Las credenciales de la cuenta del proveedor de soluciones de IPAM son necesarias para crear, configurar y editar el endpoint cuando se trabaja en vRealize Automation. vRealize Automation utiliza las credenciales de endpoint de IPAM para comunicarse con el tipo de endpoint especificado (por ejemplo, Infoblox) para asignar direcciones IP y realizar otras operaciones. Este comportamiento es similar al modo en que vRealize Automation utiliza las credenciales de endpoint de vSphere.

- 6 (opcional) Haga clic en **Propiedades** y agregue propiedades de endpoint que sean relevantes para el proveedor de soluciones IPAM específico.

Cada proveedor de soluciones de IPAM, como Infoblox y Bluecat, utiliza atributos extensibles únicos que se pueden emular mediante las propiedades personalizadas de vRealize Automation. Por ejemplo, Infoblox utiliza atributos extensibles para diferenciar los endpoints principales y secundarios.

- 7 Haga clic en **Aceptar**.

Pasos siguientes

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [Crear un grupo de tejidos](#).

Crear un endpoint de Microsoft Azure

Puede crear un endpoint de Microsoft Azure para facilitar una conexión con credenciales entre vRealize Automation y una implementación de Azure.

Un endpoint establece una conexión a un recurso (en este caso, una instancia de Azure) que puede utilizar para crear blueprints de máquina virtual. Debe tener un endpoint de Azure para usar como base de los blueprints para aprovisionar máquinas virtuales de Azure. Si cuenta con varias suscripciones a Azure, necesita endpoints para cada identificador de suscripción.

Opcionalmente, puede crear una conexión de Azure directamente desde vRealize Orchestrator utilizando el comando Agregar una conexión de Azure que se encuentra en **Biblioteca > Azure > Configuración** en el árbol de flujo de trabajo de vRealize Orchestrator. En la mayoría de los casos, la opción preferida es la creación de una conexión mediante la configuración del endpoint, tal como se describe en este documento.

Los endpoints de Azure son compatibles con la funcionalidad XaaS y vRealize Orchestrator. Puede crear, eliminar o editar un endpoint de Azure. Tenga en cuenta que si realiza cambios en un endpoint existente y no ejecuta ninguna actualización en el portal de Azure a través de la conexión actualizada por varias horas, debe reiniciar el servicio vRealize Orchestrator mediante el comando `service vco-service restart`. Si no reinicia el servicio, pueden producirse errores.

Requisitos previos

- Configure una instancia de Microsoft Azure y obtenga una suscripción válida a Microsoft Azure a partir de la pueda usar el identificador de suscripción. Consulte <http://www.vaficionado.com/2016/11/using-new-microsoft-azure-endpoint-vrealize-automation-7-2/> para obtener más información sobre cómo configurar Azure y obtener un identificador de suscripción.
- Compruebe que la implementación de vRealize Automation tenga al menos un tenant y un grupo empresarial.
- Cree una aplicación de Active Directory tal como se describe en <https://azure.microsoft.com/es-es/documentation/articles/resource-group-create-service-principal-portal>.
- Tome nota de la siguiente información relacionada con Azure, ya que la necesitará durante la configuración del endpoint y el blueprint.
 - ID de suscripción
 - ID de tenant
 - nombre de la cuenta de almacenamiento
 - nombre del grupo de recursos
 - ubicación
 - nombre de la red virtual
 - identificador de la aplicación cliente
 - clave secreta de aplicación cliente
 - URN de imagen de la máquina virtual
- Existen ajustes exclusivos necesarios para crear e implementar las aplicaciones de nube de Azure en el entorno de China. Para obtener información relacionada, consulte <https://docs.microsoft.com/en-us/azure/china/china-get-started-developer-guide>. Al crear un endpoint de Azure de vRealize Automation para China, la URL del servicio, la URL de inicio de sesión y la URL de almacenamiento se deben especificar de la siguiente manera:
 - URL de servicio: `https://management.chinacloudapi.cn`
 - URL de inicio de sesión: `https://login.chinacloudapi.cn/`
 - URL de almacenamiento: `https://storage_account_name.blob.core.chinacloudapi.cn/`

La implementación de Azure de vRealize Automation admite un subconjunto de regiones admitidas de Microsoft Azure. Consulte [Regiones admitidas de Azure](#).

- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Configuración de vRO > Endpoints**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 En la pestaña Complemento, haga clic en el menú desplegable **Complemento** y seleccione **Complemento Azure**.
- 4 Haga clic en **Siguiente**.
- 5 Especifique un nombre y, opcionalmente, una descripción.
- 6 Haga clic en **Siguiente**.
- 7 Rellene los cuadros de texto de la pestaña **Detalles** según corresponda para el endpoint.

Parámetro	Descripción
Configuración de conexión	
Conexión de Azure	
Nombre de la conexión	Nombre único para la nueva conexión de endpoint. Este nombre aparece en la interfaz de vRealize Orchestrator para ayudarlo a identificar una conexión determinada.
Identificador de suscripción de Azure	Identificador de la suscripción de Azure. El identificador define las cuentas de almacenamiento, las máquinas virtuales y otros recursos de Azure a los que puede acceder.
Configuración del administrador de recursos	
URI del servicio Azure	El URI a través del cual obtiene acceso a la instancia de Azure. El valor predeterminado de <code>https://management.azure.com/</code> es apropiado para muchas implementaciones típicas.
URI de almacenamiento de Azure	El URI a través del cual se obtiene acceso a la instancia de almacenamiento de Azure.
Identificador de tenant	El identificador de tenant de Azure que desea que use el endpoint.
Identificador del cliente	El identificador de cliente de Azure que desea que use el endpoint. Se asigna al crear una aplicación de Active Directory.
Secreto de cliente	La clave que se utiliza con un identificador de cliente de Azure. Esta clave se asigna al crear una aplicación de Active Directory.

Parámetro	Descripción
URL de inicio de sesión	La URL que se usa para acceder a la instancia de Azure. El valor predeterminado de <code>https://login.windows.net/</code> es apropiado para muchas implementaciones típicas.
Configuración de proxy	
Host de proxy	Si su empresa utiliza un servidor web proxy, introduzca el nombre de host de dicho servidor.
Puerto de proxy	Si su empresa utiliza un servidor web proxy, introduzca el número de puerto de dicho servidor.

- 8** (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades personalizadas.

- 9** Haga clic en **Finalizar**.

Pasos siguientes

Cree los grupos de recursos, las cuentas de almacenamiento y los grupos de seguridad de red adecuados en Azure. También debe crear equilibradores de carga si son apropiados para su implementación.

Acción	Opciones
Crear un grupo de recursos de Azure	<ul style="list-style-type: none"> ■ Cree el grupo de recursos desde el portal de Azure. Consulte la documentación de Azure para obtener instrucciones específicas. ■ Use el flujo de trabajo adecuado de vRealize Orchestrator, que se encuentra en <code>Library/Azure/Resource/Create resource group</code>. ■ En vRealize Automation, cree y publique un blueprint XaaS que contenga el flujo de trabajo de vRealize Orchestrator. Puede solicitar el grupo de recursos después de adjuntarlo al servicio y las autorizaciones. Tenga en cuenta que vRealize Automation no admite ni administra el tipo de recurso Grupo de recursos.
Crear una cuenta de almacenamiento de Azure	<ul style="list-style-type: none"> ■ Use Azure para crear una cuenta de almacenamiento. Consulte la documentación de Azure para obtener instrucciones específicas. ■ Use el flujo de trabajo adecuado de vRealize Orchestrator, que se encuentra en <code>Library/Azure/Storage/Create storage account</code>. ■ En vRealize Automation, cree y publique un blueprint XaaS que contenga el flujo de trabajo de vRealize Orchestrator. Puede solicitar la cuenta de almacenamiento después de adjuntarla al servicio y las autorizaciones.
Crear un grupo de seguridad de red de Azure	<ul style="list-style-type: none"> ■ Use Azure para crear un grupo de seguridad. Consulte la documentación de Azure para obtener instrucciones específicas. ■ Use el flujo de trabajo adecuado de vRealize Orchestrator, que se encuentra en <code>Library/Azure/Network/Create Network security group</code>. ■ En vRealize Automation, cree y publique un blueprint XaaS que contenga el flujo de trabajo de vRealize Orchestrator. Puede solicitar el grupo de seguridad después de adjuntarlo al servicio y las autorizaciones.

Regiones admitidas de Azure

La implementación de Azure de vRealize Automation admite un subconjunto de regiones admitidas de Microsoft Azure.

Las siguientes regiones de Azure son compatibles con la implementación de Azure en vRealize Automation.

- | | |
|-----------------------------|---------------------------|
| ■ Asia del Este | ■ Este de Australia |
| ■ Sudeste de Asia | ■ Sudeste de Australia |
| ■ Región Central de EE. UU. | ■ Sur de India |
| ■ Este de EE. UU. | ■ Centro de India |
| ■ Este de EE. UU. 2 | ■ Oeste de India |
| ■ Oeste de EE. UU. | ■ Centro de Canadá |
| ■ Oeste de EE. UU. 2 | ■ Este de Canadá |
| ■ Centro-norte de EE. UU. | ■ Centro-oeste de EE. UU. |
| ■ Centro-sur de EE. UU. | ■ Centro de Corea |
| ■ Europa del Norte | ■ Sur de Corea |
| ■ Europa Occidental | ■ Oeste de Reino Unido |
| ■ Oeste de Japón | ■ Sur de Reino Unido |
| ■ Este de Japón | ■ Este de China |
| ■ Sur de Brasil | ■ Norte de China |

Crear un endpoint de Puppet

Puede crear un endpoint de Puppet para que se puedan añadir componentes de administración de configuración de Puppet a las máquinas virtuales de vSphere. Estos componentes permiten usar un maestro de Puppet que obligue a usar una administración de la configuración en las máquinas virtuales.

Un endpoint establece una conexión a un recurso externo, en este caso, a una instancia del maestro de Puppet. El endpoint le permite colocar los componentes de administración de configuración de Puppet en los blueprints de máquina virtual de vSphere. Las máquinas virtuales aprovisionadas basadas en estos blueprints contienen un agente de Puppet que facilita el control mediante el maestro de Puppet asociado.

Para obtener más información sobre el complemento de Puppet y una demostración de su configuración, consulte <https://www.youtube.com/watch?v=P-VglzE9o-o>.

Requisitos previos

- Instale y configure Puppet Enterprise según corresponda en su entorno.
- Descargue e instale el complemento de Puppet versión 3.0 en la implementación de vRealize Orchestrator. Puede descargar el complemento de <https://marketplace.vmware.com/vsx/solutions/puppet-plugin-for-vrealize-automation?ref=search>. Consulte https://docs.puppet.com/pe/latest/vro_intro.html para obtener información sobre la forma de instalar y utilizar el complemento.

Procedimiento

- 1 Seleccione **Administración > Configuración de vRO > Endpoints**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 En la pestaña Complemento, haga clic en el menú desplegable **Complemento** y seleccione **Complemento de Puppet**.
- 4 Haga clic en **Siguiente**.
- 5 Especifique un nombre y, opcionalmente, una descripción.

6 Haga clic en **Siguiente**.

7 Rellene los cuadros de texto de la pestaña **Detalles** según corresponda para el endpoint.

Parámetro	Descripción
Nombre para mostrar de este maestro de Puppet	Nombre del maestro de Puppet asociado a la conexión de endpoint. Este nombre aparece en la interfaz de vRealize Orchestrator para ayudarle a identificar una conexión determinada.
Nombre de host o dirección IP	FQDN o dirección IP del maestro de Puppet usado por este endpoint.
Puerto SSH	Puerto definido para uso de este maestro de Puppet con una comunicación segura.
Nombre de usuario de control de acceso basado en funciones SSH	Nombre de usuario de control de acceso basado en funciones necesario para conectar con el maestro de Puppet.
Contraseña de control de acceso basado en funciones SSH	Contraseña de control de acceso basado en funciones necesaria para la configuración segura con el maestro de Puppet.
¿Usar sudo para los comandos del shell en este maestro?	Seleccione esta opción si desea que los administradores puedan usar comandos de Sudo en servidores Linux relativos a opciones de seguridad en las máquinas virtuales basadas en este endpoint.

8 Haga clic en **Aceptar**.

Resultados

Ahora puede añadir componentes de administración de configuración de Puppet a los blueprints de vSphere, lo que le permitirá implementar máquinas virtuales de vSphere que contienen los agentes de Puppet.

Crear un endpoint de Hyper-V (SCVMM)

Se pueden crear endpoints para que vRealize Automation pueda comunicarse con el entorno de SCVMM con el fin de detectar recursos informáticos, recopilar datos y aprovisionar máquinas.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.
- Debe instalar y configurar un agente de DEM para administrar su endpoint de Hyper-V (SCVMM). Para obtener información, consulte los requisitos de SCVMM en *Instalación de vRealize Automation*.

Para obtener información relacionada, consulte [Preparar el entorno de SCVMM](#).

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Virtual > Hyper-V (SCVMM)**.
- 3 Escriba un nombre en el cuadro de texto **Nombre**.

- 4 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 5 Escriba la URL del endpoint en el cuadro de texto **Dirección**.
Esta URL debe ser del tipo: *FQDN* o *IP_address*.
Por ejemplo: **mycompany-scvmm1.mycompany.local**.
- 6 Introduzca el nombre de usuario y la contraseña de nivel administrativo que ha almacenado para este endpoint.
Si todavía no ha almacenado las credenciales, puede hacerlo ahora.
- 7 (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades para el endpoint.
- 8 Haga clic en **Aceptar**.

Resultados

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Pasos siguientes

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [Crear un grupo de tejidos](#).

Crear un endpoint de OpenStack

El endpoint se crea para que vRealize Automation pueda comunicarse con su instancia de OpenStack.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.
- Verifique que los DEM de vRealize Automation estén instalados en una máquina que cumple con los requisitos de OpenStack o PowerVC. Consulte *Instalación de vRealize Automation*.
- Verifique que el tipo de OpenStack sea compatible actualmente. Consulte *Matriz de soporte de vRealize Automation*.

Tras actualizar o migrar desde una instalación de vRealize Automation anterior, si se produce un error en la recopilación de datos de los endpoints de OpenStack, puede añadir la propiedad personalizada `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` a cada endpoint de OpenStack de Keystone V3 para especificar un nombre de dominio válido y habilitar la recopilación de datos.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Nube > OpenStack**.
- 3 Especifique un nombre y, opcionalmente, una descripción.

4 Escriba la URL del endpoint en el cuadro de texto **Dirección**.

Opción	Descripción
PowerVC	La dirección URL debe tener el formato http://myPowerVC.com:5000 o http://FQDN:5000 .
OpenStack	Esta URL debe tener el formato FQDN:5000 o IP_address:5000 . No incluya el sufijo /v2.0 en la dirección del endpoint.

5 Introduzca el nombre de usuario y la contraseña de nivel administrativo.

Las credenciales que proporcione deben ser de la función de administrador del tenant de OpenStack asociado al endpoint.

6 Escriba un nombre de tenant de OpenStack en el cuadro de texto **Proyecto de OpenStack**.

Si configura varios endpoints con distintos tenants de OpenStack, cree políticas de reserva para cada tenant. De esta forma, las máquinas se aprovisionarán en los recursos del tenant adecuado.

7 Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades para el endpoint.

Si Keystone V3 está en vigor, agregue la propiedad personalizada de `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` para designar un dominio específico.

8 Haga clic en **Aceptar**.

Resultados

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Pasos siguientes

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [Crear un grupo de tejidos](#).

Crear un endpoint de Hyper-V, XenServer o grupo de Xen

Se pueden crear endpoints para que vRealize Automation pueda comunicarse con el entorno de Hyper-V, XenServer o el grupo de Xen principal con el fin de detectar recursos informáticos, recopilar datos y aprovisionar máquinas.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.
- Un administrador del sistema debe instalar un agente de proxy con credenciales almacenadas correspondientes al endpoint. Consulte *Instalación de vRealize Automation*.

Procedimiento

1 Seleccione **Infraestructura > Endpoint > Agentes**.

- 2 Escriba el nombre DNS completo del servidor de Hyper-V, XenServer o del grupo de Xen principal en el cuadro de texto **Recurso informático**.

Nota Para un endpoint de grupo de Xen, debe introducir el nombre del grupo principal. Para evitar entradas duplicadas en la tabla de recursos informáticos de vRealize Automation, especifique una dirección que coincida con la configurada en el grupo de Xen principal. Por ejemplo, si la dirección principal del grupo de Xen usa el nombre de host, escriba el nombre de host en lugar del FQDN. Si la dirección principal del grupo de Xen usa un FQDN, entonces escriba el FQDN.

- 3 En el menú desplegable **Nombre de agente de proxy**, seleccione el agente de proxy que el administrador del sistema instaló para este endpoint.
- 4 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 5 Haga clic en **Aceptar**.

Resultados

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Pasos siguientes

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [Crear un grupo de tejidos](#).

Consideraciones sobre el uso de la conexión de prueba

Puede utilizar una acción de conexión de prueba para validar las credenciales, la dirección del endpoint del host y el certificado de un endpoint de vSphere, NSX o vRealize Operations Manager.

Esta acción también comprueba que el agente y el servicio del administrador estén en ejecución para que se puedan recopilar datos del endpoint.

La acción **Probar conexión** devuelve información acerca de cualquiera de las siguientes condiciones:

- Error de certificado

Si el certificado no se encuentra o no es de confianza, o si este ha caducado, se le solicitará que acepte una huella digital de certificado. Si no la acepta, puede seguir guardando el endpoint, pero el aprovisionamiento de máquinas podría generar errores.

- Error de agente

No se encuentra el agente de vSphere asociado. El agente debe estar en ejecución para que la prueba se realice correctamente.

- Error de host

No se puede acceder a la dirección de endpoint especificada o el servicio de administrador asociado no está en ejecución. El servicio de administrador debe estar en ejecución para que la prueba se realice correctamente.

- **Error de credenciales**

La combinación especificada de nombre de usuario y contraseña no es válida para el endpoint en la dirección determinada.

- **Tiempo de espera**

No se ha podido completar la acción de prueba en el plazo de dos minutos permitido.

Si recibe errores al ejecutar **Probar conexión** en endpoints actualizados o migrados, consulte [Consideraciones al trabajar con endpoints actualizados o migrados](#) para ver qué pasos hay que seguir para establecer el certificado de confianza.

Importar o exportar endpoints mediante programación

Para importar y exportar endpoints mediante programación en vRealize Automation 7.3 o posterior debe usar cualquiera de las nuevas API de REST para el servicio de configuración de endpoints de vRealize Automation o bien vRealize CloudClient.

La documentación de vRealize CloudClient contiene todo el formato, los ejemplos y la información de uso correspondientes a la línea de comandos.

Puede descargar la documentación y la aplicación de vRealize CloudClient en la página del producto vRealize CloudClient de <https://developercenter.vmware.com/tool/cloudclient>.

Ver los orígenes de endpoint y ejecutar la recopilación de datos

Puede ver la máquina y el recurso informático que están asociados a un endpoint específico. También puede iniciar manualmente la recopilación de datos.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.
- Compruebe que existe al menos un endpoint.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione una fila de endpoint existente y haga clic en **Acciones**.

Seleccione una de las siguientes acciones disponibles.

- Haga clic en **Ver recursos informáticos** para abrir la página **Infraestructura > Recursos informáticos**. Puede usar esta página para ver y editar la configuración de los recursos informáticos.
- Haga clic en **Ver máquinas** para abrir la página **Infraestructura > Máquinas administradas**.

- Haga clic en **Recopilación de datos** para abrir la página de recopilación de datos e iniciar la recopilación de datos para el endpoint. Puede actualizar la página para que se muestre el estado actual de la solicitud.

Consideraciones al trabajar con endpoints actualizados o migrados

Después de actualizar o migrar desde una versión anterior a vRealize Automation 7.3, debe tener en cuenta las siguientes consideraciones para comprender y actuar correctamente.

Esta información se aplica a los endpoints que se hayan actualizado o migrado a esta versión de vRealize Automation.

- Cuando se actualiza o migra desde una versión previa de vRealize Automation 7.3, cada endpoint de Amazon, de vCloud Director y de vCloud Air que contenga configuración de proxy se asocia a un nuevo endpoint de proxy que contiene su configuración de proxy.

Tras la actualización o migración, el nuevo nombre de endpoint de proxy es Proxy_YYYYYY, donde YYYYYY es un hash de la dirección URL, el puerto y las credenciales del proxy. Si ha utilizado la misma configuración de proxy (por ejemplo la misma URL, el mismo puerto y las mismas credenciales) en un endpoint diferente (por ejemplo, un endpoint de vCloud Air o de Amazon), después de la actualización o migración solo habrá un endpoint de proxy y una asociación entre el endpoint de vCloud Air y el de Amazon con el nuevo endpoint de proxy. Un endpoint de proxy se puede asociar a más de un endpoint de Amazon, de vCloud Air o de vCloud Director.

- Cuando se actualizan o migran endpoints de vSphere que contienen la configuración de NSX Manager, cada endpoint de vSphere se asocia a un nuevo endpoint de NSX que contiene la configuración de NSX Manager.

Tras la actualización o migración, el nombre de endpoint de NSX es NSX_XXXXXX, donde XXXXXX es el nombre del endpoint principal de vRealize Automation en la versión previa de vSphere 7.3.

- Cuando finalice la actualización o migración de vRealize Automation, un administrador de la infraestructura puede cambiar los nuevos nombres de endpoint de NSX y proxy.
- La configuración de seguridad predeterminada relativa a endpoints actualizados o migrados consiste en no aceptar certificados que no sean de confianza.
- Si usaba certificados que no eran de confianza, después de actualizar o migrar desde una instalación de vRealize Automation anterior, deberá hacer lo siguiente para que todos los endpoints de vSphere y de NSX permitan la validación de certificados. De lo contrario, las operaciones de endpoint generarán errores de certificado. Para obtener más información, consulte los artículos de la base de conocimientos de VMware *La comunicación del endpoint*

se interrumpe después de actualizar a vRA 7.3 (2150230) en <http://kb.vmware.com/kb/2150230> y *Cómo descargar e instalar certificados raíz de vCenter Server para evitar advertencias de certificado del navegador web* (2108294) en <http://kb.vmware.com/kb/2108294>.

- a Después de la actualización o migración, inicie sesión en la máquina del agente de vSphere de vRealize Automation y reinicie los agentes de vSphere en la pestaña **Servicios**.

Es posible que no todos los agentes se reinicien con la migración, de modo que puede que sea necesario reiniciarlos manualmente.

- b Espere a que al menos un informe de ping finalice. Un informe de ping tarda uno o dos minutos en finalizar.
- c Cuando los agentes de vSphere hayan empezado a recopilar datos, inicie sesión en vRealize Automation como un administrador de IaaS.
- d Haga clic en **Infraestructura > Endpoints > Endpoints**.
- e Edite un endpoint de vSphere y haga clic en **Probar conexión**.
- f Si aparece un mensaje de certificado, haga clic en **Aceptar** para aceptar el certificado.

Si no aparece un mensaje de certificado, es posible que el certificado esté actualmente almacenado en una entidad raíz de confianza de la máquina de Windows que aloja el servicio del endpoint, por ejemplo, como una máquina de agente de proxy o una máquina de DEM.
- g Haga clic en **Aceptar** para confirmar la aceptación de certificado y guardar el endpoint.
- h Repita este procedimiento por cada endpoint de vSphere.
- i Repita este procedimiento por cada endpoint de NSX.

Si la acción **Probar conexión** finaliza correctamente, pero alguna de las operaciones de aprovisionamiento o de recopilación de datos genera errores, puede instalar el mismo certificado en todas las máquinas de agente que sirvan al endpoint y en todas las máquinas DEM. Si lo prefiere, puede desinstalar el certificado de las máquinas existentes y repetir el procedimiento anterior en el endpoint con el error.

- Las API de REST de vRealize Automation que se usaron para crear, editar y eliminar endpoints mediante programación en vRealize Automation 7.2 y versiones anteriores ya no son compatibles en vRealize Automation 7.3 y versiones posteriores. Para crear, editar y eliminar endpoints mediante programación en vRealize Automation 7.3 o versiones posteriores, debe usar cualquiera de las nuevas API de REST endpoint-configuration-service de vRealize Automation, o bien utilizar vRealize CloudClient.

- Tras actualizar o migrar desde una instalación de vRealize Automation anterior, si se produce un error en la recopilación de datos de los endpoints de OpenStack, puede añadir la propiedad personalizada `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` a cada endpoint de OpenStack de Keystone V3 para especificar un nombre de dominio válido y habilitar la recopilación de datos.
- Cuando se actualiza un endpoint de IPAM de terceros, como Infoblox IPAM, se actualiza el paquete de vRealize Orchestrator que contiene el flujo de trabajo de `RegisterIPAMEndpoint`. Es posible que tenga que volver a ejecutar el flujo de trabajo en vRealize Orchestrator cuando se complete la actualización de vRealize Automation.
- Para hacer un cambio de credenciales en varios endpoints, puede editar los endpoints de forma individual o utilizar vRealize CloudClient para realizar una actualización masiva.
- Algunos tipos de endpoint, como vCloud Air y vCloud Director, no se pueden actualizar ni migrar directamente desde vRealize Automation 6.2.x a vRealize Automation 7.3 o versiones posteriores.
- Tras actualizar o migrar correctamente a vRealize Automation 7.3, si la página **Infraestructura > Endpoints** no muestra ningún endpoint o solo muestra algunos tipos de endpoints y endpoints, consulte el [artículo 2150252 de la Base de conocimientos](#) para encontrar una solución alternativa.

Consideraciones al eliminar endpoints

Puede eliminar ciertos tipos de endpoint en determinadas condiciones.

- Se pueden eliminar los endpoints cuyos datos no se hayan recopilado.
- Se puede eliminar un endpoint de OpenStack, Amazon y VRO si se han recopilado sus datos, pero no tiene reservas. Sin embargo, otros tipos de endpoints no se pueden eliminar si se han recopilado los datos.
- Se pueden eliminar los endpoints de IPAM de terceros si no están asociados a un perfil de red.
- Cuando se elimina un endpoint de vSphere, el aviso de confirmación muestra las siguientes dependencias:
 - Se han recopilado los datos del endpoint.
 - Se hace referencia al endpoint en una reserva que asigna a un recurso informático. No se puede eliminar un endpoint al que se hace referencia en una reserva. Las reservas requieren un recurso informático.
 - El endpoint contiene una plantilla a la que se hace referencia en un blueprint existente. El blueprint no se elimina cuando se elimina el endpoint.
 - Algunas máquinas virtuales que están en uso utilizan el endpoint.

- Los endpoints se pueden eliminar mediante programación usando las API de REST del servicio de configuración de endpoints CREATE, EDIT y DELETE de vRealize Automation que se incluyen en vRealize Automation 7.3 o mediante vRealize CloudClient. No es posible eliminar endpoints mediante las API de REST del servicio de configuración de endpoints incluidas en las versiones anteriores a vRealize Automation 7.3.

Solucionar problemas cuando no se encuentra el endpoint de vSphere adjunto

Cuando se produce un problema en la recopilación de datos de un endpoint de vSphere, puede deberse a una falta de concordancia entre el nombre de proxy y el nombre de endpoint.

Problema

Se produce un error en la recopilación de datos de un endpoint de vSphere. Los mensajes de log devuelven un error similar al siguiente:

Se detectó esta excepción: No se encuentra el endpoint 'vCenter' adjunto.

Causa

El nombre de endpoint que configure en vRealize Automation debe ser el mismo que se proporcionó al agente de proxy de vSphere durante la instalación. Se produce un error en la recopilación de datos de un endpoint de vSphere si el nombre de endpoint y el nombre de agente de proxy no coinciden. Hasta que se configure un nombre de endpoint coincidente, los mensajes de log devuelven un error similar al siguiente:

Se detectó esta excepción: No se encuentra el endpoint '*expected endpoint name*' adjunto.

Solución

- 1 Seleccione **Infraestructura > Supervisión > Log**.
- 2 Busque un mensaje de error que indique que no se encuentra el endpoint adjunto, como Attached Endpoint Cannot be Found (No se puede encontrar el endpoint adjunto).

Por ejemplo:

Se detectó esta excepción: No se encuentra el endpoint '*expected endpoint name*' adjunto.

- 3 Edite el endpoint de vSphere para que coincida con el nombre de endpoint esperado que se muestra en el mensaje de log.
 - a Seleccione **Infraestructura > Endpoint > Endpoint**.
 - b Haga clic en el nombre del endpoint para editarlo.
 - c Escriba el nombre de endpoint esperado en el cuadro de texto **Nombre**.
 - d Haga clic en **Aceptar**.

Solución

El agente de proxy puede conmutarse con el endpoint y la recopilación de datos se realiza correctamente.

Crear un grupo de tejidos

Puede organizar recursos de infraestructura en grupos de tejidos y asignar uno o varios administradores de tejido para que administren los recursos del grupo de tejido.

Se necesitan grupos de tejidos en los endpoints virtuales y de nube. Puede conceder la función de administrador de tejidos a varios usuarios. Para ello, debe añadir varios usuarios, de uno en uno, o elegir un grupo de almacén de identidades o un grupo personalizado como administrador de tejidos.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de IaaS**.
- Cree al menos un endpoint. Consulte [Elegir un escenario de endpoint](#).

Procedimiento

- 1 Seleccione **Infraestructura > Grupos de tejidos**.
- 2 Haga clic en **Nuevo grupo de tejidos**.
- 3 Escriba un nombre en el cuadro de texto **Nombre**.
- 4 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 5 Escriba un nombre de usuario o un nombre de grupo en el cuadro de texto **Administradores de tejido** y presione Entrar.

Repita este paso para añadir varios usuarios o grupos a la función.

- 6 Haga clic en uno o varios **Recursos informáticos** para incluirlos en su grupo de tejidos.

Durante la recopilación de datos solo se detectan los recursos existentes en los clústeres seleccionados para el grupo de tejidos. Por ejemplo, solo las plantillas existentes en los clústeres seleccionados se detectan y pueden clonarse en las reservas que cree para los grupos empresariales.

- 7 Haga clic en **Aceptar**.

Resultados

Los administradores de tejido ya pueden configurar prefijos de máquina. Consulte [Configurar prefijos de máquina](#).

Los usuarios que han iniciado sesión en vRealize Automation deben cerrar la sesión de vRealize Automation y volver a iniciarla antes de poder desplazarse hasta las páginas a las que se les ha concedido acceso.

Configurar prefijos de máquina

Puede crear prefijos de máquina que se utilizan para crear los nombres de las máquinas aprovisionadas a través de vRealize Automation. Se requiere un prefijo de máquina para definir un componente de máquina en el lienzo de diseño del blueprint.

Un prefijo es un nombre base que debe ir seguido de un contador con un número determinado de dígitos. Cuando se agotan todos los dígitos, vRealize Automation vuelve a comenzar con el primer número.

Los prefijos de máquina deben cumplir las siguientes limitaciones:

- Solo pueden contener letras ASCII desde la a hasta la z (sin distinguir mayúsculas de minúsculas), los dígitos 0 a 9 y el guión (-).
- No deben comenzar con un guión.
- No se pueden usar otros símbolos, caracteres de puntuación ni espacios en blanco.
- No deben tener más de 15 caracteres, incluidos los dígitos, en línea con el límite de 15 caracteres en los nombres de hosts de Windows.

Los nombres de hosts más largos aparecen truncados cuando se aprovisiona una máquina y se actualizan la siguiente vez que se ejecuta la recopilación de datos. Sin embargo, en el aprovisionamiento de WIM los nombres no se truncan y el aprovisionamiento produce un error cuando el nombre especificado tiene más de 15 caracteres.

- vRealize Automation no admite que haya varias máquinas virtuales con el mismo nombre en una sola instancia. Si elige una convención de nomenclatura que provoque la superposición de nombres de máquina, vRealize Automation no aprovisiona la máquina con el nombre redundante. Si es posible, vRealize Automation omite el nombre que ya se está usando y genera un nuevo nombre de máquina con el prefijo de máquina especificado. Si no se puede generar un nombre único, se produce un error en el aprovisionamiento.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tejido**.

Procedimiento

- 1 Haga clic en **Infraestructura > Administración > Prefijos de máquina**.
- 2 Haga clic en **Nuevo**.
- 3 Especifique el prefijo de máquina en el cuadro de texto **Nombre**.
- 4 Especifique si se muestra el prefijo de máquina en todos los tenants o solo en el tenant actual en la columna **Visibilidad**.
- 5 Escriba el número de dígitos de contador en el cuadro de texto **Número de dígitos**.
- 6 Escriba el número inicial del contador en el cuadro de texto **Siguiente número**.
- 7 Haga clic en el icono **Guardar** (✓).

Resultados

Los administradores de tenants pueden crear empresariales para que los usuarios puedan acceder a vRealize Automation para solicitar máquinas.

Crear un perfil de red

Un perfil de red contiene información IP como la puerta de enlace, subred y rango de direcciones. vRealize Automation usa vSphere DHCP o algún proveedor de IPAM especificado para asignar direcciones IP a las máquinas que aprovisiona.

Puede crear un perfil de red para definir un tipo de red disponible, incluidos los perfiles de red externa y las plantillas para la traducción de direcciones de red (network address translation, NAT) a petición, así como los perfiles de red enrutada que compilan conmutadores lógicos NSX y configuraciones de enrutamiento adecuadas para un nuevo nombre de red. Los perfiles de red son necesarios cuando se agregan componentes de red a un blueprint.

Los perfiles de red se usan para configurar los ajustes de red durante el aprovisionamiento de máquinas. Los perfiles de red también especifican la configuración de los dispositivos de NSX Edge que se crean cuando aprovisiona máquinas. Al crear reservas y blueprints, se identifica un perfil de red. En una reserva se puede asignar un perfil de red a una ruta de red y especificar una de esas rutas para un componente de máquina en un blueprint.

El creador de blueprints especifica un perfil de red adecuado cuando se definen componentes de red en el blueprint. Puede usar un perfil de red existente y un perfil de red enrutada o NAT a petición mientras define los adaptadores de red y equilibradores de carga para la máquina que se aprovisiona.

Los perfiles de red también admiten proveedores de administración de direcciones IP (IP Address Management, IPAM) de terceros, como Infoblox. Cuando configura un perfil de red para IPAM, las máquinas aprovisionadas pueden obtener de la solución IPAM configurada los datos de la dirección IP e información relacionada, como el DNS y la puerta de enlace. Puede usar un paquete de IPAM externo para un proveedor de terceros, como Infoblox, para definir un endpoint de IPAM que se use con un perfil de red.

Nota Si está utilizando un proveedor de IPAM de terceros y desea especificar en qué red tiene que implementar su máquina, utilice un perfil de red independiente para cada VLAN de manera que se evite el problema conocido que se describe en el [artículo 2148656 de la Base de conocimientos](#).

Si no utiliza un proveedor de IPAM de terceros, pero en cambio usa el endpoint de IPAM suministrado por vRealize Automation, puede especificar los rangos de direcciones IP que los perfiles de red podrán emplear. Cada dirección IP en los rangos especificados que está asignada a una máquina se reclama para poder volver a asignarla cuando la máquina se destruya. Se puede crear un perfil de red para definir un rango de direcciones IP estáticas que se pueda asignar a las máquinas. Al aprovisionar máquinas virtuales mediante clonación o usando el aprovisionamiento kickstart/autoYaST, el propietario de la máquina que realiza la solicitud puede asignar direcciones IP estáticas de un rango predeterminado.

Puede asignar un perfil de red a un nombre de red específico en una reserva. En algunos tipos de componentes de máquinas, como vSphere, puede asignar un perfil de red al momento de crear o editar blueprints.

Nota Aunque no se puede cambiar el perfil de red de una máquina virtual implementada, sí se puede cambiar la red a la que está conectada la máquina virtual. Si la red está asociada a un perfil de red distinta, vRealize Automation asigna una dirección IP de ese perfil de red a la máquina virtual. Sin embargo, la máquina virtual continúa utilizando la dirección IP anterior hasta que se actualice la dirección IP en el sistema operativo invitado. También se puede utilizar la acción de reconfiguración en la máquina virtual implementada, lo que también requiere que actualice la dirección IP en el sistema operativo invitado.

Si especifica un perfil de red en una reserva y un blueprint, el valor del blueprint tiene prioridad. Por ejemplo, si especifica un perfil de red en el blueprint (mediante la propiedad personalizada `VirtualMachine.NetworkN.ProfileName`) y en una reserva utilizada por el blueprint, el perfil de red especificado en el blueprint tendrá prioridad. Sin embargo, si la propiedad personalizada no se utiliza en el blueprint, y selecciona un perfil de red para un NIC de máquina, vRealize Automation usa la ruta de red de reserva para el NIC de máquina cuyo perfil de red se haya especificado.

Para obtener más información acerca de estos tipos de red, consulte *Guía de administración de NSX* en el centro de información de NSX en https://www.vmware.com/support/pubs/nsx_pubs.html.

Tabla 2-14. Tipos de red disponibles para un perfil de red de vRealize Automation

Tipo de red	Descripción
Externo	<p>Red existente que se ha configurado en el servidor de vSphere. Son la parte externa de los tipos de redes NAT y enrutadas. Un perfil de red externa puede definir un rango de direcciones IP estáticas disponibles en la red externa.</p> <p>Puede usar rangos de IP obtenidos del endpoint de IPAM de VMware suministrado o de un endpoint de proveedor de servicios de IPAM de terceros que se haya registrado y configurado en vRealize Orchestrator (por ejemplo, Infoblox IPAM). Durante la asignación, se crea un rango de IP desde un bloque de IP.</p> <p>Tener un perfil de red externa con un rango IP estático es un requisito previo en las redes NAT y enrutadas.</p> <p>Consulte Crear un perfil de red externa para una red existente.</p>
NAT	<p>Red a petición creada durante el aprovisionamiento. Son redes NAT que usan un conjunto de direcciones IP para la comunicación externa y otro para las comunicaciones internas.</p> <p>En las redes NAT uno a uno, cada máquina virtual tiene asignada una dirección IP externa del perfil de red externa y una dirección IP interna del perfil de red NAT. En las redes NAT uno a muchos, todas las máquinas comparten una única dirección IP del perfil de red externa para la comunicación externa.</p> <p>Puede usar rangos de IP obtenidos del endpoint de IPAM de VMware suministrado o de un endpoint de proveedor de servicios de IPAM de terceros que se haya registrado y configurado en vRealize Orchestrator (por ejemplo, Infoblox IPAM). Durante la asignación, se crea un rango de IP desde un bloque de IP.</p> <p>Un perfil de red NAT define las redes local y externa que usan una tabla de traducción para la comunicación mutua.</p> <p>Consulte Crear un perfil de red NAT para una red a petición.</p>
Enrutada	<p>Red a petición creada durante el aprovisionamiento. Las redes enrutadas contienen un espacio de IP enrutable distribuido entre subredes vinculadas entre sí con un enrutador lógico distribuido (Distributed Logical Router, DLR).</p> <p>A cada nueva red enrutada se le asigna la siguiente subred que haya disponible y se asocia a otras redes enrutadas que usan el mismo perfil de red. Las máquinas virtuales aprovisionadas con redes enrutadas que tienen el mismo perfil de red enrutada se pueden comunicar entre sí y con la red externa.</p> <p>Puede usar rangos de IP obtenidos del endpoint de IPAM de VMware suministrado o de un endpoint de proveedor de servicios de IPAM de terceros que se haya registrado y configurado en vRealize Orchestrator (por ejemplo, Infoblox IPAM). Durante la asignación, se crea un rango de IP desde un bloque de IP.</p> <p>Un perfil de red enrutada define un espacio enrutable y las subredes disponibles.</p> <p>Consulte Crear un perfil de red enrutada para una red a petición.</p>

Usar perfiles de red para controlar rangos de direcciones IP

Puede usar perfiles de red para asignar direcciones IP estáticas de un rango predefinido a máquinas virtuales aprovisionadas mediante clonación, con Linux kickstart/autoYaST, o a máquinas de nube aprovisionadas en OpenStack mediante kickstart.

De forma predeterminada, vRealize Automation usa el protocolo de configuración dinámica de host (DHCP) para asignar direcciones IP a máquinas aprovisionadas.

Puede crear perfiles de red para definir un rango de direcciones IP estáticas que puede asignar a las máquinas. Puede asignar perfiles de red a nombres de red específicos en una reserva. Las máquinas que se aprovisionan mediante clonación, kickstart o autoYaST se adjuntan a un nombre de red con un perfil de red asociado y se aprovisionan con una dirección IP estática asignada. Para el aprovisionamiento con una asignación de dirección IP estática, debe utilizar una especificación de personalización.

Puede asignar un perfil de red a un componente de máquina de vSphere en un blueprint añadiendo un componente de red existente enrutada a petición o red NAT a petición al lienzo de diseño y seleccionando un perfil de red al que conectar el componente de la máquina de vSphere. También puede asignar perfiles de red a blueprints mediante la propiedad personalizada `VirtualMachine.NetworkN.ProfileName`, donde *N* es el identificador de red.

Opcionalmente, puede utilizar el IPAM de vRealize Automation suministrado o un endpoint de proveedor de servicios de IPAM de terceros registrado y configurado en el perfil de red para obtener y configurar direcciones IP. Para obtener más información sobre los requisitos de un IPAM externo, consulte [Lista de comprobación para proporcionar soporte técnico del proveedor de IPAM de terceros](#).

Cuando se selecciona un endpoint proveedor de servicios de IPAM de terceros en un perfil de red, vRealize Automation recupera los rangos de IP del endpoint de IPAM externo registrado (por ejemplo, Infoblox). A continuación, asigna los valores de IP de dicho endpoint. La máscara de subred del rango especificada se utiliza para asignar subredes desde el bloque de IP.

Si especifica un perfil de red en una reserva y un blueprint, el valor del blueprint tiene prioridad. Por ejemplo, si especifica un perfil de red en el blueprint (mediante la propiedad personalizada `VirtualMachine.NetworkN.ProfileName`) y en una reserva utilizada por el blueprint, el perfil de red especificado en el blueprint tendrá prioridad. Sin embargo, si la propiedad personalizada no se utiliza en el blueprint, y selecciona un perfil de red para un NIC de máquina, vRealize Automation usa la ruta de red de reserva para el NIC de máquina cuyo perfil de red se haya especificado.

Comprender el formato de un archivo CSV para importar direcciones IP del perfil de red

Puede importar rangos de redes de direcciones IP a un perfil de red de vRealize Automation con un archivo CSV correctamente formateado.

Las entradas de un archivo CSV deben tener el siguiente formato.

Campo de CSV	Descripción
<code>ip_address</code>	Una dirección IP con el formato IPv4.
<code>machine_name</code>	Nombre de una máquina administrada en vRealize Automation. Si el campo está vacío, no hay ningún nombre de forma predeterminada. Si el campo está vacío, el valor del campo <code>status</code> no puede ser Asignado.
<code>status</code>	Puede ser Asignado o Sin asignar. Se distingue entre mayúsculas y minúsculas. Si el campo está vacío, el valor predeterminado es Sin asignar. Si el estado es Asignado, el campo <code>machine_name</code> no puede estar vacío.
<code>NIC_offset</code>	Un entero no negativo. Opcional.

La siguiente entrada de ejemplo no especifica un desfase de NIC.

```
100.10.100.1,mymachine01,Allocated
```

Importar direcciones IP en un perfil de red desde un archivo CSV

Para añadir direcciones IP a un rango de perfiles de red, importe un archivo CSV con el formato correcto. También puede cambiar las direcciones en el rango de perfiles de red. Para ello, debe editar el rango en vRealize Automation o bien importar otro archivo CSV distinto o uno modificado.

Para añadir o cambiar las direcciones IP de un rango de perfiles de red, impórtelas desde un archivo CSV o introduzca los valores manualmente. Si lo prefiere, puede permitir a un proveedor de IPAM de terceros suministrar direcciones IP.

- Importe un rango inicial de direcciones IP en un perfil de red de vRealize Automation.
- Aplique los valores importados para crear el primer rango de redes con nombre del perfil de red.
- Elimine una o varias direcciones IP del rango de redes de vRealize Automation.
- Importe otro archivo CSV distinto, o uno modificado, para examinar cómo cambiar los valores del rango de redes.

No puede utilizar la opción **Importar de CSV** para los perfiles de red que utilicen un endpoint de IPAM de terceros debido a que las direcciones IP las administra el proveedor de IPAM de terceros, no vRealize Automation.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Cree un archivo CSV que contenga las direcciones IP que desea importar en un rango de redes. Consulte [Crear un perfil de red externa mediante un proveedor de IPAM de terceros](#) y [Comprender el formato de un archivo CSV para importar direcciones IP del perfil de red](#).

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Perfiles de red**.
- 2 Haga clic en **Nuevo** y seleccione un tipo de perfil de red en el menú desplegable.
En este ejemplo, seleccione *Externo*.
- 3 Escriba **Mi perfil de red con CSV** en el cuadro de texto **Nombre**.
- 4 Escriba **Prueba de direcciones IP de rango de redes con CSV** en el cuadro de texto **Descripción**.

La opción para importar el archivo CSV se aplica a la configuración de las páginas de las pestañas **Rangos de redes** y **Direcciones IP**. De este modo, puede pasar rápidamente por las dos primeras pestañas para introducir la información básica del perfil de red.

- 5 También puede seleccionar un endpoint de IPAM configurado, si hay alguno disponible. Si no hay ninguno, puede omitir este paso.
- 6 Escriba el valor de dirección IP adecuado en los cuadros de texto **Máscara de subred** y **Puerta de enlace**.
- 7 Haga clic en la pestaña **DNS**.
- 8 Escriba la información relevante, como el sufijo DNS, y haga clic en la pestaña **Rangos de redes**.

La opción **Importar de CVS** está disponible al hacer clic en la pestaña **Rangos de redes**.

- 9 Haga clic en **Nuevo** para especificar manualmente un nuevo nombre de rango de redes y un rango de direcciones IP, o haga clic en **Importar de CSV** para importar la información de direcciones IP de un archivo CSV con el formato correcto.

- Haga clic en **Nuevo**.

- a Introduzca un nombre de rango de redes.
- b Introduzca una descripción del rango de redes.
- c Introduzca la dirección IP de inicio del rango.
- d Introduzca la dirección IP final del rango.

- Haga clic en **Importar de CSV**.

- a Busque el archivo CSV y selecciónelo, o arrastre el archivo CSV al cuadro de diálogo **Importar de CSV**.

Las filas del archivo CSV tienen el formato *dirección_ip, nombre_máquina, estado, desplazamiento de NIC*. Por ejemplo:

```
100.10.100.1,mymachine01,Allocated
```

Campo de CSV	Descripción
ip_address	Una dirección IP con el formato IPv4.
machine_name	Nombre de una máquina administrada en vRealize Automation. Si el campo está vacío, no hay ningún nombre de forma predeterminada. Si el campo está vacío, el valor del campo status no puede ser Asignado.
status	Puede ser Asignado o Sin asignar. Se distingue entre mayúsculas y minúsculas. Si el campo está vacío, el valor predeterminado es Sin asignar. Si el estado es Asignado, el campo machine_name no puede estar vacío.
NIC_offset	Un entero no negativo. Opcional.

- b Haga clic en **Aplicar**.

- 10 Haga clic en **Aceptar**.

El nombre del rango de IP aparece en la lista Rangos definidos. Las direcciones IP del rango aparecen en la lista Direcciones IP definidas.

Las direcciones IP cargadas aparecen en la página **Direcciones IP** cuando se hace clic en **Aplicar**, o bien después de guardar y editar el perfil de red.

- 11 Haga clic en la pestaña **Direcciones IP** para mostrar los datos de dirección IP del espacio de direcciones del rango especificado.

Si se importa la información de direcciones IP de un archivo CSV, el nombre de rango se genera como *Importado de CSV*.

- 12 (opcional) Seleccione la información de dirección IP del menú desplegable **Rango de redes** para filtrar las entradas de direcciones IP.

Puede mostrar información sobre todos los rangos de redes definidos, los rangos de redes importados de un archivo CSV o un rango de redes con nombre. Se incluyen detalles como la dirección IP inicial, el nombre de la máquina, la marca de hora y la fecha de la última modificación, y el estado de IP.

Pasos siguientes

Si vuelve a importar direcciones IP de un archivo CSV, las direcciones IP anteriores quedan reemplazadas por la información del archivo CSV importado.

Crear un perfil de red externa para una red existente

Puede crear perfiles de red externa para especificar ajustes de red y configurar redes existentes para el aprovisionamiento de máquinas, incluyendo la configuración de los dispositivos NSX Edge que se usarán durante el aprovisionamiento.

Puede usar el endpoint de proveedor de IPAM de vRealize Automation suministrado o un endpoint de proveedor de IPAM de terceros, como Infoblox, que haya registrado en vRealize Orchestrator.

Crear un perfil de red externa mediante el endpoint de IPAM suministrado

Puede crear un perfil de red externa para definir las propiedades de red y un rango de direcciones IP estáticas que pueden usarse al aprovisionar máquinas en una red existente.

Se pueden definir uno o varios rangos de redes de direcciones IP estáticas en el perfil de red para usarlos al aprovisionar una máquina. Si no se especifica ningún rango, puede usar un perfil de red como política de reserva de red a fin de seleccionar un nombre de red de reserva para la tarjeta de red virtual (vNIC) de una máquina.

Para obtener información sobre cómo crear un perfil de red externa y usar un endpoint de un proveedor de IPAM externo, consulte [Crear un perfil de red externa mediante un proveedor de IPAM de terceros](#).

Procedimiento

- 1 [Indicar la información del perfil de red externa mediante el endpoint de IPAM suministrado](#)

Un perfil de red externa identifica las propiedades y configuración de la red para una red existente. Un perfil de red externa es un requisito de los perfiles de red NAT y con enrutamiento.

2 Configurar rangos de IP del perfil de red externa mediante el endpoint de IPAM suministrado

Se pueden definir uno o varios rangos de redes de direcciones IP estáticas en el perfil de red para usarlos al aprovisionar una máquina. Si no se especifica ningún rango, puede usar un perfil de red como política de reserva de red a fin de seleccionar un nombre de red de reserva para la tarjeta de red virtual (vNIC) de una máquina.

Pasos siguientes

Se puede asignar un perfil de red a un nombre de red en una reserva o un arquitecto de blueprint puede especificar el perfil de red en un blueprint. Puede usar el perfil de red externa cuando cree un perfil de red enrutada o NAT a petición.

Indicar la información del perfil de red externa mediante el endpoint de IPAM suministrado. Un perfil de red externa identifica las propiedades y configuración de la red para una red existente. Un perfil de red externa es un requisito de los perfiles de red NAT y con enrutamiento.

Para obtener información sobre cómo crear un perfil de red externa a partir de la información de direcciones de IPAM que se obtenga de un endpoint de IPAM registrado de terceros, como Infoblox, consulte [Lista de comprobación para proporcionar soporte técnico del proveedor de IPAM de terceros](#) y [Crear un perfil de red externa mediante un proveedor de IPAM de terceros](#). Use el procedimiento siguiente para crear un perfil de red mediante el endpoint de IPAM interno de VMware.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Perfiles de red**.
- 2 Haga clic en **Nuevo** y seleccione **Existente** o **Externo** del menú desplegable.
- 3 Especifique un nombre y, opcionalmente, una descripción.
- 4 Acepte el valor de **Endpoint de IPAM** predeterminado para el endpoint de **IPAM de vRealize Automation** suministrado.
- 5 Introduzca una máscara de subred IP en el cuadro de texto **Máscara de subred**.
La máscara de subred especifica el tamaño de todo el espacio de direcciones enrutables que desea definir para su perfil de red.
Por ejemplo, escriba 255.255.0.0.
- 6 Introduzca una dirección de puerta de enlace enrutada o de Edge en el cuadro de texto **Puerta de enlace**.
Utilice un formato de dirección IPv4 estándar. Por ejemplo, escriba 10.10.110.1.

La dirección IP de puerta de enlace definida en el perfil de red se asigna a la NIC durante la asignación. Si no se asigna ningún valor en el cuadro de texto **Puerta de enlace** en el perfil de red, debe usar la propiedad personalizada `VirtualMachine.Network0.Gateway` al aprovisionar el equipo de Edge.

7 Haga clic en la pestaña **DNS**.

8 Si es necesario, especifique los valores de DNS y WINS.

Los valores de DNS se utilizan para el registro y la resolución de los nombres DNS. Los campos de DNS y WINS son opcionales cuando se utiliza un endpoint de IPAM interno. Si se utiliza un endpoint de IPAM externo, el proveedor de IPAM de terceros proporciona los valores de DNS y WINS.

- a (opcional) Introduzca un valor para el servidor **DNS primario**.
- b (opcional) Introduzca un valor para el servidor **DNS secundario**.
- c (opcional) Introduzca un valor en **Sufijos DNS**.
- d (opcional) Introduzca un valor en **Sufijos de búsqueda de DNS**.
- e (opcional) Introduzca un valor para el servidor **WINS preferido**.
- f (opcional) Introduzca un valor para el servidor **WINS alternativo**.

Pasos siguientes

Puede configurar rangos IP para direcciones IP estáticas. Consulte [Configurar rangos de IP del perfil de red externa mediante el endpoint de IPAM suministrado](#).

Configurar rangos de IP del perfil de red externa mediante el endpoint de IPAM suministrado
Se pueden definir uno o varios rangos de redes de direcciones IP estáticas en el perfil de red para usarlos al aprovisionar una máquina. Si no se especifica ningún rango, puede usar un perfil de red como política de reserva de red a fin de seleccionar un nombre de red de reserva para la tarjeta de red virtual (vNIC) de una máquina.

Puede definir valores de rangos IP manualmente desde un archivo CSV importado o mediante las direcciones IP que proporcione un proveedor de IPAM externo. Se pueden combinar rangos de IP definidos manualmente y direcciones IP importadas a través de CSV. Por ejemplo, es posible definir algunos rangos mediante la interfaz de usuario y otros mediante la importación desde un archivo CSV.

Si se realiza una importación de un archivo CSV por segunda vez, independientemente del nombre de archivo CSV, se borran los rangos de IP importados del archivo CSV anterior y se añade la información de los nuevos rangos de IP. Por lo tanto, la importación anterior se sobrescribe cuando se importa por segunda o más veces. El proceso por el cual se actualiza un archivo CSV y se vuelve a importar ese archivo CSV al perfil de red se puede repetir de manera indefinida.

Si un perfil de red externa no tiene definidos rangos de IP, puede usarlo para especificar la red que se elige en una tarjeta de red virtual (vNIC). Si está usando el perfil de red existente en un perfil de red NAT o enrutada, debe tener al menos un rango IP estático.

Requisitos previos

Indicar la información del perfil de red externa mediante el endpoint de IPAM suministrado.

Procedimiento

- 1 Haga clic en la pestaña **Rangos de redes**.
- 2 Haga clic en **Nuevo** para especificar manualmente un nuevo nombre de rango de redes y un rango de direcciones IP, o haga clic en **Importar de CSV** para importar la información de direcciones IP de un archivo CSV con el formato correcto.

- Haga clic en **Nuevo**.

- a Introduzca un nombre de rango de redes.
- b Introduzca una descripción del rango de redes.
- c Introduzca la dirección IP de inicio del rango.
- d Introduzca la dirección IP final del rango.

- Haga clic en **Importar de CSV**.

- a Busque el archivo CSV y selecciónelo, o arrastre el archivo CSV al cuadro de diálogo **Importar de CSV**.

Las filas del archivo CSV tienen el formato *dirección_ip, nombre_máquina, estado, desplazamiento de NIC*. Por ejemplo:

```
100.10.100.1,mymachine01,Allocated
```

Campo de CSV	Descripción
ip_address	Una dirección IP con el formato IPv4.
machine_name	Nombre de una máquina administrada en vRealize Automation. Si el campo está vacío, no hay ningún nombre de forma predeterminada. Si el campo está vacío, el valor del campo status no puede ser Asignado.
status	Puede ser Asignado o Sin asignar. Se distingue entre mayúsculas y minúsculas. Si el campo está vacío, el valor predeterminado es Sin asignar. Si el estado es Asignado, el campo machine_name no puede estar vacío.
NIC_offset	Un entero no negativo. Opcional.

- b Haga clic en **Aplicar**.

- 3 Haga clic en **Aceptar**.

El nombre del rango de IP aparece en la lista Rangos definidos. Las direcciones IP del rango aparecen en la lista Direcciones IP definidas.

Las direcciones IP cargadas aparecen en la página **Direcciones IP** cuando se hace clic en **Aplicar**, o bien después de guardar y editar el perfil de red.

- 4 Haga clic en la pestaña **Direcciones IP** para mostrar los datos de dirección IP del espacio de direcciones del rango especificado.

Si se importa la información de direcciones IP de un archivo CSV, el nombre de rango se genera como *Importado de CSV*.

- 5 (opcional) Seleccione la información de dirección IP del menú desplegable **Rango de redes** para filtrar las entradas de direcciones IP.

Puede mostrar información sobre todos los rangos de redes definidos, los rangos de redes importados de un archivo CSV o un rango de redes con nombre. Se incluyen detalles como la dirección IP inicial, el nombre de la máquina, la marca de hora y la fecha de la última modificación, y el estado de IP.

- 6 (opcional) Seleccione un tipo de estado en el menú desplegable **Estado de IP** para filtrar las entradas de direcciones IP únicamente a aquellas que coincidan con el estado de IP seleccionado. Las opciones de estado son Asignado, Sin asignar, Destruído y Caducado.

En las direcciones IP con el estado Caducado o Destruído, puede hacer clic en **Recuperar** para permitir la asignación de esos rangos de direcciones IP. Es necesario guardar el perfil para que la recuperación sea efectiva. Las direcciones no se recuperan inmediatamente, de modo que la columna de estado no cambia al instante de Caducado o Destruído a Asignado.

- 7 Haga clic en **Aceptar** para completar el perfil de red.

Resultados

Se puede asignar un perfil de red a un nombre de red en una reserva o un arquitecto de blueprint puede especificar el perfil de red en un blueprint. Si creó un perfil de red externa, podrá usarlo para crear un perfil de red enrutada o NAT.

Crear un perfil de red externa mediante un proveedor de IPAM de terceros

Puede utilizar una solución de un proveedor de IPAM de terceros que haya importado, configurado y registrado en vRealize Orchestrator para obtener las direcciones IP de dicho proveedor de terceros.

Puede crear un perfil de red externa que use un endpoint de un proveedor de soluciones IPAM de terceros registrado para obtener la configuración de puerta de enlace, máscara de subred y DHCP/WINS.

Se pueden definir uno o varios rangos de redes de direcciones IP estáticas en el perfil de red para usarlos al aprovisionar una máquina. Si no se especifica ningún rango, puede usar un perfil de red como política de reserva de red a fin de seleccionar un nombre de red de reserva para la tarjeta de red virtual (vNIC) de una máquina.

Para obtener información sobre cómo crear un perfil de red externa sin usar un proveedor de IPAM, o usando el endpoint del proveedor de IPAM interno que se proporciona, consulte [Crear un perfil de red externa mediante el endpoint de IPAM suministrado](#).

Procedimiento

1 Indicar la información del perfil de red externa mediante un endpoint de IPAM de terceros

Un perfil de red externa identifica las propiedades y configuración de la red para una red existente. Un perfil de red externa es un requisito de los perfiles de red NAT y con enrutamiento. Si registró y configuró un endpoint de IPAM en vRealize Orchestrator, puede especificar que un proveedor de IPAM debe proporcionar la información de esa dirección IP.

2 Configurar los rangos de IP del perfil de red externa mediante un endpoint de IPAM de terceros

Se pueden definir uno o varios rangos de redes de direcciones IP estáticas en el perfil de red para usarlos al aprovisionar una máquina. Si no se especifica ningún rango, puede usar un perfil de red como política de reserva de red a fin de seleccionar un nombre de red de reserva para la tarjeta de red virtual (vNIC) de una máquina.

Pasos siguientes

Se puede asignar un perfil de red a un nombre de red en una reserva o un arquitecto de blueprint puede especificar el perfil de red en un blueprint. Puede usar el perfil de red externa cuando cree un perfil de red enrutada o NAT a petición.

Indicar la información del perfil de red externa mediante un endpoint de IPAM de terceros
Un perfil de red externa identifica las propiedades y configuración de la red para una red existente. Un perfil de red externa es un requisito de los perfiles de red NAT y con enrutamiento. Si registró y configuró un endpoint de IPAM en vRealize Orchestrator, puede especificar que un proveedor de IPAM debe proporcionar la información de esa dirección IP.

Requisitos previos

- Verifique que haya importado y configurado un complemento de proveedor de IPAM externo en vRealize Orchestrator y que haya registrado el tipo de endpoint del proveedor de IPAM en vRealize Orchestrator. En este ejemplo, el proveedor de la solución IPAM externo admitido es Infoblox. Consulte [Lista de comprobación para proporcionar soporte técnico del proveedor de IPAM de terceros](#).
- [Crear un endpoint de proveedor de IPAM de terceros](#).
- Configure vRealize Orchestrator Appliance con el flujo de trabajo del endpoint de IPAM registrado como Orchestrator independiente en el tenant global (administrador en vsphere.local).
- Inicie sesión en vRealize Automation como **administrador de tejido**.

Procedimiento

1 Seleccione **Infraestructura > Reservas > Perfiles de red**.

- 2 Haga clic en **Nuevo** y seleccione **Existente** o **Externo** del menú desplegable.
- 3 Especifique un nombre y, opcionalmente, una descripción.
- 4 Si ha configurado uno o más endpoints de proveedores de IPAM de terceros, seleccione un endpoint de IPAM de terceros del menú desplegable **Endpoint de IPAM**.

Al seleccionar un endpoint de proveedor de IPAM de terceros que se ha registrado en vRealize Orchestrator, las direcciones IP se obtienen del proveedor de servicio de IPAM especificado. Las especificaciones de IP como las opciones de máscara de subred y DNS/WINS no están disponibles porque sus funciones las controla el endpoint de IPAM de terceros seleccionado.

Pasos siguientes

Ahora puede definir rangos de red para las direcciones IP y completar la definición del perfil de red.

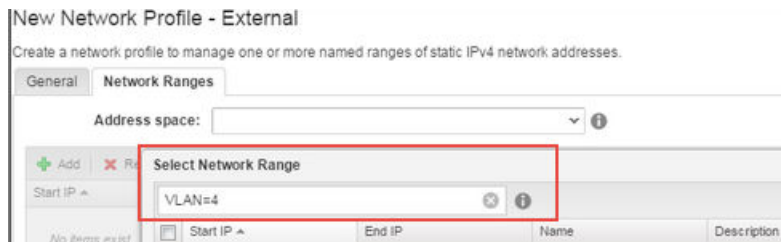
Configurar los rangos de IP del perfil de red externa mediante un endpoint de IPAM de terceros. Se pueden definir uno o varios rangos de redes de direcciones IP estáticas en el perfil de red para usarlos al aprovisionar una máquina. Si no se especifica ningún rango, puede usar un perfil de red como política de reserva de red a fin de seleccionar un nombre de red de reserva para la tarjeta de red virtual (vNIC) de una máquina.

Puede definir rangos de IP mediante las direcciones IP proporcionadas por un proveedor de IPAM de terceros.

vRealize Automation solo guarda en la base de datos los identificadores del rango de IPAM externo, pero no la información del rango. Si edita un perfil de red en esta página o en un blueprint, vRealize Automation llama al servicio de IPAM para obtener la información del rango en función de los identificadores del rango seleccionado.

Nota Un problema conocido con algunos proveedores externos de IPAM causa que se agote el tiempo de espera de una consulta al devolver rangos de redes, lo que da como resultado una lista vacía. Como solución alternativa, puede proporcionar los criterios de búsqueda para evitar que se agote el tiempo de espera y obtener la información del rango de redes.

Por ejemplo, dependiendo del proveedor de IPAM, es posible que pueda añadir una propiedad llamada VLAN a cada red de la aplicación del proveedor de IPAM y asignar un valor a dicha propiedad, como 4. A continuación, puede filtrar en función de la propiedad y el valor (por ejemplo, VLAN=4) en el cuadro de texto **Seleccionar rango de red** en la página del perfil de red de vRealize Automation.



Opcionalmente, puede aumentar el valor de tiempo de espera mediante el siguiente procedimiento:

- 1 En cada uno de los nodos del dispositivo de vRealize Automation, abra el archivo `/etc/vcac/webapps/o11n-gateway-service/WEB-INF/classes/META-INF/spring/root/o11n-gateway-service-context.xml`.
- 2 Cambie el valor de tiempo de espera de 30 segundos a un número superior.
- 3 Reinicie el servidor vCAC introduciendo `service vcac-server restart`.

Requisitos previos

[Indicar la información del perfil de red externa mediante un endpoint de IPAM de terceros.](#)

Procedimiento

- 1 Haga clic en la pestaña **Rangos de redes** para crear un nuevo rango de redes o para seleccionar un rango de redes existente.

Aparecen los detalles del rango seleccionado, como el nombre, la descripción y la dirección IP inicial y final. También se ofrece información relativa al estado.

- 2 Seleccione en el menú desplegable **Espacio de direcciones** un espacio de direcciones de la lista de todos los espacios de direcciones disponibles para el endpoint.

- 3 Haga clic en **Añadir** y seleccione uno o varios rangos de redes disponibles para el espacio de direcciones especificado.

La selección de un rango de redes puede resultar en una lista vacía al utilizar un proveedor de IPAM de terceros. Para obtener detalles, consulte el artículo 2148656 de la base de conocimientos en <http://kb.vmware.com/kb/2148656>.

- 4 Haga clic en **Aceptar**.

El nombre del rango de IP aparece en la lista Rangos definidos. Las direcciones IP del rango aparecen en la lista Direcciones IP definidas.

Las direcciones IP cargadas aparecen en la página **Direcciones IP** cuando se hace clic en **Aplicar**, o bien después de guardar y editar el perfil de red.

- 5 Haga clic en **Aceptar** para completar el perfil de red.

Pasos siguientes

Se puede asignar un perfil de red a un nombre de red en una reserva o un arquitecto de blueprint puede especificar el perfil de red en un blueprint.

Crear un perfil de red enrutada para una red a petición

Puede crear un perfil de red enrutada a petición que use el endpoint de IPAM de vRealize Automation proporcionado o un endpoint de IPAM de terceros registrado y configurado correctamente.

Un perfil de red enrutada representa espacio IP enrutable que se divide en varias redes. Cada nueva red enrutada asigna la siguiente subred disponible en el espacio IP enrutable. Una red enrutada puede acceder a todas las redes enrutadas que usan el mismo perfil de red. Cada subred enrutada puede acceder a todas las demás subredes que el mismo perfil de red ha creado.

Los proveedores de IPAM de terceros crean y administran el espacio IP enrutable. El administrador de red utiliza un proveedor de IPAM de terceros para definir un espacio IP enrutable y crear un bloque de direcciones IP para él. Puede seleccionar uno o varios bloques de direcciones IP recuperados del proveedor de IPAM de terceros al crear o editar un perfil de red enrutada.

Cuando se asigna una nueva instancia de un perfil de red enrutada desde el proveedor de IPAM de terceros, vRealize Automation efectúa una llamada al proveedor para reservar la próxima subred disponible y crea un rango mediante bloques de IP determinados por el perfil de red enrutada y el tamaño de subred. El rango resultante se utiliza para asignar direcciones IP de las máquinas que están asignadas a la red enrutada de la misma implementación.

Crear un perfil de red enrutada mediante el endpoint de IPAM suministrado

Cuando se utiliza un perfil de red enrutada con el endpoint de IPAM suministrado, puede definir un espacio de IP enrutable y las subredes disponibles para una red enrutada a petición.

Utilizando el endpoint de IPAM suministrado de vRealize Automation, puede asignar rangos de direcciones IP estáticas y una dirección IP base al perfil de red enrutada.

Puede usar rangos de IP obtenidos del endpoint de IPAM de VMware suministrado o de un endpoint de proveedor de servicios de IPAM de terceros que se haya registrado y configurado en vRealize Orchestrator (por ejemplo, Infoblox IPAM). Durante la asignación, se crea un rango de IP desde un bloque de IP.

Procedimiento

1 [Indicar información de perfil de red enrutada con el endpoint de IPAM de vRealize Automation](#)

La información de perfil de red permite identificar las propiedades de red enrutada, su perfil de red externa subyacente y otros valores que se utilizan al aprovisionar la red cuando se usa el endpoint de IPAM suministrado.

2 [Configurar rangos de IP de perfil de red enrutada con el endpoint de IPAM de vRealize Automation](#)

Se pueden definir unos o varios rangos de direcciones IP estáticas para usarlos al aprovisionar una red.

Indicar información de perfil de red enrutada con el endpoint de IPAM de vRealize Automation
La información de perfil de red permite identificar las propiedades de red enrutada, su perfil de red externa subyacente y otros valores que se utilizan al aprovisionar la red cuando se usa el endpoint de IPAM suministrado.

Si desea crear un perfil de red enrutada mediante un endpoint de IPAM de terceros, consulte [Indicar información de perfil de red enrutada con un endpoint de IPAM de terceros](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Cree un perfil de red externa. Consulte [Crear un perfil de red externa mediante el endpoint de IPAM suministrado](#).

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Perfiles de red**.
- 2 Haga clic en **Nuevo** y seleccione **Con enrutamiento** en el menú desplegable.
- 3 Especifique un nombre y, opcionalmente, una descripción.
- 4 Acepte el valor de **Endpoint de IPAM** predeterminado para el endpoint de **IPAM de vRealize Automation** suministrado.
- 5 Seleccione un perfil de red externa existente en el menú desplegable **Perfil de red externa**.
- 6 Introduzca la máscara de subred en el cuadro de texto **Máscara de subred** asociado al perfil de red externa.

La máscara de subred especifica el tamaño de todo el espacio de direcciones enrutables que desea definir para su perfil de red.

Por ejemplo, escriba 255.255.0.0.

- 7 Seleccione un valor en el menú desplegable del cuadro de texto **Máscara de subred del rango** para determinar el modo en que se generan los rangos mediante la opción **Generar rangos** de la página **Rangos de IP**.

Por ejemplo, escriba 255.255.255.0.

La máscara de subred del rango define la manera en la que desea dividir el espacio en bloques de direcciones individuales que se asignan a cada instancia de implementación de ese perfil de red. Al seleccionar un valor para la máscara de subred del rango, tenga en cuenta la cantidad de implementaciones que espera utilizar en la red enrutada.

Se utiliza un rango para cada implementación que utiliza un perfil de red enrutada. La cantidad de rangos enrutados disponibles es igual al valor de la máscara de subred dividido por el de la máscara de subred del rango, por ejemplo $255.255.0.0/255.255.255.0 = 256$.

- 8 Introduzca la primera dirección IP disponible en el cuadro de texto **IP base**.

Esta opción no está disponible si selecciona un endpoint de terceros.

Por ejemplo, escriba 120.120.0.1.

- 9 Haga clic en la pestaña **DNS**.

- 10 Si es necesario, especifique los valores de DNS y WINS.

Los valores de DNS se utilizan para el registro y la resolución de los nombres DNS. Los campos de DNS y WINS son opcionales cuando se utiliza un endpoint de IPAM interno. Si se utiliza un endpoint de IPAM externo, el proveedor de IPAM de terceros proporciona los valores de DNS y WINS.

- a (opcional) Introduzca un valor para el servidor **DNS primario**.
- b (opcional) Introduzca un valor para el servidor **DNS secundario**.
- c (opcional) Introduzca un valor en **Sufijos DNS**.
- d (opcional) Introduzca un valor en **Sufijos de búsqueda de DNS**.
- e (opcional) Introduzca un valor para el servidor **WINS preferido**.
- f (opcional) Introduzca un valor para el servidor **WINS alternativo**.

Pasos siguientes

[Configurar rangos de IP de perfil de red enrutada con el endpoint de IPAM de vRealize Automation.](#)

Configurar rangos de IP de perfil de red enrutada con el endpoint de IPAM de vRealize Automation

Se pueden definir unos o varios rangos de direcciones IP estáticas para usarlos al aprovisionar una red.

Durante el aprovisionamiento, cada red enrutada nueva asigna el siguiente rango disponible y lo usa como su espacio de IP.

Requisitos previos

Indicar información de perfil de red enrutada con el endpoint de IPAM de vRealize Automation.

Procedimiento

- 1 Haga clic en la pestaña **Rangos de redes** para crear un nuevo rango de redes o para seleccionar un rango de redes existente.

Aparecen los detalles del rango seleccionado, como el nombre, la descripción y la dirección IP inicial y final. También se ofrece información relativa al estado.

- 2 Haga clic en **Generar rangos** para generar rangos de red conforme a la máscara de subred, máscara de subred del rango e información sobre la dirección IP base que ingresó en la pestaña General.

vRealize Automation genera rangos (empezando por la dirección IP base) basados en la máscara de subred del rango.

Por ejemplo, vRealize Automation genera intervalos de 255 rangos IP si la máscara de subred es 255.255.0.0 y la máscara de subred del rango es 255.255.255.0, del nombre Range1 al Rangen.

- 3 Haga clic en **Aceptar**.

Crear un perfil de red enrutada mediante un endpoint de IPAM de terceros

Cuando se utiliza un perfil de red enrutada con un endpoint de IPAM de terceros, el proveedor de IPAM de terceros crea y administra un espacio de IP enrutable.

Cuando se utiliza un endpoint de IPAM de terceros en el perfil de red enrutada, el proveedor crea nuevos rangos de IP para cada instancia de la red a petición.

Puede usar rangos de IP obtenidos del endpoint de IPAM de VMware suministrado o de un endpoint de proveedor de servicios de IPAM de terceros que se haya registrado y configurado en vRealize Orchestrator (por ejemplo, Infoblox IPAM). Durante la asignación, se crea un rango de IP desde un bloque de IP.

Procedimiento

- 1 [Indicar información de perfil de red enrutada con un endpoint de IPAM de terceros](#)

La información de perfil de red permite identificar las propiedades de red enrutada, su perfil de red externa subyacente y otros valores que se utilizan al aprovisionar la red cuando se usa un endpoint de IPAM de terceros.

- 2 [Configurar rangos de IP de perfil de red enrutada con un endpoint de IPAM de terceros](#)

Puede administrar uno o varios rangos con nombre de direcciones de red IPv4 estáticas para usarlos en el aprovisionamiento de una red.

Indicar información de perfil de red enrutada con un endpoint de IPAM de terceros

La información de perfil de red permite identificar las propiedades de red enrutada, su perfil de red externa subyacente y otros valores que se utilizan al aprovisionar la red cuando se usa un endpoint de IPAM de terceros.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Cree un perfil de red externa. Consulte [Crear un perfil de red externa mediante el endpoint de IPAM suministrado](#) o [Crear un perfil de red externa mediante un proveedor de IPAM de terceros](#).
- Cree y configure un endpoint de IPAM de terceros. Consulte [Crear un endpoint de proveedor de IPAM de terceros](#).

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Perfiles de red**.
- 2 Haga clic en **Nuevo** y seleccione **Con enrutamiento** en el menú desplegable.
- 3 Especifique un nombre y, opcionalmente, una descripción.
- 4 Si ha configurado uno o más endpoints de proveedores de IPAM de terceros, seleccione un endpoint de IPAM de terceros del menú desplegable **Endpoint de IPAM**.

Al seleccionar un endpoint de proveedor de IPAM de terceros que se ha registrado en vRealize Orchestrator, las direcciones IP se obtienen del proveedor de servicio de IPAM especificado. Las especificaciones de IP como las opciones de máscara de subred y DNS/WINS no están disponibles porque sus funciones las controla el endpoint de IPAM de terceros seleccionado.

- 5 Seleccione un perfil de red externa existente en el menú desplegable **Perfil de red externa**.
Solo los perfiles de redes externas que están configurados para usar el endpoint de IPAM especificado se enumeran y se pueden seleccionar.
- 6 Seleccione un valor en el menú desplegable del cuadro de texto **Máscara de subred del rango** para determinar la cantidad de subredes de red que se crean para el aprovisionamiento.

Por ejemplo, escriba 255.255.255.0.

La máscara de subred del rango define la manera en la que desea dividir el espacio en bloques de direcciones individuales que se asignan a cada instancia de implementación de ese perfil de red. Al seleccionar un valor para la máscara de subred del rango, tenga en cuenta la cantidad de implementaciones que espera utilizar en la red enrutada.

Se utiliza un rango para cada implementación que utiliza un perfil de red enrutada. La cantidad de rangos enrutados disponibles es igual al valor de la máscara de subred dividido por el de la máscara de subred del rango, por ejemplo $255.255.0.0/255.255.255.0 = 256$.

- 7 Haga clic en la pestaña **Bloques IP** para definir un espacio de direcciones y administrar uno o más rangos nombrados de direcciones de red IPv4 estáticas.

Los bloques de IP disponibles son el origen de los rangos de IP que se crean o asignan para el enrutamiento a petición.

Pasos siguientes

Configurar rangos de IP de perfil de red enrutada con un endpoint de IPAM de terceros.

Configurar rangos de IP de perfil de red enrutada con un endpoint de IPAM de terceros. Puede administrar uno o varios rangos con nombre de direcciones de red IPv4 estáticas para usarlos en el aprovisionamiento de una red.

Durante el aprovisionamiento, cada nueva red enrutada asigna el siguiente rango disponible y lo utiliza como su espacio de IP. Los bloques de IP se obtienen del proveedor de IPAM de terceros. Durante el aprovisionamiento, se asigna una red enrutada desde el bloque con una máscara de subred que coincide con la máscara de subred del rango que se ha proporcionado.

Requisitos previos

Indicar información de perfil de red enrutada con un endpoint de IPAM de terceros.

Procedimiento

- 1 Seleccione un espacio de direcciones del menú desplegable **Espacio de direcciones** para limitar los bloques de IP disponibles para el aprovisionamiento.

Una vez que añada uno o más bloques de IP en la sección que se encuentra debajo del cuadro de texto Espacio de direcciones, ya no puede seleccionar un valor de **Espacio de direcciones**. Un perfil de red enrutada no puede abarcar más de un espacio de direcciones.

- 2 Añada uno o más bloques de IP o rangos de proveedores de IPAM mediante la sintaxis de búsqueda específica del proveedor o a través del menú desplegable Buscar.

Los bloques de IP se obtienen del proveedor de IPAM de terceros.

La selección de un rango de redes puede resultar en una lista vacía al utilizar un proveedor de IPAM de terceros. Para obtener detalles, consulte el artículo 2148656 de la base de conocimientos en <http://kb.vmware.com/kb/2148656>.

- a Haga clic en **Agregar**.
- b Haga clic en **Buscar**.
- c Escriba la sintaxis de búsqueda o seleccione uno o más bloques de IP del menú desplegable.
- d Haga clic en **Aceptar**.

- 3 Haga clic en **Aplicar**.

- 4 Haga clic en **Aceptar**.

Crear un perfil de red NAT para una red a petición

Puede crear un perfil de red NAT a petición que use el endpoint de IPAM de vRealize Automation proporcionado o un endpoint de IPAM de terceros registrado y configurado correctamente.

Crear un perfil de red NAT mediante el endpoint de IPAM suministrado

Puede crear un perfil de red NAT de NSX a petición relativo a un perfil de red externa. Cuando se usa el endpoint de IPAM de vRealize Automation proporcionado, se pueden asignar rangos de direcciones DHCP e IP estáticas al perfil de red NAT.

Las redes NAT usan un conjunto de direcciones IP para la comunicación externa y otro para la comunicación interna. Las direcciones IP externas se asignan a partir de un perfil de red externa, mientras que las direcciones IP NAT internas se definen mediante un perfil de red NAT. Cuando aprovisiona una nueva red NAT, se crea una nueva instancia del perfil de red NAT, el cual se utiliza para asignar direcciones IP de máquina.

Puede usar rangos de IP obtenidos del endpoint de IPAM de VMware suministrado o de un endpoint de proveedor de servicios de IPAM de terceros que se haya registrado y configurado en vRealize Orchestrator (por ejemplo, Infoblox IPAM). Durante la asignación, se crea un rango de IP desde un bloque de IP.

En una red NAT uno a muchos, puede definir las reglas NAT que se pueden configurar cuando se añade un componente de red NAT al blueprint y se pueden cambiar cuando se edita la red NAT en una implementación.

Procedimiento

1 Indicar información de perfil de red NAT con el endpoint de IPAM de vRealize Automation

El perfil de red distingue las propiedades de red NAT, el perfil de red externa subyacente, el tipo de NAT y otros valores que se utilizan para aprovisionar la red mediante el IPAM vRealize Automation integrado.

2 Configurar rangos de IP de perfil de red NAT con el endpoint de IPAM de vRealize Automation

Se pueden definir unos o varios rangos de direcciones IP estáticas para usarlos al aprovisionar una red.

Indicar información de perfil de red NAT con el endpoint de IPAM de vRealize Automation

El perfil de red distingue las propiedades de red NAT, el perfil de red externa subyacente, el tipo de NAT y otros valores que se utilizan para aprovisionar la red mediante el IPAM vRealize Automation integrado.

Si desea crear un perfil de red NAT que utilice un endpoint de IPAM de terceros, consulte [Especificación de la información de perfil de red NAT con un endpoint de IPAM de terceros](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Cree un perfil de red externa. Consulte [Crear un perfil de red externa mediante el endpoint de IPAM suministrado](#).

Procedimiento

1 Seleccione **Infraestructura > Reservas > Perfiles de red**.

- 2 Haga clic en **Nuevo** y seleccione **NAT** en el menú desplegable.
- 3 Especifique un nombre y, opcionalmente, una descripción.
- 4 Acepte el valor de **Endpoint de IPAM** predeterminado para el endpoint de **IPAM de vRealize Automation** suministrado.
- 5 Seleccione un perfil de red externa existente en el menú desplegable **Perfil de red externa**.
- 6 Seleccione el tipo de conversión de dirección de red uno a uno o uno a varios en el menú desplegable **Tipo de NAT**.

Opción	Descripción
Uno a uno	<p>Asigne una dirección IP estática externa a cada adaptador de red. Todas las máquinas pueden acceder a la red externa y serán accesibles desde la red externa.</p> <p>Todas las direcciones IP externas que estén asignadas a un vínculo superior de NSX Edge deben formar parte de la misma subred. Cuando se utiliza NAT 1:1 en vRealize Automation, el perfil de red externa correspondiente debe contener solo los rangos de IP que existen dentro de una única subred.</p>
Uno a muchos	<p>Todas las máquinas de la red comparten una dirección IP externa. Una máquina interna puede tener direcciones IP estáticas o DHCP. Todas las máquinas pueden acceder a la red externa, pero ninguna de ellas estará accesible desde la red externa. Cuando esta opción se selecciona, se activa la casilla Habilitado correspondiente al grupo de DHCP.</p> <p>El tipo de conversión de red NAT uno a muchos le permite definir las reglas NAT cuando se agrega un componente de red NAT a un blueprint.</p>

- 7 Introduzca una máscara de subred IP en el cuadro de texto **Máscara de subred**.

La máscara de subred especifica el tamaño de todo el espacio de direcciones enrutables que desea definir para su perfil de red.

Por ejemplo, escriba 255.255.0.0.
- 8 Introduzca una dirección de puerta de enlace enrutada o de Edge en el cuadro de texto **Puerta de enlace**.

Utilice un formato de dirección IPv4 estándar. Por ejemplo, escriba 10.10.110.1.

La dirección IP de puerta de enlace definida en el perfil de red se asigna a la NIC durante la asignación. Si no se asigna ningún valor en el cuadro de texto **Puerta de enlace** en el perfil de red, debe usar la propiedad personalizada `VirtualMachine.Network0.Gateway` al aprovisionar el equipo de Edge.
- 9 (opcional) En el grupo de DHCP, active la casilla de verificación **Habilitado** e introduzca los valores de **Inicio de rango de IP** y **Final de rango de IP**.

Esta casilla solo se puede activar si el tipo de NAT se estableció en Uno a muchos.
- 10 (opcional) Establezca un tiempo de concesión de DHCP para indicar el período durante el que una máquina puede usar una dirección IP.
- 11 Haga clic en la pestaña **DNS**.

12 Si es necesario, especifique los valores de DNS y WINS.

Los valores de DNS se utilizan para el registro y la resolución de los nombres DNS. Los campos de DNS y WINS son opcionales cuando se utiliza un endpoint de IPAM interno. Si se utiliza un endpoint de IPAM externo, el proveedor de IPAM de terceros proporciona los valores de DNS y WINS.

- a (opcional) Introduzca un valor para el servidor **DNS primario**.
- b (opcional) Introduzca un valor para el servidor **DNS secundario**.
- c (opcional) Introduzca un valor en **Sufijos DNS**.
- d (opcional) Introduzca un valor en **Sufijos de búsqueda de DNS**.
- e (opcional) Introduzca un valor para el servidor **WINS preferido**.
- f (opcional) Introduzca un valor para el servidor **WINS alternativo**.

Pasos siguientes

[Configurar rangos de IP de perfil de red NAT con el endpoint de IPAM de vRealize Automation.](#)

Configurar rangos de IP de perfil de red NAT con el endpoint de IPAM de vRealize Automation. Se pueden definir unos o varios rangos de direcciones IP estáticas para usarlos al aprovisionar una red.

No es posible superponer las direcciones IP del rango de red inicial y final con las direcciones DHCP. Si intenta guardar un perfil que contiene rangos de direcciones que se superponen, vRealize Automation muestra un error de validación.

Requisitos previos

[Indicar información de perfil de red NAT con el endpoint de IPAM de vRealize Automation.](#)

Procedimiento

- 1** Haga clic en la pestaña **Rangos de redes** para crear un nuevo rango de redes o para seleccionar un rango de redes existente.

Aparecen los detalles del rango seleccionado, como el nombre, la descripción y la dirección IP inicial y final. También se ofrece información relativa al estado.

- 2** Haga clic en **Nuevo** para especificar manualmente un nuevo nombre de rango de redes y un rango de direcciones IP, o haga clic en **Importar de CSV** para importar la información de direcciones IP de un archivo CSV con el formato correcto.

- Haga clic en **Nuevo**.
 - a Introduzca un nombre de rango de redes.
 - b Introduzca una descripción del rango de redes.
 - c Introduzca la dirección IP de inicio del rango.
 - d Introduzca la dirección IP final del rango.

- Haga clic en **Importar de CSV**.

- a Busque el archivo CSV y selecciónelo, o arrastre el archivo CSV al cuadro de diálogo **Importar de CSV**.

Las filas del archivo CSV tienen el formato *dirección_ip, nombre_máquina, estado, desplazamiento de NIC*. Por ejemplo:

```
100.10.100.1,mymachine01,Allocated
```

Campo de CSV	Descripción
ip_address	Una dirección IP con el formato IPv4.
machine_name	Nombre de una máquina administrada en vRealize Automation. Si el campo está vacío, no hay ningún nombre de forma predeterminada. Si el campo está vacío, el valor del campo status no puede ser Asignado.
status	Puede ser Asignado o Sin asignar. Se distingue entre mayúsculas y minúsculas. Si el campo está vacío, el valor predeterminado es Sin asignar. Si el estado es Asignado, el campo machine_name no puede estar vacío.
NIC_offset	Un entero no negativo. Opcional.

- b Haga clic en **Aplicar**.

3 Haga clic en **Aceptar**.

El nombre del rango de IP aparece en la lista Rangos definidos. Las direcciones IP del rango aparecen en la lista Direcciones IP definidas.

Las direcciones IP cargadas aparecen en la página **Direcciones IP** cuando se hace clic en **Aplicar**, o bien después de guardar y editar el perfil de red.

- 4 Haga clic en la pestaña **Direcciones IP** para mostrar las direcciones IP del rango de redes con nombre.
- 5 (opcional) Seleccione la información de dirección IP del menú desplegable **Rango de redes** para filtrar las entradas de direcciones IP.

Puede mostrar información sobre todos los rangos de redes definidos, los rangos de redes importados de un archivo CSV o un rango de redes con nombre. Se incluyen detalles como la dirección IP inicial, el nombre de la máquina, la marca de hora y la fecha de la última modificación, y el estado de IP.

- 6 (opcional) Seleccione un tipo de estado en el menú desplegable **Estado de IP** para filtrar las entradas de direcciones IP únicamente a aquellas que coincidan con el estado de IP seleccionado. Las opciones de estado son Asignado, Sin asignar, Destruído y Caducado.

En las direcciones IP con el estado Caducado o Destruído, puede hacer clic en **Recuperar** para permitir la asignación de esos rangos de direcciones IP. Es necesario guardar el perfil para que la recuperación sea efectiva. Las direcciones no se recuperan inmediatamente, de modo que la columna de estado no cambia al instante de Caducado o Destruído a Asignado.

7 Haga clic en **Aceptar**.

Crear un perfil de red NAT mediante un endpoint de IPAM de terceros

Puede crear un perfil de red NAT de NSX a petición relativo a un perfil de red externa. Cuando se utiliza un perfil de red NAT de NSX con un endpoint de IPAM de terceros, el proveedor de IPAM de terceros crea y administra un espacio de IP.

Cuando se utiliza un endpoint de IPAM de terceros en el perfil de red NAT, el proveedor crea nuevos rangos de IP para cada instancia de la red a petición. Se crea un conjunto interno de las direcciones IP definidas con uno o varios rangos en el endpoint del proveedor de IPAM de terceros por cada instancia de la red NAT. Estos rangos de IP se utilizan para asignar direcciones IP de las máquinas asignadas a la red NAT en la misma implementación. Dado que no se pueden definir direcciones IP duplicadas en el mismo espacio de direcciones, el proveedor crea un nuevo espacio de direcciones por cada instancia de la red NAT. Cuando se destruye una red NAT, sus rangos se destruyen en el endpoint del proveedor de IPAM y en el nuevo espacio de direcciones.

Puede usar rangos de IP obtenidos del endpoint de IPAM de VMware suministrado o de un endpoint de proveedor de servicios de IPAM de terceros que se haya registrado y configurado en vRealize Orchestrator (por ejemplo, Infoblox IPAM). Durante la asignación, se crea un rango de IP desde un bloque de IP.

En una red NAT uno a muchos, puede definir las reglas NAT que se pueden configurar cuando se añade un componente de red NAT al blueprint y se pueden cambiar cuando se edita la red NAT en una implementación.

Procedimiento

1 Especificación de la información de perfil de red NAT con un endpoint de IPAM de terceros

La información de perfil de red permite identificar las propiedades de red NAT, su perfil de red externa subyacente y otros valores que se utilizan al aprovisionar la red cuando se usa un endpoint de IPAM de terceros.

2 Configurar rangos de IP de perfil de red NAT con un endpoint de IPAM de terceros

Puede definir uno o varios rangos de direcciones IP para utilizarlos en el aprovisionamiento de una red mediante NAT.

Especificación de la información de perfil de red NAT con un endpoint de IPAM de terceros

La información de perfil de red permite identificar las propiedades de red NAT, su perfil de red externa subyacente y otros valores que se utilizan al aprovisionar la red cuando se usa un endpoint de IPAM de terceros.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Cree un perfil de red externa. Consulte [Crear un perfil de red externa mediante el endpoint de IPAM suministrado](#) o [Crear un perfil de red externa mediante un proveedor de IPAM de terceros](#).
- Cree y configure un endpoint de IPAM de terceros. Consulte [Crear un endpoint de proveedor de IPAM de terceros](#).

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Perfiles de red**.
- 2 Haga clic en **Nuevo** y seleccione **NAT** en el menú desplegable.
- 3 Especifique un nombre y, opcionalmente, una descripción.
- 4 Si ha configurado uno o más endpoints de proveedores de IPAM de terceros, seleccione un endpoint de IPAM de terceros del menú desplegable **Endpoint de IPAM**.

Al seleccionar un endpoint de proveedor de IPAM de terceros que se ha registrado en vRealize Orchestrator, las direcciones IP se obtienen del proveedor de servicio de IPAM especificado. Las especificaciones de IP como las opciones de máscara de subred y DNS/WINS no están disponibles porque sus funciones las controla el endpoint de IPAM de terceros seleccionado.

- 5 Seleccione un perfil de red externa existente en el menú desplegable **Perfil de red externa**.

Solo los perfiles de redes externas que están configurados para usar el endpoint de IPAM especificado se enumeran y se pueden seleccionar.

- 6 Seleccione el tipo de conversión de dirección de red uno a uno o uno a varios en el menú desplegable **Tipo de NAT**.

Opción	Descripción
Uno a uno	<p>Asigne una dirección IP estática externa a cada adaptador de red. Todas las máquinas pueden acceder a la red externa y serán accesibles desde la red externa.</p> <p>Todas las direcciones IP externas que estén asignadas a un vínculo superior de NSX Edge deben formar parte de la misma subred. Cuando se utiliza NAT 1:1 en vRealize Automation, el perfil de red externa correspondiente debe contener solo los rangos de IP que existen dentro de una única subred.</p>
Uno a muchos	<p>Todas las máquinas de la red comparten una dirección IP externa. Una máquina interna solo puede utilizar direcciones IP estáticas. Todas las máquinas pueden acceder a la red externa, pero ninguna de ellas estará accesible desde la red externa.</p> <p>DHCP no es compatible cuando se utiliza NAT con un proveedor IPAM de terceros.</p> <p>El tipo de conversión de red NAT uno a muchos le permite definir las reglas NAT cuando se agrega un componente de red NAT a un blueprint.</p>

- 7 Introduzca una máscara de subred IP en el cuadro de texto **Máscara de subred**.

La máscara de subred especifica el tamaño de todo el espacio de direcciones enrutables que desea definir para su perfil de red.

Por ejemplo, escriba 255.255.0.0.

- 8 Introduzca una dirección de puerta de enlace enrutada o de Edge en el cuadro de texto **Puerta de enlace**.

Utilice un formato de dirección IPv4 estándar. Por ejemplo, escriba 10.10.110.1.

La dirección IP de puerta de enlace definida en el perfil de red se asigna a la NIC durante la asignación. Si no se asigna ningún valor en el cuadro de texto **Puerta de enlace** en el perfil de red, debe usar la propiedad personalizada `VirtualMachine.Network0.Gateway` al aprovisionar el equipo de Edge.

9 Haga clic en la pestaña **DNS**.

10 Si es necesario, especifique los valores de DNS y WINS.

Los valores de DNS se utilizan para el registro y la resolución de los nombres DNS. Los campos de DNS y WINS son opcionales cuando se utiliza un endpoint de IPAM interno. Si se utiliza un endpoint de IPAM externo, el proveedor de IPAM de terceros proporciona los valores de DNS y WINS.

- a (opcional) Introduzca un valor para el servidor **DNS primario**.
- b (opcional) Introduzca un valor para el servidor **DNS secundario**.
- c (opcional) Introduzca un valor en **Sufijos DNS**.
- d (opcional) Introduzca un valor en **Sufijos de búsqueda de DNS**.
- e (opcional) Introduzca un valor para el servidor **WINS preferido**.
- f (opcional) Introduzca un valor para el servidor **WINS alternativo**.

Pasos siguientes

[Configurar rangos de IP de perfil de red NAT con un endpoint de IPAM de terceros.](#)

Configurar rangos de IP de perfil de red NAT con un endpoint de IPAM de terceros
Puede definir uno o varios rangos de direcciones IP para utilizarlos en el aprovisionamiento de una red mediante NAT.

Requisitos previos

[Especificación de la información de perfil de red NAT con un endpoint de IPAM de terceros.](#)

Procedimiento

1 Haga clic en la pestaña **Rangos de redes** para crear un nuevo rango de redes o para seleccionar un rango de redes existente.

Aparecen los detalles del rango seleccionado, como el nombre, la descripción y la dirección IP inicial y final. También se ofrece información relativa al estado.

2 Haga clic en **Nuevo** y defina un rango de redes.

- a Introduzca un nombre de rango de redes y una descripción.
- b Introduzca la dirección IP de inicio y finalización para definir el rango.
- c Haga clic en **Aplicar**.

3 Haga clic en **Aceptar**.

El nombre del rango de IP aparece en la lista Rangos definidos. Las direcciones IP del rango aparecen en la lista Direcciones IP definidas.

Las direcciones IP cargadas aparecen en la página **Direcciones IP** cuando se hace clic en **Aplicar**, o bien después de guardar y editar el perfil de red.

4 Haga clic en la pestaña **Direcciones IP** para mostrar las direcciones IP del rango de redes con nombre.**5** (opcional) Seleccione la información de dirección IP del menú desplegable **Rango de redes** para filtrar las entradas de direcciones IP.

Puede mostrar información sobre todos los rangos de redes definidos, los rangos de redes importados de un archivo CSV o un rango de redes con nombre. Se incluyen detalles como la dirección IP inicial, el nombre de la máquina, la marca de hora y la fecha de la última modificación, y el estado de IP.

6 (opcional) Seleccione un tipo de estado en el menú desplegable **Estado de IP** para filtrar las entradas de direcciones IP únicamente a aquellas que coincidan con el estado de IP seleccionado. Las opciones de estado son Asignado, Sin asignar, Destruído y Caducado.

En las direcciones IP con el estado Caducado o Destruído, puede hacer clic en **Recuperar** para permitir la asignación de esos rangos de direcciones IP. Es necesario guardar el perfil para que la recuperación sea efectiva. Las direcciones no se recuperan inmediatamente, de modo que la columna de estado no cambia al instante de Caducado o Destruído a Asignado.

7 Haga clic en **Aceptar**.**Liberar las direcciones IP mediante la destrucción de máquinas aprovisionadas**

Cuando destruye una implementación, las direcciones IP se eliminan. Las direcciones IP asignadas, por ejemplo la IP en un rango de perfiles de red, se liberan y quedan disponibles para el aprovisionamiento posterior.

Si destruye una máquina que tenga una dirección IP estática, su dirección IP queda disponible para que la usen otras máquinas. Es posible que las direcciones no utilizadas no queden disponibles inmediatamente, ya que el proceso de recuperación de direcciones IP estáticas se ejecuta cada 30 minutos.

Si está utilizando un proveedor de IPAM de terceros, vRealize Automation elimina las direcciones IP asociadas mediante el flujo de trabajo de vRealize Orchestrator del complemento o el paquete del proveedor de IPAM de terceros.

Configurar las reservas y las políticas de reserva

Una reserva de vRealize Automation puede definir políticas, prioridades y cuotas que determinan la colocación de máquinas para las solicitudes de aprovisionamiento.

Las políticas de reserva limitan el aprovisionamiento de máquinas a un subconjunto de reservas disponibles. Las políticas de reserva de almacenamiento permiten a los arquitectos de blueprint asignar volúmenes de máquinas a distintos almacenes de datos.

Para aprovisionar correctamente, la reserva debe tener suficiente espacio de almacenamiento disponible. La disponibilidad de almacenamiento de la reserva depende de:

- La cantidad de almacenamiento disponible en el almacén de datos o clúster.
- La cantidad de almacenamiento reservado para ese almacén de datos o clúster.
- La cantidad de almacenamiento que ya se ha asignado en vRealize Automation

Por ejemplo, incluso si vCenter Server tiene almacenamiento disponible para el almacén de datos o clúster, si no se reservó suficiente espacio de almacenamiento en la reserva, el aprovisionamiento genera un error "No hay reservas disponibles para asignar...". El almacenamiento asignado en una reserva depende de la cantidad de máquinas virtuales (independientemente de su estado) en esa reserva específica. Consulte el artículo de la base de conocimientos de VMware *Equipo XXX: no hay reservas disponibles para asignar dentro del grupo XXX. Se solicitó un total de XX GB de almacenamiento (2151030)* en <http://kb.vmware.com/kb/2151030> para obtener más información.

Reservas

Puede crear una reserva de vRealize Automation para asignar recursos de aprovisionamiento del grupo de tejidos a un grupo empresarial específico.

Por ejemplo, se pueden usar reservas para especificar que un recurso compartido de la memoria, CPU, redes y recursos de almacenamiento de un solo recurso informático pertenece a un grupo empresarial en particular, o bien para indicar que algunas máquinas se asignen a un grupo empresarial concreto.

Nota El almacenamiento y la memoria que se asignan a una máquina aprovisionada por una reserva se liberan cuando se elimina en vRealize Automation la máquina a la que están asignados, mediante la acción Destruir. El almacenamiento y la memoria no se liberan si la máquina se elimina en vCenter Server.

Una reserva se puede crear para los siguientes tipos de máquina:

- vSphere
- vCloud Air
- vCloud Director
- Amazon EC2
- Azure
- Hyper V (SCVMM)
- Hyper-V independiente
- KVM (RHEV)

- OpenStack
- XenServer

Puede configurar opciones de seguridad para las máquinas virtuales que se van a aprovisionar mediante la especificación de información en el script de una reserva, un blueprint o un agente invitado. Si las máquinas que se aprovisionarán requieren un agente invitado, debe añadir una regla de seguridad que contenga ese requisito a la reserva o el blueprint. Por ejemplo, si usa una política de seguridad predeterminada que deniegue la comunicación entre todas las máquinas y dependa de una política de seguridad independiente para permitir la comunicación entre máquinas específicas, es posible que el agente invitado no pueda comunicarse con vRealize Automation durante la fase de personalización. Para evitar este problema durante el aprovisionamiento de máquinas, use una política de seguridad predeterminada que permita la comunicación durante la fase de personalización.

Elegir un escenario de reserva

Puede crear reservas con las que asignar recursos a grupos empresariales. El procedimiento para crear una reserva depende del escenario.

Elija un escenario de reserva en función del tipo de endpoint de destino.

Cada grupo empresarial debe contar como mínimo con una reserva para que sus miembros puedan aprovisionar máquinas de ese tipo. Por ejemplo, un grupo empresarial que tiene una reserva de OpenStack, pero no una reserva de Amazon, no podrá solicitar una máquina de Amazon. En este ejemplo, el grupo empresarial deberá asignar una reserva para recursos de Amazon expresamente.

Tabla 2-15. Elegir un escenario de reserva

Escenario	Procedimiento
Crear una reserva de vSphere.	Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer
Crear una reserva para asignar recursos para un endpoint de vCloud Air.	Crear una reserva de vCloud Air
Crear una reserva para asignar recursos para un endpoint de vCloud Director.	Crear una reserva de vCloud Director
Crear una reserva para asignar recursos de Amazon (usando o no Amazon Virtual Private Cloud).	Crear una reserva de Amazon EC2
Crear una reserva para asignar recursos de OpenStack.	Crear una reserva de OpenStack
Crear una reserva para asignar recursos para Hyper-V.	Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer
Crear una reserva para asignar recursos para KVM.	Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer
Crear una reserva para asignar recursos de OpenStack.	Crear una reserva de OpenStack
Crear una reserva para asignar recursos para SCVMM.	Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer

Tabla 2-15. Elegir un escenario de reserva (continuación)

Escenario	Procedimiento
Crear una reserva para asignar recursos para XenServer.	Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer
Crear una reserva para asignar recursos para Microsoft Azure.	Crear una reserva de Microsoft Azure

Crear reservas de la categoría de nube

Una reserva del tipo de categoría de nube proporciona acceso a los servicios de aprovisionamiento de una cuenta de servicio de nube de un grupo empresarial de vRealize Automation concreto. Los tipos de reserva de nube disponibles son Amazon, OpenStack, vCloud Air y vCloud Director.

Una reserva es un recurso compartido de la memoria, CPU, redes y almacenamiento de un recurso informático asignado a un grupo empresarial de vRealize Automation concreto.

Un grupo empresarial puede tener varias reservas en uno o varios endpoints.

El modelo de asignación de una reserva depende del modelo de asignación en el centro de datos asociado. Los modelos de asignación disponibles son Grupo de asignación, Pago por uso y Grupo de reserva. Para obtener información sobre los modelos de asignación, consulte la documentación de vCloud Director o de vCloud Air.

Además de definir el uso compartido de recursos de tejido asignados al grupo empresarial, una reserva puede definir también las políticas, prioridades y cuotas que determinan la colocación de las máquinas.

Para aprovisionar correctamente, la reserva debe tener suficiente espacio de almacenamiento disponible. La disponibilidad de almacenamiento de la reserva depende de:

- La cantidad de almacenamiento disponible en el almacén de datos o clúster.
- La cantidad de almacenamiento reservado para ese almacén de datos o clúster.
- La cantidad de almacenamiento que ya se ha asignado en vRealize Automation

Por ejemplo, incluso si vCenter Server tiene almacenamiento disponible para el almacén de datos o clúster, si no se reservó suficiente espacio de almacenamiento en la reserva, el aprovisionamiento genera un error "No hay reservas disponibles para asignar...". El almacenamiento asignado en una reserva depende de la cantidad de máquinas virtuales (independientemente de su estado) en esa reserva específica. Consulte el artículo de la base de conocimientos de VMware *Equipo XXX: no hay reservas disponibles para asignar dentro del grupo XXX. Se solicitó un total de XX GB de almacenamiento (2151030)* en <http://kb.vmware.com/kb/2151030> para obtener más información.

Explicación de la lógica de selección de las reservas de nube

Cuando un miembro de un grupo empresarial crea una solicitud de aprovisionamiento para una máquina en la nube, vRealize Automation selecciona una máquina de una de las reservas que están disponibles para ese grupo empresarial. Las reservas de nube incluyen Amazon, OpenStack, vCloud Air y vCloud Director.

La reserva para la que se aprovisiona una máquina debe cumplir los siguientes criterios:

- La reserva debe ser del mismo tipo de plataforma que el blueprint desde el que se ha solicitado la máquina.
- La reserva debe estar habilitada.
- La reserva debe tener capacidad de sobra en la cuota de máquinas o tener una cuota ilimitada.

La cuota de máquinas asignada incluye solo las máquinas que están encendidas. Por ejemplo, si una reserva tiene una cuota de 50, y se han aprovisionado 40 máquinas, pero solo 20 de ellas están encendidas, la cuota de la reserva se ha asignado al 40 %, no al 80 %.

- La reserva debe tener grupos de seguridad especificados en la solicitud de máquina.
- La reserva debe asociarse a una región que tenga la imagen de máquina especificada en el blueprint.
- La reserva debe tener suficiente memoria y recursos de almacenamiento no asignados para aprovisionar la máquina.

En las reservas de pago por uso, los recursos pueden ser ilimitados.

- Para las máquinas de Amazon, la solicitud especifica una zona de disponibilidad y si la máquina debe aprovisionarse con una subred en nube privada virtual (VPC) o una ubicación no de VPC. La reserva debe coincidir con el tipo de red (VPC o no de VPC).
- Para vCloud Air o vCloud Director, si la solicitud especifica un modelo de asignación, el centro de datos virtual asociado a la reserva debe tener el mismo modelo de asignación.
- Para vCloud Director o vCloud Air, se debe habilitar la organización especificada.
- Las plantillas de blueprint deben estar disponibles en la reserva. Si la política de reserva se asigna a más de un recurso, las plantillas deberían ser públicas.
- Si el proveedor de nube es compatible con la selección de red y el blueprint tiene una configuración de red específica, la reserva debe tener las mismas redes.

Si el blueprint o la reserva especifican un perfil de red para la asignación de direcciones IP estáticas, debe haber una dirección IP disponible para asignarla a la nueva máquina.

- Si la solicitud especifica un modelo de asignación, el modelo de asignación de la reserva debe coincidir con el de la solicitud.
- Si el blueprint especifica una política de reserva, la reserva debe pertenecer a la política de reserva.

Las políticas de reserva son un modo de garantizar que la reserva seleccionada cumple los requisitos de aprovisionamiento de máquinas desde un blueprint específico. Por ejemplo, si un blueprint usa una imagen de máquina específica, puede usar políticas de reserva para restringir el aprovisionamiento para las reservas asociadas a las regiones que contienen la imagen necesaria.

Si no hay reservas que cumplan todos los criterios de selección disponibles, se producirá un error de aprovisionamiento.

Si hay varias reservas que cumplen todos los criterios, la reserva desde la que se aprovisionará la máquina solicitada se determinará mediante la siguiente lógica:

- Una reserva con un valor de prioridad inferior se selecciona antes que una reserva con un valor de prioridad mayor.
- Si hay varias reservas con la misma prioridad, se seleccionará la reserva cuyo porcentaje de cuota de máquinas asignado sea menor.
- Si hay varias reservas con la misma prioridad y el mismo uso de cuota, las máquinas se distribuirán entre las reservas por turnos.

Nota Aunque no se admite la selección por turnos de perfiles de red, sí se admite la selección por turnos de redes (si las hay), que pueden asociarse a distintos perfiles de red.

Si hay varias rutas de almacenamiento disponibles en una reserva con suficiente capacidad para aprovisionar los volúmenes de máquinas, las rutas de almacenamiento se seleccionarán según la siguiente lógica:

- Una ruta de almacenamiento con un valor de prioridad inferior se selecciona antes que una ruta de almacenamiento con un valor de prioridad mayor.
- Si el blueprint o la solicitud especifican una política de reserva de almacenamiento, la ruta de almacenamiento debe pertenecer a la política de reserva de almacenamiento.

Si la propiedad personalizada `VirtualMachine.DiskN.StorageReservationPolicyMode` se establece como `NotExact`, y no hay ninguna ruta de almacenamiento con suficiente capacidad disponible en la política de reserva de almacenamiento, el aprovisionamiento continuará con una ruta de almacenamiento externa a la política de reserva de almacenamiento. El valor predeterminado de `VirtualMachine.DiskN.StorageReservationPolicyMode` es `Exacta`.

- Si hay varias rutas de almacenamiento con la misma prioridad, las máquinas se distribuirán entre las rutas de almacenamiento mediante una programación por turnos.

Crear una reserva de Amazon EC2

Debe asignar recursos a máquinas; para ello, cree una reserva antes de que los miembros de un grupo empresarial puedan solicitar el aprovisionamiento de máquinas.

Puede trabajar con reservas de Amazon para Amazon Virtual Private Cloud o no VPC de Amazon. Los usuarios de Amazon Web Services pueden crear una Amazon Virtual Private Cloud para diseñar una topología de red virtual acorde con sus especificaciones. Si tiene previsto utilizar Amazon VPC, deberá asignar una Amazon VPC a una reserva de vRealize Automation. Consulte .

Cuando cree una reserva de Amazon o configure un componente de máquina en el blueprint, puede elegir en la lista de grupos de seguridad que están disponibles en la región de Amazon especificada. Los grupos de seguridad se importan durante la recopilación de datos.

Nota Tras crear una reserva, no podrá cambiar el grupo empresarial ni las asociaciones de recursos informáticos.

Para obtener información sobre cómo crear una Amazon VPC usando la AWS Management Console, consulte la documentación de Amazon Web Services.

Procedimiento

1 Especificar la información de reserva de Amazon

Cada reserva se configura para un grupo empresarial específico, de forma que este pueda solicitar máquinas en un recurso informático determinado.

2 Especificar los recursos y valores de configuración de red de reservas de Amazon

Indique los recursos y valores de configuración de red para aprovisionar máquinas desde esta reserva de vRealize Automation.

3 Especificar propiedades personalizadas y alertas de reservas de Amazon

Se pueden asociar propiedades personalizadas a una reserva de vRealize Automation. También se pueden configurar alertas para enviar notificaciones de correo electrónico cuando el nivel de recursos de las reservas sea bajo.

Especificar la información de reserva de Amazon

Cada reserva se configura para un grupo empresarial específico, de forma que este pueda solicitar máquinas en un recurso informático determinado.

Nota Tras crear una reserva, no podrá cambiar el grupo empresarial ni las asociaciones de recursos informáticos.

Puede controlar la visualización de las reservas al añadir, editar o eliminar mediante la opción **Filtrar por categoría** de la página Reservas. Tenga en cuenta que las reservas del agente de prueba no aparecen en la lista de reservas al filtrar por categoría.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Compruebe que un administrador de tenants haya creado al menos un grupo empresarial.
- Compruebe que existe un recurso informático.
- Configure los ajustes de red.
- (opcional) Configure la información del perfil de red.
- Compruebe que tiene acceso a la red de Amazon deseada. Por ejemplo, si quiere usar VPC, confirme que tiene acceso a la red de Amazon Virtual Private Cloud (VPC).

- Confirme que existen los pares de claves necesarios. Consulte [Administrar pares de claves](#).

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Reservas**.
- 2 Haga clic en el icono **Nuevo** (+) y seleccione el tipo de reserva que desea crear.
 Seleccione **Amazon EC2**.
- 3 (opcional) Seleccione una reserva existente en el menú desplegable **Copiar de reserva existente**.
 Aparecerán los datos de la reserva seleccionada. Puede efectuar los cambios necesarios para la nueva reserva.
- 4 Escriba un nombre en el cuadro de texto **Nombre**.
- 5 Seleccione un tenant en el menú desplegable **Tenant**.
- 6 Seleccione un grupo empresarial en el menú desplegable **Grupo empresarial**.
 Solo los usuarios de este grupo empresarial podrán aprovisionar máquinas mediante esta reserva.
- 7 (opcional) Seleccione una política de reserva del menú desplegable **Política de reserva**.
 Esta opción requiere que existan una o más políticas de reserva. Puede editar la reserva más tarde para especificar una política de reserva.
 Use una política de reserva para limitar el aprovisionamiento a reservas determinadas.
- 8 Escriba un número en el cuadro de texto **Prioridad** para establecer la prioridad de la reserva.
 La prioridad se utiliza cuando un grupo empresarial tiene más de una reserva. Una reserva con prioridad 1 se utiliza para el aprovisionamiento antes que una con prioridad 2.
- 9 (opcional) Anule la selección de la casilla de verificación **Habilitar esta reserva** si no desea activar la reserva.

Resultados

No abandone esta página. La reserva no se ha completado.

Especificar los recursos y valores de configuración de red de reservas de Amazon

Indique los recursos y valores de configuración de red para aprovisionar máquinas desde esta reserva de vRealize Automation.

Cuando cree una reserva de Amazon o configure un componente de máquina en el blueprint, puede elegir en la lista de grupos de seguridad que están disponibles en la región de la cuenta de Amazon especificada. Los grupos de seguridad se importan durante la recopilación de datos. Un grupo de seguridad actúa como un firewall para controlar el acceso a una máquina. Cada región incluye, como mínimo, el grupo de seguridad predeterminado. Los administradores

pueden usar la Amazon Web Services Management Console para crear grupos de seguridad adicionales, configurar puertos para Microsoft Remote Desktop Protocol o SSH, y configurar una red privada virtual para una Amazon VPN. Para obtener información sobre la creación y el uso de grupos de seguridad en Amazon Web Services, consulte la documentación de Amazon.

Para obtener información relacionada sobre los equilibradores de carga, consulte *Configuración de vRealize Automation*.

Requisitos previos

[Especificar la información de reserva de Amazon.](#)

Procedimiento

- 1 Haga clic en la pestaña **Recursos**.
- 2 Seleccione un recurso informático en el que aprovisionar máquinas en el menú desplegable **Recurso informático**.

Aparecerá una lista con las regiones de Amazon disponibles.

- 3 (opcional) Escriba un número en el cuadro de texto **Cuota de máquinas** para establecer el número máximo de máquinas que se puede aprovisionar en esta reserva.

Solo las máquinas que están encendidas cuentan para la cuota. Deje el campo en blanco para que la reserva sea ilimitada.

- 4 Seleccione un método de asignación de pares de claves a instancias informáticas en el menú desplegable **Par de claves**.

Opción	Descripción
Sin especificar	Controla el comportamiento del par de claves a nivel de blueprint en vez de a nivel de reserva.
Autogenerado por cada grupo empresarial	Cada máquina aprovisionada del mismo grupo empresarial tiene el mismo par de claves, incluidas las máquinas aprovisionadas en otras reservas cuando la máquina tiene el mismo recurso informático y el mismo grupo empresarial. Debido a que los pares de claves que se generan de este modo se asocian a un grupo empresarial, los pares de claves se eliminan cuando se elimina el grupo empresarial.
Autogenerado por cada máquina	Cada máquina tiene un par de claves único. Este es el método más seguro porque las máquinas no comparten pares de claves.
Par de claves específico	Cada máquina aprovisionada de la reserva tiene el mismo par de claves. Busque un par de claves para usarlo en la reserva.

- 5 Si ha seleccionado **Par de claves específico** en el menú desplegable **Par de claves**, seleccione un valor de par de claves en el menú desplegable **Par de claves específico**.

- 6** Si su configuración es para Amazon Virtual Private Cloud, active la casilla **Asignar a una subred de un VPC**. Si no, déjela desactivada.

Si activa **Asignar a una subred de un VPC**, las siguientes opciones de ubicaciones o subredes, grupos de seguridad y equilibradores de carga aparecen en un menú emergente, en lugar de en esta misma página.

Para una reserva de VPC, especifique las subredes y los grupos de seguridad de cada VPC autorizada en la reserva.

- 7** Seleccione una o varias de las ubicaciones (no VPC) o subredes (VPC) disponibles de las listas **Ubicaciones** o **Subredes**.

Seleccione todas las ubicaciones o subredes que quiera que estén disponibles para el aprovisionamiento.

- 8** Seleccione uno o más grupos de seguridad que se puedan asignar a una máquina durante el aprovisionamiento en la lista **Grupos de seguridad**.

Seleccione cada grupo de seguridad que se puede asignar a una máquina durante el aprovisionamiento. Todas las regiones disponibles requieren al menos un grupo de seguridad especificado.

- 9** Seleccione uno o más equilibradores de carga disponibles en la lista **Equilibradores de carga**.

Si usa la función de equilibradores de carga flexibles, seleccione uno o varios equilibradores de carga disponibles aplicables a las ubicaciones o subredes seleccionadas.

Resultados

Puede guardar la reserva al hacer clic en **Guardar**. O bien, puede añadir propiedades personalizadas para controlar aún más las especificaciones de reserva. También puede configurar alertas de correo electrónico para enviar notificaciones cuando disminuyan los recursos asignados a esa reserva.

Especificar propiedades personalizadas y alertas de reservas de Amazon

Se pueden asociar propiedades personalizadas a una reserva de vRealize Automation. También se pueden configurar alertas para enviar notificaciones de correo electrónico cuando el nivel de recursos de las reservas sea bajo.

Las alertas de correo electrónico y las propiedades personalizadas son configuraciones opcionales de la reserva. Si no desea asociar propiedades personalizadas ni establecer alertas, haga clic en **Guardar** para finalizar la creación de la reserva.

Puede añadir tantas propiedades personalizadas como sea necesario.

Si se configuran alertas, estas se generan diariamente, en vez de cuando se alcanzan los umbrales especificados.

Importante Las notificaciones solo se envían si se han configurado las alertas de correo electrónico y se han habilitado las notificaciones.

Requisitos previos

[Especificar los recursos y valores de configuración de red de reservas de Amazon.](#)

Procedimiento

- 1 Haga clic en la pestaña **Propiedades**.
- 2 Haga clic en **Nuevo**.
- 3 Escriba un nombre de propiedad personalizada válido.
- 4 Si corresponde, introduzca un valor de propiedad.
- 5 Haga clic en **Guardar**.
- 6 (opcional) Añada cualquier propiedad personalizada adicional.
- 7 Haga clic en la pestaña **Alertas**.
- 8 Active la casilla de verificación **Alertas de capacidad** para configurar las alertas que se enviarán.
- 9 Use el control deslizante para establecer los umbrales de la asignación de recursos disponibles.
- 10 Introduzca los nombres de usuario o grupo de AD (no las direcciones de correo electrónico) para recibir notificaciones de alerta en el cuadro de texto **Destinatarios**.
Introduzca un nombre en cada línea. Pulse Entrar para separar varias entradas.
- 11 Seleccione **Enviar alertas al administrador del grupo** para incluir a los administradores de los grupos en las alertas de correo electrónico.
Las alertas de correo electrónico se envían a los usuarios que estén incluidos en la lista **Enviar correos electrónicos del administrador a** del grupo empresarial.
- 12 Especifique la frecuencia de recordatorio (días).
- 13 Haga clic en **Guardar**.

Resultados

La reserva se ha guardado y aparece en la lista Reservas.

Pasos siguientes

Puede configurar políticas de reserva opcionales o empezar a preparar el aprovisionamiento.

Los usuarios con autorización para crear blueprints pueden crearlos ahora.

Crear una reserva de OpenStack

Debe asignar recursos a máquinas; para ello, cree una reserva antes de que los miembros de un grupo empresarial puedan solicitar el aprovisionamiento de máquinas.

Cree una reserva de OpenStack.

Procedimiento

1 Especificar la información de reserva de OpenStack

Cada reserva se configura para un grupo empresarial específico, de forma que este pueda solicitar máquinas en un recurso informático determinado.

2 Especificar los recursos y valores de configuración de red de reservas de reserva de OpenStack

Indique los recursos y valores de configuración de red disponibles para las máquinas que se aprovisionan desde esta reserva de vRealize Automation.

3 Especificar propiedades personalizadas y alertas de reservas de OpenStack

Se pueden asociar propiedades personalizadas a una reserva de vRealize Automation. También se pueden configurar alertas para enviar notificaciones de correo electrónico cuando el nivel de recursos de las reservas sea bajo.

Especificar la información de reserva de OpenStack

Cada reserva se configura para un grupo empresarial específico, de forma que este pueda solicitar máquinas en un recurso informático determinado.

Nota Tras crear una reserva, no podrá cambiar el grupo empresarial ni las asociaciones de recursos informáticos.

Puede controlar la visualización de las reservas al añadir, editar o eliminar mediante la opción **Filtrar por categoría** de la página Reservas. Tenga en cuenta que las reservas del agente de prueba no aparecen en la lista de reservas al filtrar por categoría.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Compruebe que un administrador de tenants haya creado al menos un grupo empresarial.
- Compruebe que existe un recurso informático.
- Compruebe que se han configurado las direcciones IP flotantes o grupos de seguridad opcionales.
- Confirme que existen los pares de claves necesarios. Consulte [Administrar pares de claves](#).
- Compruebe que existe un recurso informático.
- Configure los ajustes de red.

Procedimiento

1 Seleccione **Infraestructura > Reservas > Reservas**.

2 Haga clic en el icono **Nuevo** (+) y seleccione el tipo de reserva que desea crear.

Seleccione **OpenStack**.

- 3 (opcional) Seleccione una reserva existente en el menú desplegable **Copiar de reserva existente**.

Aparecerán los datos de la reserva seleccionada. Puede efectuar los cambios necesarios para la nueva reserva.

- 4 Escriba un nombre en el cuadro de texto **Nombre**.

- 5 Seleccione un tenant en el menú desplegable **Tenant**.

- 6 Seleccione un grupo empresarial en el menú desplegable **Grupo empresarial**.

Solo los usuarios de este grupo empresarial podrán aprovisionar máquinas mediante esta reserva.

- 7 (opcional) Seleccione una política de reserva del menú desplegable **Política de reserva**.

Esta opción requiere que existan una o más políticas de reserva. Puede editar la reserva más tarde para especificar una política de reserva.

Use una política de reserva para limitar el aprovisionamiento a reservas determinadas.

- 8 Escriba un número en el cuadro de texto **Prioridad** para establecer la prioridad de la reserva.

La prioridad se utiliza cuando un grupo empresarial tiene más de una reserva. Una reserva con prioridad 1 se utiliza para el aprovisionamiento antes que una con prioridad 2.

- 9 (opcional) Anule la selección de la casilla de verificación **Habilitar esta reserva** si no desea activar la reserva.

Resultados

No abandone esta página. La reserva no se ha completado.

Especificar los recursos y valores de configuración de red de reservas de reserva de OpenStack
Indique los recursos y valores de configuración de red disponibles para las máquinas que se aprovisionan desde esta reserva de vRealize Automation.

Requisitos previos

[Especificar la información de reserva de OpenStack.](#)

Procedimiento

- 1 Haga clic en la pestaña **Recursos**.

- 2 Seleccione un recurso informático en el que aprovisionar máquinas en el menú desplegable **Recurso informático**.

Solo las plantillas que se encuentran en el clúster que ha seleccionado están disponibles para la clonación con la reserva.

Durante el aprovisionamiento, las máquinas se ubican en un host conectado al almacenamiento local. Si la reserva usa almacenamiento local, todas las máquinas que se aprovisionan mediante la reserva se crean en el host que contiene el almacenamiento local. Sin embargo, si usa la propiedad personalizada `VirtualMachine.Admin.ForceHost`, que

obliga a una máquina a aprovisionarse en otro host, el aprovisionamiento no se realiza correctamente. El aprovisionamiento tampoco se realiza correctamente si la plantilla a partir de la cual se clona la máquina se encuentra almacenada localmente, pero está conectada a una máquina de otro clúster. En tal caso, el aprovisionamiento no se realiza correctamente porque no puede acceder a la plantilla.

- 3 (opcional) Escriba un número en el cuadro de texto **Cuota de máquinas** para establecer el número máximo de máquinas que se puede aprovisionar en esta reserva.

Solo las máquinas que están encendidas cuentan para la cuota. Deje el campo en blanco para que la reserva sea ilimitada.

- 4 Seleccione un método de asignación de pares de claves a instancias informáticas en el menú desplegable **Par de claves**.

Opción	Descripción
Sin especificar	Controla el comportamiento del par de claves a nivel de blueprint en vez de a nivel de reserva.
Autogenerado por cada grupo empresarial	Cada máquina aprovisionada del mismo grupo empresarial tiene el mismo par de claves, incluidas las máquinas aprovisionadas en otras reservas cuando la máquina tiene el mismo recurso informático y el mismo grupo empresarial. Debido a que los pares de claves que se generan de este modo se asocian a un grupo empresarial, los pares de claves se eliminan cuando se elimina el grupo empresarial.
Autogenerado por cada máquina	Cada máquina tiene un par de claves único. Este es el método más seguro porque las máquinas no comparten pares de claves.
Par de claves específico	Cada máquina aprovisionada de la reserva tiene el mismo par de claves. Busque un par de claves para usarlo en la reserva.

- 5 Si ha seleccionado **Par de claves específico** en el menú desplegable **Par de claves**, seleccione un valor de par de claves en el menú desplegable **Par de claves específico**.
- 6 Seleccione uno o más grupos de seguridad que se puedan asignar a una máquina durante el aprovisionamiento en la lista **Grupos de seguridad**.
- 7 Haga clic en la pestaña **Red**.

8 Configure un nombre de red para las máquinas aprovisionadas mediante la reserva.

- a (opcional) Si la opción está disponible, seleccione un endpoint de almacenamiento en el menú desplegable **Endpoint**.

La opción FlexClone estará disponible en la columna de endpoint si hay un endpoint de NetApp ONTAP y si el host es virtual. Si hay un endpoint de NetApp ONTAP, la página de reservas mostrará el endpoint asignado a la ruta de almacenamiento. Cuando se añade, actualiza o elimina un endpoint de una ruta de almacenamiento, el cambio se puede ver en todas las reservas relevantes.

Cuando se añade, actualiza o elimina un endpoint de una ruta de almacenamiento, el cambio se puede ver en la página de reservas.

- b Seleccione un nombre de red para las máquinas aprovisionadas mediante esta reserva en la lista **Nombres de red**.

- c (opcional) Seleccione un perfil de red de la lista en el menú desplegable **Perfil de red**.

Esta opción requiere que existan uno o más perfiles de red.

Puede seleccionar más de un nombre de red en una reserva, pero solo se usará una red al aprovisionar máquinas.

Resultados

Puede guardar la reserva al hacer clic en **Guardar**. O bien, puede añadir propiedades personalizadas para controlar aún más las especificaciones de reserva. También puede configurar alertas de correo electrónico para enviar notificaciones cuando disminuyan los recursos asignados a esa reserva.

Especificar propiedades personalizadas y alertas de reservas de OpenStack

Se pueden asociar propiedades personalizadas a una reserva de vRealize Automation. También se pueden configurar alertas para enviar notificaciones de correo electrónico cuando el nivel de recursos de las reservas sea bajo.

Las alertas de correo electrónico y las propiedades personalizadas son configuraciones opcionales de la reserva. Si no desea asociar propiedades personalizadas ni establecer alertas, haga clic en **Guardar** para finalizar la creación de la reserva.

Puede añadir tantas propiedades personalizadas como sea necesario.

Importante Las notificaciones solo se envían si se han configurado las alertas de correo electrónico y se han habilitado las notificaciones.

Si se configuran alertas, estas se generan diariamente, en vez de cuando se alcanzan los umbrales especificados.

Requisitos previos

[Especificar los recursos y valores de configuración de red de reservas de reserva de OpenStack.](#)

Procedimiento

- 1 Haga clic en la pestaña **Propiedades**.
- 2 Haga clic en **Nuevo**.
- 3 Escriba un nombre de propiedad personalizada válido.
- 4 Si corresponde, introduzca un valor de propiedad.
- 5 Haga clic en **Guardar**.
- 6 (opcional) Añada cualquier propiedad personalizada adicional.
- 7 Haga clic en la pestaña **Alertas**.
- 8 Active la casilla de verificación **Alertas de capacidad** para configurar las alertas que se enviarán.
- 9 Use el control deslizante para establecer los umbrales de la asignación de recursos disponibles.
- 10 Introduzca los nombres de usuario o grupo de AD (no las direcciones de correo electrónico) para recibir notificaciones de alerta en el cuadro de texto **Destinatarios**.
Introduzca un nombre en cada línea. Pulse Entrar para separar varias entradas.
- 11 Seleccione **Enviar alertas al administrador del grupo** para incluir a los administradores de los grupos en las alertas de correo electrónico.
Las alertas de correo electrónico se envían a los usuarios que estén incluidos en la lista **Enviar correos electrónicos del administrador a** del grupo empresarial.
- 12 Especifique la frecuencia de recordatorio (días).
- 13 Haga clic en **Guardar**.

Resultados

La reserva se ha guardado y aparece en la lista Reservas.

Pasos siguientes

Puede configurar políticas de reserva opcionales o empezar a preparar el aprovisionamiento.

Los usuarios con autorización para crear blueprints pueden crearlos ahora.

Crear una reserva de vCloud Air

Debe asignar recursos a máquinas; para ello, cree una reserva de vRealize Automation antes de que los miembros de un grupo empresarial puedan solicitar el aprovisionamiento de máquinas.

Cada grupo empresarial debe contar como mínimo con una reserva para que sus miembros puedan aprovisionar máquinas de ese tipo.

Procedimiento

1 Especificar la información de reserva de vCloud Air

Puede crear una reserva por cada recurso de OnDemand o suscripción de máquina de vCloud Air. Cada reserva se configura para un grupo empresarial específico, de forma que este pueda solicitar máquinas.

2 Especificar los recursos y valores de configuración de red de una reserva de vCloud Air

Indique los recursos y valores de configuración de red disponibles para las máquinas de vCloud Air que se aprovisionan desde esta reserva de vRealize Automation.

3 Especificar propiedades personalizadas y alertas de una reserva de vCloud Air

Se pueden asociar propiedades personalizadas a una reserva de vRealize Automation. También se pueden configurar alertas para enviar notificaciones de correo electrónico cuando el nivel de recursos de las reservas sea bajo.

Pasos siguientes

Puede configurar políticas de reserva opcionales o empezar a preparar el aprovisionamiento.

Los usuarios con autorización para crear blueprints pueden crearlos ahora.

Especificar la información de reserva de vCloud Air

Puede crear una reserva por cada recurso de OnDemand o suscripción de máquina de vCloud Air. Cada reserva se configura para un grupo empresarial específico, de forma que este pueda solicitar máquinas.

Puede controlar la visualización de las reservas al añadir, editar o eliminar mediante la opción **Filtrar por categoría** de la página Reservas. Tenga en cuenta que las reservas del agente de prueba no aparecen en la lista de reservas al filtrar por categoría.

Nota Tras crear una reserva, no podrá cambiar el grupo empresarial ni las asociaciones de recursos informáticos.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Compruebe que un administrador de tenants haya creado al menos un grupo empresarial.
- Compruebe que existe un recurso informático.
- Configure los ajustes de red.
- (opcional) Configure la información del perfil de red.

Procedimiento

1 Seleccione **Infraestructura > Reservas > Reservas**.

- 2 Haga clic en el icono **Nuevo** (+) y seleccione el tipo de reserva que desea crear.

Los tipos de reserva de nube disponibles son Amazon, OpenStack, vCloud Air y vCloud Director.

Seleccione **vCloud Air**.

- 3 (opcional) Seleccione una reserva existente en el menú desplegable **Copiar de reserva existente**.

Aparecerán los datos de la reserva seleccionada. Puede efectuar los cambios necesarios para la nueva reserva.

- 4 Escriba un nombre en el cuadro de texto **Nombre**.

- 5 Seleccione un tenant en el menú desplegable **Tenant**.

- 6 Seleccione un grupo empresarial en el menú desplegable **Grupo empresarial**.

Solo los usuarios de este grupo empresarial podrán aprovisionar máquinas mediante esta reserva.

- 7 (opcional) Seleccione una política de reserva del menú desplegable **Política de reserva**.

Esta opción requiere que existan una o más políticas de reserva. Puede editar la reserva más tarde para especificar una política de reserva.

Use una política de reserva para limitar el aprovisionamiento a reservas determinadas.

- 8 Escriba un número en el cuadro de texto **Prioridad** para establecer la prioridad de la reserva.

La prioridad se utiliza cuando un grupo empresarial tiene más de una reserva. Una reserva con prioridad 1 se utiliza para el aprovisionamiento antes que una con prioridad 2.

- 9 (opcional) Anule la selección de la casilla de verificación **Habilitar esta reserva** si no desea activar la reserva.

Resultados

No abandone esta página. La reserva no se ha completado.

Especificar los recursos y valores de configuración de red de una reserva de vCloud Air

Indique los recursos y valores de configuración de red disponibles para las máquinas de vCloud Air que se aprovisionan desde esta reserva de vRealize Automation.

Los modelos de asignación de recursos existentes para las máquinas aprovisionadas desde una reserva de vCloud Director son Grupo de asignación, Pago por uso y Grupo de reserva. En Pago por uso no es necesario especificar las cantidades de almacenamiento o memoria, pero sí una prioridad de la ruta de almacenamiento. Para obtener información detallada sobre estos modelos de asignación, consulte la documentación de vCloud Air.

Puede especificar un perfil de almacenamiento estándar o de nivel de disco. El almacenamiento en disco multinivel está disponible para endpoints de vCloud Air.

Para las integraciones que utilizan el almacenamiento Storage Distributed Resource Scheduler (SDRS), puede seleccionar un clúster de almacenamiento para permitir que SDRS controle la ubicación del almacenamiento y el equilibrio de carga de las máquinas aprovisionadas desde esta reserva. El modo de automatización de SDRS debe establecerse como Automático. De lo contrario, seleccione un almacén de datos del clúster para el comportamiento del almacén de datos independiente. SDRS no es compatible con dispositivos de almacenamiento de FlexClone.

Nota Las reservas definidas para los endpoints de vCloud Air y los endpoints de vCloud Director no admiten el uso de perfiles de red para aprovisionar máquinas.

Requisitos previos

[Especificar la información de reserva de vCloud Director.](#)

Procedimiento

1 Haga clic en la pestaña **Recursos**.

2 Seleccione un recurso informático en el que aprovisionar máquinas en el menú desplegable **Recurso informático**.

Solo las plantillas que se encuentran en el clúster que ha seleccionado están disponibles para la clonación con la reserva.

3 Seleccione un modelo de asignación.

4 (opcional) Escriba un número en el cuadro de texto **Cuota de máquinas** para establecer el número máximo de máquinas que se puede aprovisionar en esta reserva.

Solo las máquinas que están encendidas cuentan para la cuota. Deje el campo en blanco para que la reserva sea ilimitada.

5 Especifique la cantidad de memoria en GB que se asignará a la reserva en la tabla Memoria.

El valor de memoria total de la reserva se basa en la selección de recursos informáticos.

6 Seleccione una o más rutas de almacenamiento de la lista.

Las opciones de ruta de almacenamiento disponibles dependen de la selección de recursos informáticos.

a Escriba un valor en el cuadro de texto **Esta reserva reservada** para especificar la cantidad de almacenamiento que se asignará a la reserva.

b Escriba un valor en el cuadro de texto **Prioridad** para especificar el valor de prioridad de la ruta de almacenamiento relativo a otras rutas de almacenamiento que pertenecen a la reserva.

La prioridad se usa cuando hay varias rutas de almacenamiento. Una ruta de almacenamiento con prioridad 0 se usa antes que una con prioridad 1.

- c Haga clic en la opción **Deshabilitar** si no desea habilitar la ruta de almacenamiento para que la use esta reserva.
- d Repita este paso para configurar los clústeres y los almacenes de datos si es necesario.

7 Haga clic en la pestaña **Red**.

8 Configure un nombre de red para las máquinas aprovisionadas mediante la reserva.

- a (opcional) Si la opción está disponible, seleccione un endpoint de almacenamiento en el menú desplegable **Endpoint**.

La opción FlexClone estará disponible en la columna de endpoint si hay un endpoint de NetApp ONTAP y si el host es virtual. Si hay un endpoint de NetApp ONTAP, la página de reservas mostrará el endpoint asignado a la ruta de almacenamiento. Cuando se añade, actualiza o elimina un endpoint de una ruta de almacenamiento, el cambio se puede ver en todas las reservas relevantes.

Cuando se añade, actualiza o elimina un endpoint de una ruta de almacenamiento, el cambio se puede ver en la página de reservas.

- b Seleccione un nombre de red para las máquinas aprovisionadas mediante esta reserva en la lista **Nombres de red**.
- c (opcional) Seleccione un perfil de red de la lista en el menú desplegable **Perfil de red**.

Esta opción requiere que existan uno o más perfiles de red.

Puede seleccionar más de un nombre de red en una reserva, pero solo se usará una red al aprovisionar máquinas.

Resultados

Puede guardar la reserva al hacer clic en **Guardar**. O bien, puede añadir propiedades personalizadas para controlar aún más las especificaciones de reserva. También puede configurar alertas de correo electrónico para enviar notificaciones cuando disminuyan los recursos asignados a esa reserva.

Especificar propiedades personalizadas y alertas de una reserva de vCloud Air

Se pueden asociar propiedades personalizadas a una reserva de vRealize Automation. También se pueden configurar alertas para enviar notificaciones de correo electrónico cuando el nivel de recursos de las reservas sea bajo.

Las alertas de correo electrónico y las propiedades personalizadas son configuraciones opcionales de la reserva. Si no desea asociar propiedades personalizadas ni establecer alertas, haga clic en **Guardar** para finalizar la creación de la reserva.

Puede añadir tantas propiedades personalizadas como sea necesario.

Si se configuran alertas, estas se generan diariamente, en vez de cuando se alcanzan los umbrales especificados.

Importante Las notificaciones solo se envían si se han configurado las alertas de correo electrónico y se han habilitado las notificaciones.

Las alertas no están disponibles para las reservas de pago por uso que se crean sin límites específicos.

Requisitos previos

[Especificar los recursos y valores de configuración de red de una reserva de vCloud Air](#)

Procedimiento

- 1 Haga clic en la pestaña **Propiedades**.
- 2 Haga clic en **Nuevo**.
- 3 Escriba un nombre de propiedad personalizada válido.
- 4 Si corresponde, introduzca un valor de propiedad.
- 5 (opcional) Active la casilla de verificación **Cifrado** para cifrar el valor de propiedad.
- 6 (opcional) Active la casilla de verificación **Preguntar al usuario** para que sea obligatorio que el usuario introduzca un valor.

Esta opción no puede reemplazarse durante el aprovisionamiento.

- 7 Haga clic en **Guardar**.
- 8 (opcional) Añada cualquier propiedad personalizada adicional.
- 9 Haga clic en la pestaña **Alertas**.
- 10 Active la casilla de verificación **Alertas de capacidad** para configurar las alertas que se enviarán.
- 11 Use el control deslizante para establecer los umbrales de la asignación de recursos disponibles.
- 12 Introduzca los nombres de usuario o grupo de AD (no las direcciones de correo electrónico) para recibir notificaciones de alerta en el cuadro de texto **Destinatarios**.
Introduzca un nombre en cada línea. Pulse Entrar para separar varias entradas.
- 13 Seleccione **Enviar alertas al administrador del grupo** para incluir a los administradores de los grupos en las alertas de correo electrónico.
Las alertas de correo electrónico se envían a los usuarios que estén incluidos en la lista **Enviar correos electrónicos del administrador a** del grupo empresarial.
- 14 Especifique la frecuencia de recordatorio (días).
- 15 Haga clic en **Guardar**.

Resultados

La reserva se ha guardado y aparece en la lista Reservas.

Crear una reserva de vCloud Director

Debe asignar recursos a máquinas; para ello, cree una reserva de vRealize Automation antes de que los miembros de un grupo empresarial puedan solicitar el aprovisionamiento de máquinas.

Cada grupo empresarial debe contar como mínimo con una reserva para que sus miembros puedan aprovisionar máquinas de ese tipo.

Procedimiento

1 Especificar la información de reserva de vCloud Director

Puede crear una reserva por cada centro de datos virtual (vDC) de organización de vCloud Director. Cada reserva se configura para un grupo empresarial específico, de forma que este pueda solicitar máquinas en un recurso informático determinado.

2 Especificar los recursos y valores de configuración de red de una reserva de vCloud Director

Indique los recursos y valores de configuración de red disponibles para las máquinas de vCloud Director que se aprovisionan desde esta reserva de vRealize Automation.

3 Especificar propiedades personalizadas y alertas de reservas de vCloud Director

Se pueden asociar propiedades personalizadas a una reserva de vRealize Automation. También se pueden configurar alertas para enviar notificaciones de correo electrónico cuando el nivel de recursos de las reservas sea bajo.

Pasos siguientes

Puede configurar políticas de reserva opcionales o empezar a preparar el aprovisionamiento.

Los usuarios con autorización para crear blueprints pueden crearlos ahora.

Especificar la información de reserva de vCloud Director

Puede crear una reserva por cada centro de datos virtual (vDC) de organización de vCloud Director. Cada reserva se configura para un grupo empresarial específico, de forma que este pueda solicitar máquinas en un recurso informático determinado.

Puede controlar la visualización de las reservas al añadir, editar o eliminar mediante la opción **Filtrar por categoría** de la página Reservas. Tenga en cuenta que las reservas del agente de prueba no aparecen en la lista de reservas al filtrar por categoría.

Nota Tras crear una reserva, no podrá cambiar el grupo empresarial ni las asociaciones de recursos informáticos.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Compruebe que un administrador de tenants haya creado al menos un grupo empresarial.
- Compruebe que existe un recurso informático.
- Configure los ajustes de red.
- (opcional) Configure la información del perfil de red.

Procedimiento

1 Seleccione **Infraestructura > Reservas > Reservas**.

- 2 Haga clic en el icono **Nuevo** (+) y seleccione el tipo de reserva que desea crear.

Los tipos de reserva de nube disponibles son Amazon, OpenStack, vCloud Air y vCloud Director.

Seleccione **vCloud Director**.

- 3 (opcional) Seleccione una reserva existente en el menú desplegable **Copiar de reserva existente**.

Aparecerán los datos de la reserva seleccionada. Puede efectuar los cambios necesarios para la nueva reserva.

- 4 Escriba un nombre en el cuadro de texto **Nombre**.

- 5 Seleccione un tenant en el menú desplegable **Tenant**.

- 6 Seleccione un grupo empresarial en el menú desplegable **Grupo empresarial**.

Solo los usuarios de este grupo empresarial podrán aprovisionar máquinas mediante esta reserva.

- 7 (opcional) Seleccione una política de reserva del menú desplegable **Política de reserva**.

Esta opción requiere que existan una o más políticas de reserva. Puede editar la reserva más tarde para especificar una política de reserva.

Use una política de reserva para limitar el aprovisionamiento a reservas determinadas.

- 8 Escriba un número en el cuadro de texto **Prioridad** para establecer la prioridad de la reserva.

La prioridad se utiliza cuando un grupo empresarial tiene más de una reserva. Una reserva con prioridad 1 se utiliza para el aprovisionamiento antes que una con prioridad 2.

- 9 (opcional) Anule la selección de la casilla de verificación **Habilitar esta reserva** si no desea activar la reserva.

Resultados

No abandone esta página. La reserva no se ha completado.

Especificar los recursos y valores de configuración de red de una reserva de vCloud Director

Indique los recursos y valores de configuración de red disponibles para las máquinas de vCloud Director que se aprovisionan desde esta reserva de vRealize Automation.

Los modelos de asignación de recursos existentes para las máquinas aprovisionadas desde una reserva de vCloud Director son Grupo de asignación, Pago por uso y Grupo de reserva. En Pago por uso no es necesario especificar las cantidades de almacenamiento o memoria, pero sí una prioridad de la ruta de almacenamiento. Para obtener información detallada sobre estos modelos de asignación, consulte la documentación de vCloud Director.

Puede especificar un perfil de almacenamiento estándar o de nivel de disco. El almacenamiento en disco multinivel está disponible para vCloud Director 5.6 y endpoints superiores. No se admite el almacenamiento en disco multinivel para los endpoints de vCloud Director 5.5.

Para las integraciones que utilizan el almacenamiento Storage Distributed Resource Scheduler (SDRS), puede seleccionar un clúster de almacenamiento para permitir que SDRS controle la ubicación del almacenamiento y el equilibrio de carga de las máquinas aprovisionadas desde esta reserva. El modo de automatización de SDRS debe establecerse como Automático. De lo contrario, seleccione un almacén de datos del clúster para el comportamiento del almacén de datos independiente. SDRS no es compatible con dispositivos de almacenamiento de FlexClone.

Nota Las reservas definidas para los endpoints de vCloud Air y los endpoints de vCloud Director no admiten el uso de perfiles de red para aprovisionar máquinas.

Requisitos previos

[Especificar la información de reserva de vCloud Director.](#)

Procedimiento

1 Haga clic en la pestaña **Recursos**.

2 Seleccione un recurso informático en el que aprovisionar máquinas en el menú desplegable **Recurso informático**.

Solo las plantillas que se encuentran en el clúster que ha seleccionado están disponibles para la clonación con la reserva.

3 Seleccione un modelo de asignación.

4 (opcional) Escriba un número en el cuadro de texto **Cuota de máquinas** para establecer el número máximo de máquinas que se puede aprovisionar en esta reserva.

Solo las máquinas que están encendidas cuentan para la cuota. Deje el campo en blanco para que la reserva sea ilimitada.

5 Especifique la cantidad de memoria en GB que se asignará a la reserva en la tabla Memoria.

El valor de memoria total de la reserva se basa en la selección de recursos informáticos.

6 Seleccione una o más rutas de almacenamiento de la lista.

Las opciones de ruta de almacenamiento disponibles dependen de la selección de recursos informáticos.

a Escriba un valor en el cuadro de texto **Esta reserva reservada** para especificar la cantidad de almacenamiento que se asignará a la reserva.

b Escriba un valor en el cuadro de texto **Prioridad** para especificar el valor de prioridad de la ruta de almacenamiento relativo a otras rutas de almacenamiento que pertenecen a la reserva.

La prioridad se usa cuando hay varias rutas de almacenamiento. Una ruta de almacenamiento con prioridad 0 se usa antes que una con prioridad 1.

- c Haga clic en la opción **Deshabilitar** si no desea habilitar la ruta de almacenamiento para que la use esta reserva.
- d Repita este paso para configurar los clústeres y los almacenes de datos si es necesario.

7 Haga clic en la pestaña **Red**.

8 Configure un nombre de red para las máquinas aprovisionadas mediante la reserva.

- a (opcional) Si la opción está disponible, seleccione un endpoint de almacenamiento en el menú desplegable **Endpoint**.

La opción FlexClone estará disponible en la columna de endpoint si hay un endpoint de NetApp ONTAP y si el host es virtual. Si hay un endpoint de NetApp ONTAP, la página de reservas mostrará el endpoint asignado a la ruta de almacenamiento. Cuando se añade, actualiza o elimina un endpoint de una ruta de almacenamiento, el cambio se puede ver en todas las reservas relevantes.

Cuando se añade, actualiza o elimina un endpoint de una ruta de almacenamiento, el cambio se puede ver en la página de reservas.

- b Seleccione un nombre de red para las máquinas aprovisionadas mediante esta reserva en la lista **Nombres de red**.
- c (opcional) Seleccione un perfil de red de la lista en el menú desplegable **Perfil de red**.

Esta opción requiere que existan uno o más perfiles de red.

Puede seleccionar más de un nombre de red en una reserva, pero solo se usará una red al aprovisionar máquinas.

Resultados

Puede guardar la reserva al hacer clic en **Guardar**. O bien, puede añadir propiedades personalizadas para controlar aún más las especificaciones de reserva. También puede configurar alertas de correo electrónico para enviar notificaciones cuando disminuyan los recursos asignados a esa reserva.

Especificar propiedades personalizadas y alertas de reservas de vCloud Director

Se pueden asociar propiedades personalizadas a una reserva de vRealize Automation. También se pueden configurar alertas para enviar notificaciones de correo electrónico cuando el nivel de recursos de las reservas sea bajo.

Las alertas de correo electrónico y las propiedades personalizadas son configuraciones opcionales de la reserva. Si no desea asociar propiedades personalizadas ni establecer alertas, haga clic en **Guardar** para finalizar la creación de la reserva.

Puede añadir tantas propiedades personalizadas como sea necesario.

Si se configuran alertas, estas se generan diariamente, en vez de cuando se alcanzan los umbrales especificados.

Importante Las notificaciones solo se envían si se han configurado las alertas de correo electrónico y se han habilitado las notificaciones.

Las alertas no están disponibles para las reservas de pago por uso que se crean sin límites específicos.

Requisitos previos

[Especificar los recursos y valores de configuración de red de una reserva de vCloud Director.](#)

Procedimiento

- 1 Haga clic en la pestaña **Propiedades**.
- 2 Haga clic en **Nuevo**.
- 3 Escriba un nombre de propiedad personalizada válido.
- 4 Si corresponde, introduzca un valor de propiedad.
- 5 (opcional) Active la casilla de verificación **Cifrado** para cifrar el valor de propiedad.
- 6 (opcional) Active la casilla de verificación **Preguntar al usuario** para que sea obligatorio que el usuario introduzca un valor.

Esta opción no puede reemplazarse durante el aprovisionamiento.

- 7 Haga clic en **Guardar**.
- 8 (opcional) Añada cualquier propiedad personalizada adicional.
- 9 Haga clic en la pestaña **Alertas**.
- 10 Active la casilla de verificación **Alertas de capacidad** para configurar las alertas que se enviarán.
- 11 Use el control deslizante para establecer los umbrales de la asignación de recursos disponibles.
- 12 Introduzca los nombres de usuario o grupo de AD (no las direcciones de correo electrónico) para recibir notificaciones de alerta en el cuadro de texto **Destinatarios**.
Introduzca un nombre en cada línea. Pulse Entrar para separar varias entradas.
- 13 Seleccione **Enviar alertas al administrador del grupo** para incluir a los administradores de los grupos en las alertas de correo electrónico.
Las alertas de correo electrónico se envían a los usuarios que estén incluidos en la lista **Enviar correos electrónicos del administrador a** del grupo empresarial.
- 14 Especifique la frecuencia de recordatorio (días).
- 15 Haga clic en **Guardar**.

Resultados

La reserva se ha guardado y aparece en la lista Reservas.

Crear una reserva de Microsoft Azure

Cree una reserva de Azure para un grupo empresarial específico a fin de otorgar a los usuarios de ese grupo la capacidad de solicitar máquinas virtuales de Azure en un recurso informático específico.

Si la implementación admite Single Sign-On a través de un túnel VPN, puede configurar compatibilidad de esta funcionalidad en máquinas virtuales de Azure mediante las opciones de la pestaña **Propiedades**.

Nota Ignore la pestaña **Alertas** al crear una reserva de Azure, ya que no es relevante. Tras crear una reserva, no podrá cambiar las asociaciones de los grupos empresariales. Además, a diferencia de otros tipos de máquinas, no existe ningún vínculo directo entre una reserva de Azure y un blueprint.

Puede controlar la visualización de las reservas al añadir, editar o eliminar mediante la opción **Filtrar por categoría** de la página **Reservas**. Tenga en cuenta que las reservas del agente de prueba no aparecen en la lista de reservas al filtrar por categoría.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Compruebe que un administrador de tenants haya creado al menos un grupo empresarial.
- (opcional) Configure la información del perfil de red.
- Compruebe que tenga acceso a cualquiera de los recursos de Azure requeridos.
- Confirme que existen los pares de claves necesarios. Consulte *Configuración de vRealize Automation* para obtener información acerca de pares de claves.
- Obtenga un identificador de suscripción de Azure válido que coincida con el que se usa con el endpoint de Azure correspondiente. Si utiliza varias suscripciones a Azure, debe crear una reserva para cada suscripción.
- Si la implementación admite Single Sign-On a través de un túnel VPN, debe configurar la conectividad VPC adecuada antes de crear una reserva. Consulte [Configurar la conectividad VPC de red a Azure](#).

Configurar la información de reservas básica de Microsoft Azure

Especifique la información básica de una reserva de Microsoft Azure.

Toda la información de la página **Información de reserva** es obligatoria, salvo la política de reserva. Toda la información en las páginas de reserva de Azure subsiguientes es opcional.

Procedimiento

- 1 Seleccione **Infraestructura > Administración > Reservas**.
- 2 Haga clic en el icono **Nuevo** (+) y seleccione el tipo de reserva que desea crear.
 Seleccione **Azure**.

- 3 (opcional) Seleccione una reserva existente en el menú desplegable **Copiar de reserva existente**.
Aparecerán los datos de la reserva seleccionada. Puede efectuar los cambios necesarios para la nueva reserva.
- 4 Escriba un nombre en el cuadro de texto **Nombre**.
- 5 Seleccione un grupo empresarial en el menú desplegable **Grupo empresarial**.
Solo los usuarios de este grupo empresarial podrán aprovisionar máquinas mediante esta reserva.
- 6 Omita el cuadro de texto **Política de reserva**, puesto que no se aplica a las reservas de Azure.
- 7 Escriba un número en el cuadro de texto **Prioridad** para establecer la prioridad de la reserva.
La prioridad se utiliza cuando un grupo empresarial tiene más de una reserva. Una reserva con prioridad 1 se utiliza para el aprovisionamiento antes que una con prioridad 2.
- 8 (opcional) Anule la selección de la casilla de verificación **Habilitar esta reserva** si no desea activar la reserva.
- 9 Haga clic en **Aceptar**.

Configurar la información de recursos de reserva de Azure

Al configurar una reserva de Azure, puede asignar información de la cuenta de almacenamiento y del grupo de recursos en función de la instancia de Azure que esté usando. Cuando configura una reserva, la lógica de aprovisionamiento de vRealize Automation intenta asignar recursos, como grupos de recursos y cuentas de almacenamiento, de acuerdo con la información de recursos especificada por la reserva al aprovisionar una máquina virtual.

Puede configurar la información del grupo de recursos y de la cuenta de almacenamiento para una máquina virtual de Azure en la reserva, pero también puede dejar vacíos estos campos en la reserva. Si deja los campos vacíos, la información predeterminada del grupo de recursos y de la cuenta de almacenamiento relativa al identificador de suscripción de Azure especificado se utilizará para todos los blueprints relacionados. También puede actualizar esta información al crear un blueprint o al aprovisionar una máquina virtual.

Requisitos previos

Obtenga el identificador de suscripción de la instancia de Azure.

Procedimiento

- 1 Escriba o pegue el identificador de suscripción de Azure en el cuadro de texto **Identificador de suscripción**.
- 2 Seleccione la ubicación de la reserva haciendo clic en el menú desplegable **Ubicación**.
Puede dejar este campo vacío para crear una reserva válida para distintas ubicaciones, en cuyo caso la información de ubicación debe especificarse al crear un blueprint o al aprovisionar una máquina virtual de Azure.

3 Haga clic en **Nuevo** en la tabla Grupos de recursos.

- a Pegue la información adecuada del nombre del grupo de recursos de la instancia de Azure en el cuadro de texto **Nombre**.

Nota El cuadro **Nombre** no puede dejarse vacío.

- b Asigne un valor de prioridad numérico en el cuadro de texto **Prioridad**.

Esta asignación determina la prioridad cuando un grupo de recursos tiene más de un grupo de recursos (los números más pequeños indican mayor prioridad).

- c Haga clic en **Guardar** para añadir el grupo de recursos a la reserva.

4 Haga clic en **Nuevo** en la tabla Cuentas de almacenamiento.

- a Pegue la información adecuada del nombre de la cuenta de almacenamiento de la instancia de Azure en el cuadro de texto **Nombre**.

Nota El cuadro **Nombre** no puede dejarse vacío.

- b Asigne un valor de prioridad numérico en el cuadro de texto **Prioridad**.

- c Haga clic en **Guardar** para añadir la cuenta de almacenamiento a la reserva.

Esta asignación determina la prioridad cuando una reserva tiene más de una cuenta de almacenamiento (los números más pequeños indican mayor prioridad).

5 Haga clic en **Aceptar** para pasar a la pestaña siguiente.

Configurar propiedades de Azure

Puede añadir propiedades personalizadas a una reserva de Azure para dar cabida a opciones como los túneles VPN para, así, posibilitar la comunicación entre varias redes. Esta funcionalidad también permite añadir componentes de software a los blueprints.

Debe crear propiedades personalizadas que definan las URL adecuadas para admitir túneles VPN en la red. Además, debe crear propiedades que definan la ruta de acceso a los scripts de configuración de túneles de Azure que descargó previamente.

Utilice la dirección IP privada de la máquina física de túnel de Azure y el puerto 1443, que asignó a *vRealize_automation_appliance_fqdn* al invocar el túnel SSH.

En las siguientes tablas se recogen los nombres y valores de las propiedades necesarias para admitir túneles VPN.

Nombre	Valor
Azure.Windows.ScriptPath	Especifica la ruta de acceso al script descargado que configura los túneles de los sistemas basados en Windows. Actualice la ruta de acceso según corresponda a su implementación.
Azure.Linux.ScriptPath	Especifica la ruta de acceso al script descargado que configura los túneles de los sistemas basados en Linux. Actualice la ruta de acceso según corresponda a su implementación.

Nombre	Valor
agent.download.url	Especifica la dirección URL del agente VPN en la implementación. El formato de la URL es <code>https://Private_IP:1443/software-service/resources/noble-agent.jar</code> .
software.agent.service.url	Introduzca la URL del servicio de agente de software VPN de su implementación. El formato de la URL es <code>https://Private_IP:1443/software-service/api</code> .
software.ebs.url	Introduzca la URL del servicio de agente de eventos de su implementación. El formato de la URL es <code>https://Private_IP:1443/event-broker-service/api</code> .

Requisitos previos

- Descargue los scripts de Azure suministrados por VMware de la página de **instaladores del agente invitado y del agente de software** en el dispositivo de vRealize Automation.
Con estos scripts se instalan las extensiones de Azure necesarias para admitir túneles VPN. Hay dos scripts: `script.ps1` y `script.sh`. El archivo `.ps1` es para los sistemas Windows y el archivo `.sh`, para los sistemas Linux.
 - a Ejecute `https://vrealize-automation-appliance-fqdn/software` para abrir la página del dispositivo de VMware vRealize Automation.
 - b Haga clic en el vínculo **Agentes de software e invitado** que verá en la sección para instalar componentes de vRealize Automation (agentes IaaS, de software e invitado).
 - c Descargue los archivos de script de Azure de la sección de máquinas de Azure. Guarde los archivos de script en la ubicación que corresponda. Cuando configure las propiedades personalizadas de reserva de Azure, deberá remitir a esta ubicación.

Procedimiento

- 1 Haga clic en la pestaña **Propiedades**.
- 2 Haga clic en **Nuevo**.
- 3 Introduzca el nombre y el valor correspondiente de la propiedad personalizada en el cuadro de diálogo Propiedades.
- 4 A medida que vaya creando cada propiedad, haga clic en **Aceptar** en el cuadro de diálogo para añadir dicha propiedad.
- 5 Cuando termine de añadir todas las propiedades necesarias, haga clic en **Aceptar** para guardar la configuración.

Pasos siguientes

Después de crear las propiedades personalizadas para admitir túneles VPN, puede crear componentes de software para los blueprints de Azure. Consulte *Configuración de vRealize Automation* para obtener más información.

Cuando configure un componente de software de Azure, seleccione **Máquina virtual de Azure** en el menú desplegable Contenedor de la página Nuevo software.

Configurar la información de red de reserva de Azure

Puede configurar la información de la red virtual y del equilibrador de carga para una máquina virtual de Azure en la reserva.

También puede dejar esta página parcialmente o completamente vacía, y configurar la información de la red virtual y del equilibrador de carga cuando aprovisiona una máquina virtual.

Si especifica un perfil de red, pero no una subred, el nombre del primer rango de red existente del perfil de red especificado se utilizará como nombre de subred. Si se especifica un perfil de red, puede dejar vacío el cuadro de texto vNet. En este caso, el nombre del primer rango de red del perfil de red especificado se usará como nombre de subred y el nombre de la vNet se resolverá en la primera vNet de Azure que contenga una subred adecuada.

Requisitos previos

Cuando corresponda, obtenga la información adecuada para la red virtual y el equilibrador de carga desde la instancia de Azure.

Procedimiento

1 Haga clic en **Nueva** en la tabla Redes para configurar la red virtual de Azure apropiada para usarla con la máquina virtual.

a Pegue la información adecuada del nombre de la vNet de la instancia de Azure en el cuadro de texto **vNet**.

b Pegue la información adecuada del nombre de la subred de la instancia de Azure en el cuadro de texto **Subred**.

No es obligatorio que especifique la subred. Si deja este cuadro vacío, se utilizará la subred de la vNet especificada de forma predeterminada.

c Escriba o pegue el nombre apropiado en el cuadro de texto **Perfil de red**. Puede utilizar el perfil de red del blueprint para asociar una tarjeta de interfaz de red a una red.

No es obligatorio que especifique el perfil de red. Utilícelo si desea crear un blueprint en función del perfil de red definido en vRealize Automation, en lugar de combinarlo con construcciones de red de Azure.

d Asigne un valor de prioridad numérico en el cuadro de texto **Prioridad**, si corresponde.

Esta asignación determina la prioridad cuando una red virtual tiene más de una reserva (los números más pequeños indican mayor prioridad).

e Haga clic en **Guardar** para añadir el grupo de recursos a la reserva.

- 2 Haga clic en **Nuevo** en la tabla Equilibradores de carga si está implementando varias máquinas y emplea un equilibrador de carga.
 - a Pegue el nombre adecuado del equilibrador de carga de la instancia de Azure en el cuadro de texto **Nombre**.
 - b Pegue el nombre apropiado de la instancia de Azure en el cuadro de texto **Grupo de direcciones de back-end**.
 - c Asigne un valor de prioridad numérico en el cuadro de texto **Prioridad**, si corresponde.
Esta asignación determina la prioridad cuando una red virtual tiene más de un equilibrador de carga (los números más pequeños indican mayor prioridad).
 - d Haga clic en **Guardar** para añadir el equilibrador de carga a la reserva.
- 3 Haga clic en **Nuevo** en la tabla Grupos de seguridad si está implementando varias máquinas que deben comunicarse a través de un firewall.
 - a Pegue el nombre del grupo de seguridad de la instancia de Azure en el cuadro de texto **Nombre**.
 - b Asigne un valor de prioridad numérico en el cuadro de texto **Prioridad**, si corresponde.
Esta asignación determina la prioridad cuando una red virtual tiene más de un grupo de seguridad (los números más pequeños indican mayor prioridad).
 - c Haga clic en **Guardar** para añadir el grupo de seguridad a la reserva.
- 4 Haga clic en **Aceptar**.

Escenario: Crear una reserva de Amazon para un entorno de prueba de concepto

Como ha usado un túnel SSH para establecer de forma temporal la conectividad entre la red y el VPC de Amazon en el entorno de prueba de concepto, debe añadir propiedades personalizadas a las reservas de Amazon para asegurarse de que el agente de arranque de Software y el agente invitado ejecuten las comunicaciones a través del túnel.

La conectividad entre la red y el VPC de Amazon solamente es necesaria si desea usar el agente invitado para personalizar máquinas aprovisionadas, o bien si desea incluir componentes de Software en sus blueprints. En un entorno de producción, se configurará esta conectividad de forma oficial a través de Amazon Web Services, pero, como está trabajando en un entorno de prueba de concepto, ha configurado en su lugar un túnel SSH temporal.

Haciendo uso de sus privilegios de administrador de tejido, cree una reserva para asignar sus recursos de Amazon Web Services e incluya varias propiedades personalizadas para ofrecer compatibilidad con los túneles SSH. Además, debe configurar la reserva en la misma región y el mismo VPC que la máquina de túnel.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.

- Configure un túnel SSH para establecer la conectividad entre la red y el VPC de Amazon. Anote la subred, el grupo de seguridad y la dirección IP privada de la máquina de túnel de Amazon AWS. Consulte [Configurar la conectividad de red a VPC de Amazon para un entorno de prueba de concepto](#).
- Cree un grupo empresarial para los miembros de su organización de T.I. que necesiten blueprints de arquitecto en su entorno de prueba de concepto. Consulte [Crear un grupo empresarial](#).
- Compruebe que un administrador de tenants haya creado al menos un grupo empresarial.

Procedimiento

1 [Escenario: Especificar la información de reserva de Amazon AWS para un entorno de prueba de concepto](#)

Necesitará reservar recursos para su equipo de arquitectos de blueprint para que puedan probar la funcionalidad en el entorno de prueba de concepto, de modo que configura esta reserva para asignar recursos a su grupo empresarial de arquitectos.

2 [Escenario: Especificar la configuración de red de Amazon AWS para un entorno de prueba de concepto](#)

Se configura la reserva para que use la misma configuración de región y red que la máquina de túnel y se restringe el número de máquinas que se pueden encender para esta reserva, con el fin de gestionar el uso de los recursos.

3 [Escenario: Especificar las propiedades personalizadas para ejecutar las comunicaciones de agente a través de su túnel](#)

Al configurar la conectividad de red a Amazon VPC, configuró el reenvío de puerto para permitir el acceso de la máquina de túnel de Amazon AWS a los recursos de vRealize Automation.

Escenario: Especificar la información de reserva de Amazon AWS para un entorno de prueba de concepto

Necesitará reservar recursos para su equipo de arquitectos de blueprint para que puedan probar la funcionalidad en el entorno de prueba de concepto, de modo que configura esta reserva para asignar recursos a su grupo empresarial de arquitectos.

Nota Tras crear una reserva, no podrá cambiar el grupo empresarial ni las asociaciones de recursos informáticos.

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Reservas**.
- 2 Haga clic en el icono **Nuevo** (+) y seleccione el tipo de reserva que desea crear.
 Seleccione **Amazon**.
- 3 Escriba **POC de túnel de Amazon** en el cuadro de texto **Nombre**.

- 4 Seleccione el grupo empresarial creado para sus arquitectos de blueprint del menú desplegable **Grupo empresarial**.
- 5 Escriba un **1** en el cuadro de texto **Prioridad** para establecer esta reserva con el nivel de prioridad más alto.

Resultados

Ha configurado el grupo empresarial y el nivel de prioridad de la reserva, pero todavía debe asignar recursos y configurar las propiedades personalizadas del túnel SSH.

Escenario: Especificar la configuración de red de Amazon AWS para un entorno de prueba de concepto

Se configura la reserva para que use la misma configuración de región y red que la máquina de túnel y se restringe el número de máquinas que se pueden encender para esta reserva, con el fin de gestionar el uso de los recursos.

Procedimiento

- 1 Haga clic en la pestaña **Recursos**.
- 2 Seleccione un recurso informático en el que aprovisionar máquinas en el menú desplegable **Recurso informático**.

Seleccione la región de Amazon AWS donde se encuentre la máquina de túnel.
- 3 (opcional) Escriba un número en el cuadro de texto **Cuota de máquinas** para establecer el número máximo de máquinas que se puede aprovisionar en esta reserva.

Solo las máquinas que están encendidas cuentan para la cuota. Deje el campo en blanco para que la reserva sea ilimitada.
- 4 Seleccione **Especificar par de claves** en el menú desplegable **Par de claves**.

Como se trata de un entorno de prueba de concepto, se decide compartir un solo par de claves entre todas las máquinas aprovisionadas mediante esta reserva.
- 5 Seleccione el par de claves que desee compartir con sus usuarios arquitectos en el menú desplegable **Par de claves**.
- 6 Active la casilla **Asignar a una subred de un VPC**.
- 7 Seleccione la misma subred y los mismos grupos de seguridad que esté usando la máquina de túnel.

Resultados

Ha configurado la reserva para que use la misma configuración de región y red que la máquina de túnel, pero aún debe añadir propiedades personalizadas para asegurarse de que el agente de arranque de Software y el agente invitado ejecuten las comunicaciones a través del túnel.

Escenario: Especificar las propiedades personalizadas para ejecutar las comunicaciones de agente a través de su túnel

Al configurar la conectividad de red a Amazon VPC, configuró el reenvío de puerto para permitir el acceso de la máquina de túnel de Amazon AWS a los recursos de vRealize Automation.

Debe añadir propiedades personalizadas de túnel a la reserva con objeto de configurar los agentes para que accedan a esos puertos.

Nota Si utiliza una red de sistema PAT o NAT entre la red de su organización y la red de vRealize Automation, puede usar estas propiedades para acceder a su dirección IP privada y al puerto.

Procedimiento

- 1 Haga clic en la pestaña **Propiedades**.
- 2 Haga clic en **Nuevo**.
- 3 Configurar las propiedades personalizadas del túnel.

Utilice la dirección IP privada de la máquina túnel de Amazon AWS y el puerto 1443, que asignó a `vRealize_automation_appliance_fqdn` al invocar el túnel SSH.

Opción	Valor
<code>software.ebs.url</code>	<code>https://Private_IP:1443/event-broker-service/api</code>
<code>software.agent.service.url</code>	<code>https://Private_IP:1443/software-service/api</code>
<code>agent.download.url</code>	<code>https://Private_IP:1443/software-service/resources/nobel-agent.jar</code>

- 4 Haga clic en **Guardar**.

Resultados

Creó una reserva para asignar recursos de Amazon AWS a su grupo empresarial de arquitectos. Configuró la reserva para admitir el agente invitado y el agente de arranque de Software. Sus arquitectos pueden crear blueprints que saquen provecho del agente invitado para personalizar las máquinas implementadas o incluir componentes de Software.

Crear reservas de categoría virtuales

Una reserva de tipo de categoría virtual proporciona acceso a los servicios de aprovisionamiento de una implementación de máquina virtual de un grupo empresarial de vRealize Automation concreto. Los tipos de reserva virtual disponibles son vSphere, Hyper-V, KVM, SCVMM y XenServer.

Una reserva es un recurso compartido de la memoria, CPU, redes y almacenamiento de un recurso informático asignado a un grupo empresarial de vRealize Automation concreto.

Un grupo empresarial puede tener varias reservas en uno o varios endpoints.

Para aprovisionar máquinas virtuales, un grupo empresarial debe tener al menos una reserva en un recurso informático virtual. Cada reserva corresponde únicamente a un grupo empresarial, pero un grupo empresarial puede tener varias reservas en un solo recurso informático, o varias reservas en recursos informáticos de varios tipos.

Además de definir el uso compartido de recursos de tejido asignados al grupo empresarial, una reserva puede definir también las políticas, prioridades y cuotas que determinan la colocación de las máquinas.

Para aprovisionar correctamente, la reserva debe tener suficiente espacio de almacenamiento disponible. La disponibilidad de almacenamiento de la reserva depende de:

- La cantidad de almacenamiento disponible en el almacén de datos o clúster.
- La cantidad de almacenamiento reservado para ese almacén de datos o clúster.
- La cantidad de almacenamiento que ya se ha asignado en vRealize Automation

Por ejemplo, incluso si vCenter Server tiene almacenamiento disponible para el almacén de datos o clúster, si no se reservó suficiente espacio de almacenamiento en la reserva, el aprovisionamiento genera un error "No hay reservas disponibles para asignar...". El almacenamiento asignado en una reserva depende de la cantidad de máquinas virtuales (independientemente de su estado) en esa reserva específica. Consulte el artículo de la base de conocimientos de VMware *Equipo XXX: no hay reservas disponibles para asignar dentro del grupo XXX. Se solicitó un total de XX GB de almacenamiento (2151030)* en <http://kb.vmware.com/kb/2151030> para obtener más información.

Explicación de la lógica de selección de las reservas

Cuando un miembro de un grupo empresarial crea una solicitud de aprovisionamiento para una máquina virtual, vRealize Automation selecciona una máquina de una de las reservas que están disponibles para ese grupo empresarial.

La reserva para la que se aprovisiona una máquina debe cumplir los siguientes criterios:

- La reserva debe ser del mismo tipo de plataforma que el blueprint desde el que se ha solicitado la máquina.
Un blueprint virtual genérico se puede aprovisionar en cualquier tipo de reserva virtual.
- La reserva debe estar habilitada.
- El recurso informático debe estar disponible y no debe estar en modo de mantenimiento.
- La reserva debe tener capacidad de sobra en la cuota de máquinas o tener una cuota ilimitada.

La cuota de máquinas asignada incluye solo las máquinas que están encendidas. Por ejemplo, si una reserva tiene una cuota de 50, y se han aprovisionado 40 máquinas, pero solo 20 de ellas están encendidas, la cuota de la reserva se ha asignado al 40 %, no al 80 %.

- La reserva debe tener suficiente memoria y recursos de almacenamiento no asignados para aprovisionar la máquina.

Cuando se han asignado por completo la cuota de máquinas, la memoria o el almacenamiento de una reserva virtual, no se pueden aprovisionar más máquinas virtuales desde esta. Los recursos se pueden reservar más allá de la capacidad física de un recurso informático de virtualización (con asignaciones adicionales), pero cuando se ha asignado la capacidad física de un recurso informático al 100 %, no se podrán aprovisionar más máquinas en las reservas con ese recurso informático, hasta que se recuperen los recursos.

- Si el blueprint tiene una configuración de red específica, la reserva debe tener las mismas redes.

Si el blueprint o la reserva especifican un perfil de red para la asignación de direcciones IP estáticas, debe haber una dirección IP disponible para asignarla a la nueva máquina.

- Si el blueprint o la solicitud especifican una ubicación, el recurso informático deberá asociarse a dicha ubicación.

Si el valor de la propiedad personalizada `Vrm.DataCenter.Policy` es **Exact** y no hay ninguna reserva para un recurso informático asociado a esa ubicación que satisfaga todos los demás criterios, se produce un error de aprovisionamiento.

Si el valor de `Vrm.DataCenter.Policy` es **NotExact** y no hay ninguna reserva para un recurso informático asociado a esa ubicación que satisfaga todos los demás criterios, el aprovisionamiento puede continuar en otra reserva independientemente de la ubicación. Esta es la opción predeterminada.

- Si el blueprint o la solicitud especifican la propiedad personalizada `VirtualMachine.Host.TpmEnabled`, el hardware de confianza debe instalarse en el recurso informático de la reserva.
- Si el blueprint especifica una política de reserva, la reserva debe pertenecer a la política de reserva.

Las políticas de reserva son un modo de garantizar que la reserva seleccionada cumple los requisitos de aprovisionamiento de máquinas desde un blueprint específico. Por ejemplo, puede usar políticas de reserva para restringir el aprovisionamiento de los recursos informáticos con una plantilla específica para clonación.

Si no hay reservas que cumplan todos los criterios de selección disponibles, se producirá un error de aprovisionamiento.

Si hay varias reservas que cumplen todos los criterios, la reserva desde la que se aprovisionará la máquina solicitada se determinará mediante la siguiente lógica:

- Una reserva con un valor de prioridad inferior se selecciona antes que una reserva con un valor de prioridad mayor.
- Si hay varias reservas con la misma prioridad, se seleccionará la reserva cuyo porcentaje de cuota de máquinas asignado sea menor.
- Si hay varias reservas con la misma prioridad y el mismo uso de cuota, las máquinas se distribuirán entre las reservas por turnos.

Nota Aunque no se admite la selección por turnos de perfiles de red, sí se admite la selección por turnos de redes (si las hay), que pueden asociarse a distintos perfiles de red.

Si hay varias rutas de almacenamiento disponibles en una reserva con suficiente capacidad para aprovisionar los volúmenes de máquinas, las rutas de almacenamiento se seleccionarán según la siguiente lógica:

- Si el blueprint o la solicitud especifican una política de reserva de almacenamiento, la ruta de almacenamiento debe pertenecer a la política de reserva de almacenamiento.

Si el valor de la propiedad personalizada

`VirtualMachine.DiskN.StorageReservationPolicyMode` es **NotExact** y no hay ninguna ruta de almacenamiento con suficiente capacidad en la política de reserva de almacenamiento, el aprovisionamiento puede continuar con una ruta de almacenamiento ajena a la política de reserva de almacenamiento especificada. El valor predeterminado de `VirtualMachine.DiskN.StorageReservationPolicyMode` es **Exact**.

- Una ruta de almacenamiento con un valor de prioridad inferior se selecciona antes que una ruta de almacenamiento con un valor de prioridad mayor.
- Si hay varias rutas de almacenamiento con la misma prioridad, las máquinas se distribuirán entre las rutas de almacenamiento por turnos.

Crear una reserva de vSphere para la virtualización de red y seguridad de NSX

Puede crear una reserva de vSphere para asignar redes externas y puertas de enlace enrutadas a los perfiles de red, así como para especificar una zona de transporte y asignar grupos de seguridad a componentes de máquina.

Si ha configurado NSX, puede especificar la configuración de la zona de transporte, la política de reserva de puerta de enlace enrutada y de Edge, y el aislamiento de aplicaciones de NSX cuando cree o edite un blueprint. Estas opciones de configuración están disponibles en la pestaña **Configuración de NSX** de las páginas **Blueprint** y **Propiedades de blueprint**.

La configuración del componente de red y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario ejecutar la recopilación de datos en el inventario de NSX de clústeres de vSphere. Los componentes de redes y seguridad son específicos de NSX y solo se pueden usar con componentes de máquina de vSphere. Para obtener información sobre cómo configurar NSX, consulte la *guía de administración de NSX*.

Cuando vRealize Automation aprovisiona máquinas con redes NAT o enrutadas, aprovisiona una puerta de enlace enrutada como enrutador de red. Esta puerta de enlace enrutada o Edge es una máquina de administración que consume recursos informáticos. También se encarga de administrar las comunicaciones de red de los componentes de máquina aprovisionados. La reserva empleada para aprovisionar la puerta de enlace enrutada o Edge determina la red externa que se usa en los perfiles de red NAT y enrutada. También define la puerta de enlace enrutada o Edge de reserva utilizada para configurar redes enrutadas. La puerta de enlace enrutada de reserva vincula las redes enrutadas con entradas en la tabla de enrutamiento.

Se puede especificar una política de reserva de puerta de enlace enrutada o Edge para identificar qué reservas hay que usar para aprovisionar las máquinas mediante la puerta de enlace enrutada o Edge. vRealize Automation usa de forma predeterminada las mismas reservas para los componentes de puerta de enlace enrutada y de máquina.

En la reserva se seleccionan uno o varios grupos de seguridad para implantar una política de seguridad de referencia para todas las máquinas de componentes aprovisionadas con esa reserva en vRealize Automation. Todas las máquinas aprovisionadas se añaden a estos grupos de seguridad especificados.

Para que el aprovisionamiento se realice correctamente, la zona de transporte de la reserva debe ser la misma que la de un blueprint de máquina si ese blueprint define las redes de máquina. Igualmente, para realizar el aprovisionamiento de una puerta de enlace enrutada de una máquina, la zona de transporte definida en la reserva debe ser la misma que la definida en el blueprint.

Cuando seleccione una puerta de enlace enrutada o de Edge y un perfil de red en una reserva al configurar redes enrutadas, seleccione el nombre de red que se usará para vincular las redes enrutadas y asígnele el perfil de red externa que se empleará para configurar el perfil de red enrutada. La lista de perfiles de red disponibles para asignarlos a un nombre de red se filtra para que coincida con la subred del nombre de red en función de la máscara de subred y de la dirección IP principal seleccionadas para la interfaz de red.

Si desea utilizar una puerta de enlace enrutada o de Edge en las reservas de vRealize Automation, configúrela de forma externa en el entorno de NSX, y después ejecute la recopilación de datos de inventario. Para NSX, debe poseer una instancia de NSX Edge que funcione antes de configurar la puerta de enlace predeterminada para las rutas estáticas o la información de enrutamiento dinámico para un enrutador distribuido o una puerta de enlace de servicios de Edge. Consulte la *guía de administración de NSX*.

Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer

Debe asignar recursos a máquinas; para ello, cree una reserva antes de que los miembros de un grupo empresarial puedan solicitar el aprovisionamiento de máquinas.

Cada grupo empresarial debe contar como mínimo con una reserva para que sus miembros puedan aprovisionar máquinas de ese tipo. Por ejemplo, un grupo empresarial que tiene una reserva de vSphere, pero no una reserva de KVM (RHEV), no podrá solicitar una máquina virtual de KVM (RHEV). En este ejemplo, el grupo empresarial deberá asignar una reserva para recursos de KVM (RHEV) expresamente.

Procedimiento

1 Especificar la información de reserva virtual

Cada reserva se configura para un grupo empresarial específico, de forma que sus usuarios puedan solicitar máquinas en un recurso informático determinado.

2 Especificar los recursos y valores de configuración de red de una reserva virtual

Indique los recursos y valores de configuración de red para aprovisionar máquinas desde esta reserva de vRealize Automation.

3 Especificar propiedades personalizadas y alertas de reservas virtuales

Se pueden asociar propiedades personalizadas a una reserva de vRealize Automation. También se pueden configurar alertas para enviar notificaciones de correo electrónico cuando el nivel de recursos de las reservas sea bajo.

Especificar la información de reserva virtual

Cada reserva se configura para un grupo empresarial específico, de forma que sus usuarios puedan solicitar máquinas en un recurso informático determinado.

Puede controlar la visualización de las reservas al añadir, editar o eliminar mediante la opción **Filtrar por categoría** de la página Reservas. Tenga en cuenta que las reservas del agente de prueba no aparecen en la lista de reservas al filtrar por categoría.

Nota Tras crear una reserva, no podrá cambiar el grupo empresarial ni las asociaciones de recursos informáticos.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Compruebe que un administrador de tenants haya creado al menos un grupo empresarial.
- Compruebe que existe un recurso informático.
- Configure los ajustes de red.
- (opcional) Configure la información del perfil de red.

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Reservas**.
- 2 Haga clic en el icono **Nuevo** (+) y seleccione el tipo de reserva que desea crear.
Los tipos de reserva virtual disponibles son Hyper-V, KVM, SCVMM, vSphere y XenServer.
Por ejemplo, seleccione **vSphere**.
- 3 (opcional) Seleccione una reserva existente en el menú desplegable **Copiar de reserva existente**.
Aparecerán los datos de la reserva seleccionada. Puede efectuar los cambios necesarios para la nueva reserva.
- 4 Escriba un nombre en el cuadro de texto **Nombre**.
- 5 Seleccione un tenant en el menú desplegable **Tenant**.
- 6 Seleccione un grupo empresarial en el menú desplegable **Grupo empresarial**.
Solo los usuarios de este grupo empresarial podrán aprovisionar máquinas mediante esta reserva.
- 7 (opcional) Seleccione una política de reserva del menú desplegable **Política de reserva**.
Esta opción requiere que existan una o más políticas de reserva. Puede editar la reserva más tarde para especificar una política de reserva.
Use una política de reserva para limitar el aprovisionamiento a reservas determinadas.
- 8 Escriba un número en el cuadro de texto **Prioridad** para establecer la prioridad de la reserva.
La prioridad se utiliza cuando un grupo empresarial tiene más de una reserva. Una reserva con prioridad 1 se utiliza para el aprovisionamiento antes que una con prioridad 2.

- 9 (opcional) Anule la selección de la casilla de verificación **Habilitar esta reserva** si no desea activar la reserva.

Resultados

No abandone esta página. La reserva no se ha completado.

Especificar los recursos y valores de configuración de red de una reserva virtual

Indique los recursos y valores de configuración de red para aprovisionar máquinas desde esta reserva de vRealize Automation.

Puede seleccionar un almacén de datos de FlexClone en la reserva si tiene dispositivos de almacenamiento y un entorno de vSphere que usan la tecnología Net App FlexClone. SDRS no es compatible con dispositivos de almacenamiento de FlexClone.

Para aprovisionar correctamente, la reserva debe tener suficiente espacio de almacenamiento disponible. La disponibilidad de almacenamiento de la reserva depende de:

- La cantidad de almacenamiento disponible en el almacén de datos o clúster.
- La cantidad de almacenamiento reservado para ese almacén de datos o clúster.
- La cantidad de almacenamiento que ya se ha asignado en vRealize Automation

Por ejemplo, incluso si vCenter Server tiene almacenamiento disponible para el almacén de datos o clúster, si no se reservó suficiente espacio de almacenamiento en la reserva, el aprovisionamiento genera un error "No hay reservas disponibles para asignar...". El almacenamiento asignado en una reserva depende de la cantidad de máquinas virtuales (independientemente de su estado) en esa reserva específica. Consulte el artículo de la base de conocimientos de VMware *Equipo XXX: no hay reservas disponibles para asignar dentro del grupo XXX. Se solicitó un total de XX GB de almacenamiento (2151030)* en <http://kb.vmware.com/kb/2151030> para obtener más información.

Requisitos previos

[Especificar la información de reserva virtual.](#)

Procedimiento

- 1 Haga clic en la pestaña **Recursos**.
- 2 Seleccione un recurso informático en el que aprovisionar máquinas en el menú desplegable **Recurso informático**.

Solo las plantillas que se encuentran en el clúster que ha seleccionado están disponibles para la clonación con la reserva.

Durante el aprovisionamiento, las máquinas se ubican en un host conectado al almacenamiento local. Si la reserva usa almacenamiento local, todas las máquinas que se aprovisionan mediante la reserva se crean en el host que contiene el almacenamiento local. Sin embargo, si usa la propiedad personalizada `VirtualMachine.Admin.ForceHost`, que obliga a una máquina a aprovisionarse en otro host, el aprovisionamiento no se realiza

correctamente. El aprovisionamiento tampoco se realiza correctamente si la plantilla a partir de la cual se clona la máquina se encuentra almacenada localmente, pero está conectada a una máquina de otro clúster. En tal caso, el aprovisionamiento no se realiza correctamente porque no puede acceder a la plantilla.

- 3 (opcional) Escriba un número en el cuadro de texto **Cuota de máquinas** para establecer el número máximo de máquinas que se puede aprovisionar en esta reserva.

Solo las máquinas que están encendidas cuentan para la cuota. Deje el campo en blanco para que la reserva sea ilimitada.

- 4 Especifique la cantidad de memoria en GB que se asignará a la reserva en la tabla Memoria.

El valor de memoria total de la reserva se basa en la selección de recursos informáticos.

- 5 Seleccione una o más rutas de almacenamiento de la lista.

Las opciones de ruta de almacenamiento disponibles dependen de la selección de recursos informáticos.

Para las integraciones que utilizan el almacenamiento Storage Distributed Resource Scheduler (SDRS), puede seleccionar un clúster de almacenamiento para permitir que SDRS controle la ubicación del almacenamiento y el equilibrio de carga de las máquinas aprovisionadas desde esta reserva. El modo de automatización de SDRS debe establecerse como Automático. De lo contrario, seleccione un almacén de datos del clúster para el comportamiento del almacén de datos independiente. SDRS no es compatible con dispositivos de almacenamiento de FlexClone.

Puede seleccionar discos individuales del clúster o un clúster de almacenamiento, pero no ambos. Si selecciona un clúster de almacenamiento, el SDRS controla la colocación del almacenamiento y el equilibrio de carga de las máquinas aprovisionadas desde esta reserva.

- 6 Si está disponible para el recurso informático, seleccione un grupo de recursos en el menú desplegable **Grupo de recursos**.
- 7 Haga clic en la pestaña **Red**.

8 Configure un nombre de red para las máquinas aprovisionadas mediante la reserva.

- a (opcional) Si la opción está disponible, seleccione un endpoint de almacenamiento en el menú desplegable **Endpoint**.

La opción FlexClone estará disponible en la columna de endpoint si hay un endpoint de NetApp ONTAP y si el host es virtual. Si hay un endpoint de NetApp ONTAP, la página de reservas mostrará el endpoint asignado a la ruta de almacenamiento. Cuando se añade, actualiza o elimina un endpoint de una ruta de almacenamiento, el cambio se puede ver en todas las reservas relevantes.

Cuando se añade, actualiza o elimina un endpoint de una ruta de almacenamiento, el cambio se puede ver en la página de reservas.

- b Seleccione un nombre de red para las máquinas aprovisionadas mediante esta reserva en la lista **Nombres de red**.
- c (opcional) Seleccione un perfil de red de la lista en el menú desplegable **Perfil de red**.

Esta opción requiere que existan uno o más perfiles de red.

Puede seleccionar más de un nombre de red en una reserva, pero solo se usará una red al aprovisionar máquinas.

Resultados

Puede guardar la reserva al hacer clic en **Guardar**. O bien, puede añadir propiedades personalizadas para controlar aún más las especificaciones de reserva. También puede configurar alertas de correo electrónico para enviar notificaciones cuando disminuyan los recursos asignados a esa reserva.

Especificar propiedades personalizadas y alertas de reservas virtuales

Se pueden asociar propiedades personalizadas a una reserva de vRealize Automation. También se pueden configurar alertas para enviar notificaciones de correo electrónico cuando el nivel de recursos de las reservas sea bajo.

Las alertas de correo electrónico y las propiedades personalizadas son configuraciones opcionales de la reserva. Si no desea asociar propiedades personalizadas ni establecer alertas, haga clic en **Guardar** para finalizar la creación de la reserva.

Puede añadir tantas propiedades personalizadas como sea necesario.

Importante Las notificaciones solo se envían si se han configurado las alertas de correo electrónico y se han habilitado las notificaciones.

Si se configuran alertas, estas se generan diariamente, en vez de cuando se alcanzan los umbrales especificados.

Requisitos previos

[Especificar los recursos y valores de configuración de red de una reserva virtual.](#)

Procedimiento

- 1 Haga clic en la pestaña **Propiedades**.
- 2 Haga clic en **Nuevo**.
- 3 Escriba un nombre de propiedad personalizada válido.
- 4 Si corresponde, introduzca un valor de propiedad.
- 5 (opcional) Active la casilla de verificación **Cifrado** para cifrar el valor de propiedad.
- 6 (opcional) Active la casilla de verificación **Preguntar al usuario** para que sea obligatorio que el usuario introduzca un valor.

Esta opción no puede reemplazarse durante el aprovisionamiento.

- 7 (opcional) Añada cualquier propiedad personalizada adicional.
- 8 Haga clic en la pestaña **Alertas**.
- 9 Active la casilla de verificación **Alertas de capacidad** para configurar las alertas que se enviarán.
- 10 Use el control deslizante para establecer los umbrales de la asignación de recursos disponibles.
- 11 Introduzca los nombres de usuario o grupo de AD (no las direcciones de correo electrónico) para recibir notificaciones de alerta en el cuadro de texto **Destinatarios**.
Introduzca un nombre en cada línea. Pulse Entrar para separar varias entradas.
- 12 Seleccione **Enviar alertas al administrador del grupo** para incluir a los administradores de los grupos en las alertas de correo electrónico.
Las alertas de correo electrónico se envían a los usuarios que estén incluidos en la lista **Enviar correos electrónicos del administrador a** del grupo empresarial.
- 13 Especifique la frecuencia de recordatorio (días).
- 14 Haga clic en **Guardar**.

Resultados

La reserva se ha guardado y aparece en la lista Reservas.

Pasos siguientes

Puede configurar políticas de reserva opcionales o empezar a preparar el aprovisionamiento.

Los usuarios con autorización para crear blueprints pueden crearlos ahora.

Editar una reserva para asignarle un perfil de red

Puede asignar un perfil de red a una reserva, por ejemplo, para habilitar la asignación de direcciones IP estáticas en las máquinas aprovisionadas en dicha reserva.

También puede asignar un perfil de red a un blueprint mediante la propiedad personalizada `VirtualMachine.NetworkN.ProfileName` en la pestaña **Propiedades** de la página **Nuevo blueprint** o **Propiedades de blueprint**.

Si especifica un perfil de red en una reserva y un blueprint, el valor del blueprint tiene prioridad. Por ejemplo, si especifica un perfil de red en el blueprint (mediante la propiedad personalizada `VirtualMachine.NetworkN.ProfileName`) y en una reserva utilizada por el blueprint, el perfil de red especificado en el blueprint tendrá prioridad. Sin embargo, si la propiedad personalizada no se utiliza en el blueprint, y selecciona un perfil de red para un NIC de máquina, vRealize Automation usa la ruta de red de reserva para el NIC de máquina cuyo perfil de red se haya especificado.

Nota Esta información no se aplica a Amazon Web Services.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Cree un perfil de red. Consulte [Crear un perfil de red](#).

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Reservas**.
- 2 Señale una reserva y haga clic en **Editar**.
- 3 Haga clic en la pestaña **Red**.
- 4 Asigne un perfil de red a un nombre de red.
 - a Seleccione un nombre de red en el que desea habilitar direcciones IP estáticas.
Los nombres de red se derivan de la configuración de la pestaña **Recursos**.
 - b Para asignar un perfil de red disponible a la ruta, seleccione un perfil en el menú desplegable **Perfil de red**.
 - c (opcional) Repita este paso para asignar perfiles de red a nombres de red adicionales en esta reserva.
- 5 Haga clic en **Aceptar**.

Políticas de reserva

Puede usar una política de reserva para controlar el modo en que se procesan las solicitudes de reserva. Cuando se aprovisionan máquinas desde el blueprint, el aprovisionamiento se limita a los recursos especificados en la política de reserva.

Las políticas de reserva son un medio opcional para controlar la forma en que se procesan las solicitudes de reserva. Puede aplicar una política de reserva a un blueprint para restringir las máquinas aprovisionadas de ese blueprint en un subconjunto de reservas disponibles.

La política de reserva se usa para recopilar recursos en grupos para varios niveles de servicio, o para hacer que se pueda acceder fácilmente a un tipo específico de recurso para un propósito particular. Cuando un usuario solicita una máquina, se puede aprovisionar en cualquier reserva del tipo apropiado que tenga la capacidad suficiente para la máquina. Los siguientes escenarios proporcionan unos pocos ejemplos de usos posibles de las políticas de reserva:

- Para asegurar que las máquinas aprovisionadas se colocan en reservas con dispositivos específicos compatibles con NetApp FlexClone.
- Para restringir el aprovisionamiento de máquinas de nube a una región específica que contenga una imagen de máquina requerida para un blueprint específico.
- Como un método adicional para usar el modelo de asignación de pago por uso para tipos de máquina compatibles con dicha función.

Puede añadir varias reservas a una política de reserva, pero una reserva puede pertenecer solo a una política. Puede asignar una política de reserva única a más de un blueprint. Un blueprint solo puede tener una política de reserva.

Nota Las reservas definidas para los endpoints de vCloud Air y los endpoints de vCloud Director no admiten el uso de perfiles de red para aprovisionar máquinas.

Nota Si tiene SDRS habilitado en su plataforma, puede permitir que SDRS realice el equilibrio de carga del almacenamiento para los discos de máquinas virtuales individuales o todo el almacenamiento de la máquina virtual. Si trabaja con clústeres de almacenes de datos SDRS, se pueden producir conflictos al usar políticas de reserva y políticas de reserva de almacenamiento. Por ejemplo, si se selecciona un almacén de datos independiente o un almacén de datos de un clúster de SDRS en una de las reservas de una política o una política de almacenamiento, su almacenamiento de máquina virtual podría congelarse en vez de basarse en SDRS. Si solicita el reaprovisionamiento para una máquina con ubicación del almacenamiento en un clúster de SDRS, la máquina se elimina si el nivel de automatización de SDRS está desactivado. Para obtener información relacionada con el aprovisionamiento y SDRS, consulte la propiedad personalizada `VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec`.

Configurar una política de reserva

Se pueden crear políticas de reserva para recopilar recursos en grupos para varios niveles de servicio, o para lograr que se pueda acceder fácilmente a un tipo específico de recurso para un propósito particular. Tras crear la política de reserva, hay que rellenarla con reservas para que los administradores de tenants y administradores de grupos empresariales puedan usarla de manera eficaz en un blueprint.

Una política de reserva puede incluir reservas de varios tipos, pero solo se tienen en cuenta las reservas que coinciden con el tipo de blueprint al seleccionar una reserva para una solicitud particular.

Procedimiento

1 Crear una política de reserva

Se pueden usar políticas de reserva para agrupar reservas similares.

2 Asignar una política de reserva a una reserva

Cuando se crea una reserva, se le puede asignar una política de reserva. También puede editar una reserva existente y asignarle una política de reserva o cambiar su asignación de política de reserva.

Crear una política de reserva

Se pueden usar políticas de reserva para agrupar reservas similares.

Cree primero la política de reserva y, luego, añádala a reservas para que un creador de blueprint pueda usarla en un blueprint.

La política se crea como un contenedor vacío.

Puede controlar la visualización de las políticas de reserva al añadir, editar o eliminar mediante la opción **Filtrar por tipo** de la página Políticas de reserva.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tejido**.

Procedimiento

1 Seleccione **Infraestructura > Reservas > Políticas de reserva**.

2 Haga clic en **Agregar**.

3 Escriba un nombre en el cuadro de texto **Nombre**.

4 Seleccione **Política de reserva** en el menú desplegable **Tipo**.

5 Escriba una descripción en el cuadro de texto **Descripción**.

6 Haga clic en **Actualizar** para guardar la política.

Asignar una política de reserva a una reserva

Cuando se crea una reserva, se le puede asignar una política de reserva. También puede editar una reserva existente y asignarle una política de reserva o cambiar su asignación de política de reserva.

Requisitos previos

[Crear una política de reserva](#).

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Reservas**.
- 2 Señale una reserva y haga clic en **Editar**.
- 3 Seleccione una política de reserva del menú desplegable **Política de reserva**.
- 4 Haga clic en **Guardar**.

Políticas de reserva de almacenamiento

Puede crear políticas de reserva de almacenamiento para permitir que los arquitectos de blueprints asignen los volúmenes de una máquina virtual a varios almacenes de datos a los tipos de plataforma de vSphere, KVM (RHEV), y SCVMM o a varios perfiles de almacenamiento de otros recursos, como recursos de vCloud Air o vCloud Director.

Asignar los volúmenes de una máquina virtual a varios almacenes de datos o a varios perfiles de almacenamiento permite que los arquitectos de blueprints controlen y usen el espacio de almacenamiento con más eficiencia. Por ejemplo, podrían implementar el volumen de sistema operativo en un almacén de datos, o un perfil de almacenamiento, más lento y menos costoso, y el volumen de base de datos en un almacén o perfil de datos más rápido.

Algunos endpoints de máquinas solo admiten un único perfil de almacenamiento, mientras que otros admiten el almacenamiento en disco multinivel. El almacenamiento en disco multinivel está disponible para endpoints de vCloud Director 5.6 y versiones posteriores, además de para endpoints de vCloud Air. No se admite el almacenamiento en disco multinivel para los endpoints de vCloud Director 5.5.

Cuando se crea un blueprint, se puede asignar un solo almacén de datos o una política de reserva de almacenamiento que represente varios almacenes de datos en un volumen. Cuando se asigna un solo almacén de datos, o un perfil de almacenamiento, a un volumen, vRealize Automation utiliza dicho almacén o perfil de datos durante el período de aprovisionamiento, si es posible. Cuando se asigna una directiva de reserva de almacenamiento a un volumen, vRealize Automation usa uno de sus almacenes de datos, o perfiles de almacenamiento si se trabaja con otros recursos, como vCloud Air o vCloud Director durante el período de aprovisionamiento.

Una política de reserva de almacenamiento es, básicamente, una etiqueta que el administrador de tejido aplica a uno o más almacenes de datos o perfiles de almacenamiento para agrupar los almacenes de datos o perfiles de almacenamiento con características similares, como la velocidad o el precio. Un almacén de datos o perfil de almacenamiento solo se puede asignar a una única política de reserva de almacenamiento, pero una política de reserva de almacenamiento puede tener muchos almacenes de datos o perfiles de almacenamiento distintos.

Puede crear una política de reserva de almacenamiento y asignarla a uno o varios almacenes de datos o perfiles de almacenamiento. A continuación, el creador de un blueprint podrá asignar la política de reserva de almacenamiento a un volumen en un blueprint virtual. Cuando un usuario solicite una máquina que utilice el blueprint, vRealize Automation usará la política de reserva de almacenamiento especificada en el blueprint para seleccionar el almacén de datos o el perfil de almacenamiento para el volumen de la máquina.

Nota Si tiene SDRS habilitado en su plataforma, puede permitir que SDRS realice el equilibrio de carga del almacenamiento para los discos de máquinas virtuales individuales o todo el almacenamiento de la máquina virtual. Si trabaja con clústeres de almacenes de datos SDRS, se pueden producir conflictos al usar políticas de reserva y políticas de reserva de almacenamiento. Por ejemplo, si se selecciona un almacén de datos independiente o un almacén de datos de un clúster de SDRS en una de las reservas de una política o una política de almacenamiento, su almacenamiento de máquina virtual podría congelarse en vez de basarse en SDRS. Si solicita el reaprovisionamiento para una máquina con ubicación del almacenamiento en un clúster de SDRS, la máquina se elimina si el nivel de automatización de SDRS está desactivado. Para obtener información relacionada con el aprovisionamiento y SDRS, consulte la propiedad personalizada `VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec`.

El almacenamiento y la memoria que se asignan a una máquina aprovisionada por una reserva se liberan cuando se elimina en vRealize Automation la máquina a la que están asignados, mediante la acción Destruir. El almacenamiento y la memoria no se liberan si la máquina se elimina en vCenter Server.

Por ejemplo, no puede eliminar una reserva que esté asociada con máquinas en una implementación existente. Si mueve o elimina de forma manual máquinas implementadas en vCenter Server, vRealize Automation las sigue reconociendo como activas y le impide eliminar las reservas asociadas.

Configurar una política de reserva de almacenamiento

Se pueden crear políticas de reserva de almacenamiento para agrupar los almacenes de datos con características parecidas, como la velocidad o el precio. Tras crear la política de reserva de almacenamiento, hay que rellenarla con almacenes de datos para que se pueda usar en un blueprint.

Procedimiento

1 Crear una política de reserva de almacenamiento

Una política de reserva de almacenamiento se puede usar para agrupar almacenes de datos con características parecidas, como la velocidad o el precio.

2 Asignar una política de reserva de almacenamiento a un almacén de datos

Es posible asociar una política de reserva de almacenamiento a un recurso informático. Después de crear la política de reserva de almacenamiento, rellénela con almacenes de datos. Un almacén de datos puede pertenecer a una política de reserva de almacenamiento única y exclusivamente. Añada varios almacenes de datos para crear un grupo de almacenes de datos para usarlo con un blueprint.

Crear una política de reserva de almacenamiento

Una política de reserva de almacenamiento se puede usar para agrupar almacenes de datos con características parecidas, como la velocidad o el precio.

La política se crea como un contenedor vacío.

Puede controlar la visualización de las políticas de reserva al añadir, editar o eliminar mediante la opción **Filtrar por tipo** de la página Políticas de reserva.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tejido**.

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Políticas de reserva**.
- 2 Haga clic en **Agregar**.
- 3 Escriba un nombre en el cuadro de texto **Nombre**.
- 4 Seleccione la **Política de reserva de almacenamiento** en el menú desplegable **Tipo**.
- 5 Escriba una descripción en el cuadro de texto **Descripción**.
- 6 Haga clic en **Actualizar** para guardar la política.


Asignar una política de reserva de almacenamiento a un almacén de datos

Es posible asociar una política de reserva de almacenamiento a un recurso informático. Después de crear la política de reserva de almacenamiento, rellénela con almacenes de datos. Un almacén de datos puede pertenecer a una política de reserva de almacenamiento única y exclusivamente. Añada varios almacenes de datos para crear un grupo de almacenes de datos para usarlo con un blueprint.

Requisitos previos

[Crear una política de reserva de almacenamiento](#).

Procedimiento

- 1 Seleccione **Infraestructura > Recursos informáticos > Recursos informáticos**.
- 2 Vaya a un recurso informático y haga clic en **Editar**.
- 3 Haga clic en la pestaña **Configuración**.
- 4 Busque en la tabla Almacenamiento el almacén de datos que quiera añadir a la política de reserva de almacenamiento.
- 5 Haga clic en el icono **Editar** () junto al objeto de **Ruta de almacenamiento** que desee.
- 6 Seleccione una política de reserva de almacenamiento del menú desplegable **Política de reserva de almacenamiento**.

Tras aprovisionar una máquina, no podrá cambiar su política de reserva de almacenamiento si al hacerlo cambiase el perfil de almacenamiento de un disco.

- 7 Haga clic en el icono **Guardar** (✓).
- 8 Haga clic en **Aceptar**.
- 9 (opcional) Asigne más almacenes de datos a la política de reserva de almacenamiento.

Colocación de cargas de trabajo

Cuando se implementa un blueprint, la colocación de cargas de trabajo utiliza los datos recopilados para recomendar la ubicación donde se puede implementar el blueprint según los recursos disponibles. vRealize Automation y vRealize Operations Manager trabajan juntos para proporcionar recomendaciones de colocación de cargas de trabajo en la implementación de nuevos blueprints.

Mientras vRealize Automation administra las políticas organizativas, como los grupos empresariales, las reservas y las cuotas, se integra con los análisis de capacidad de vRealize Operations Manager para colocar las máquinas. La colocación de cargas de trabajo solo se encuentra disponible para endpoints de vSphere.

Términos utilizados en la colocación de cargas de trabajo

Se utilizan varios términos con la colocación de cargas de trabajo.

- Los clústeres en vSphere se asignan a los recursos informáticos en vRealize Automation.
- Las reservas contienen recursos informáticos y almacenamiento, donde el almacenamiento puede constar de almacenes de datos individuales o clústeres de almacenes de datos. Una reserva puede incluir varios almacenes de datos, clústeres de almacenes de datos o ambos.
- Varias reservas pueden hacer referencia a un mismo clúster.
- Es posible mover las máquinas virtuales a varios clústeres.
- Cuando se habilita la colocación de cargas de trabajo, el flujo de trabajo de aprovisionamiento utiliza la política de colocación para recomendar la ubicación donde se puede implementar el blueprint.

Aprovisionar blueprints con la colocación de cargas de trabajo

Cuando se utiliza la colocación de cargas de trabajo para aprovisionar los blueprints, el flujo de trabajo de aprovisionamiento utiliza las reservas de vRealize Automation y la optimización de colocación de vRealize Operations Manager.

- 1 vRealize Automation proporciona las reglas de control para permitir los destinos de colocación.
- 2 vRealize Operations Manager proporciona recomendaciones de optimización de la colocación según los datos de los análisis.
- 3 vRealize Automation continúa con el proceso de aprovisionamiento según las recomendaciones de colocación de vRealize Operations Manager.

Si vRealize Operations Manager no puede proporcionar una recomendación o no se puede usar la recomendación, vRealize Automation recurre a su lógica de colocación predeterminada.

Cuando un desarrollador selecciona un elemento de catálogo y completa el formulario para solicitar el elemento de catálogo, vRealize Automation tiene en cuenta las siguientes consideraciones para aprovisionar las máquinas virtuales.

Tabla 2-16. Consideraciones para aprovisionar máquinas virtuales

Consideración	Efecto
Políticas	La política de reserva de vRealize Automation puede indicar más de una reserva.
Reservas	<p>vRealize Automation evalúa la solicitud y determina las reservas que pueden satisfacer las restricciones especificadas en la solicitud.</p> <ul style="list-style-type: none"> ■ Si la colocación se encuentra habilitada y se basa en los análisis de vRealize Operations Manager, vRealize Automation transfiere la lista de reservas a vRealize Operations Manager para determinar la reserva más adecuada para la colocación en función de las métricas operativas. ■ Si la colocación no se basa en vRealize Operations Manager, vRealize Automation decide la colocación en función de las prioridades y la disponibilidad. <p>Se actualizan las reservas para realizar un seguimiento de los recursos que se consumieron. Si vRealize Operations Manager recomienda un clúster o un almacén de datos que vRealize Automation considera sin capacidad o que ya no sea aplicable, vRealize Automation registra la excepción. vRealize Automation permite el aprovisionamiento para seguir conforme a sus mecanismos de colocación predeterminados.</p>

Para identificar los recursos para una máquina virtual, vRealize Automation proporciona una lista de reservas candidatas. Cada candidata de la lista puede incluir un clúster y uno o varios almacenes de datos o clústeres de almacenes de datos. vRealize Operations Manager utiliza las reservas candidatas para crear la lista de candidatas de destino y ubicar el destino adecuado.

La política en vRealize Operations Manager establece el nivel de equilibrio, el uso y el espacio en búfer para el clúster. Para una reserva única, que es un clúster o un clúster de almacenes de datos, vRealize Automation valida si la recomendación es un destino de colocación viable.

- Si el destino es viable, vRealize Automation implementa el blueprint de acuerdo con la recomendación.
- Si el destino no es viable, vRealize Automation utiliza el comportamiento de colocación predeterminado para colocar las máquinas virtuales.

Las consideraciones de colocación también deben tener en cuenta los problemas de estado y uso. Mientras que el administrador de la nube y el administrador de la infraestructura virtual administran la infraestructura, los desarrolladores se preocupan por el estado de sus aplicaciones. Para ayudar a los desarrolladores, la estrategia de colocación de cargas de trabajo también debe tener en cuenta los problemas de estado y uso.

Tabla 2-17. Consideraciones sobre problemas de uso y estado

Problema de carga de trabajo	Solución de colocación
El desarrollador detecta un problema de estado en el entorno.	vRealize Automation aprovisiona los blueprints en clústeres donde se observan problemas o un uso excesivo debido a cargas de trabajo grandes. vRealize Automation debe integrarse con los análisis de capacidad de vRealize Operations Manager para garantizar que los blueprints se aprovisionen en clústeres con capacidad suficiente.
El desarrollador detecta un problema de uso.	Los clústeres en el entorno se encuentran infrutilizados. vRealize Automation debe integrarse con los análisis de capacidad que proporciona vRealize Operations Manager para garantizar que los blueprints se aprovisionen en un clúster donde se maximice el uso.

Usuarios que aprovisionan blueprints

Los siguientes usuarios realizan acciones para aprovisionar los blueprints.

Tabla 2-18. Usuarios y funciones para aprovisionar blueprints

Paso	Administración	Acción	Función necesaria
1	Administrador de la nube o administrador de la infraestructura virtual	Asegúrese de que la colocación inicial de las máquinas virtuales cumpla con las políticas organizativas y de que las máquinas se optimicen según los datos de los análisis operativos.	Función de administrador de IaaS
1	Administrador de tejido	Define las reservas, las políticas de reserva y la política de colocación en vRealize Automation.	Función de administrador de tejido, arquitecto de infraestructura
1	Administrador de IaaS	Define los endpoints para vSphere y vRealize Operations Manager, los cuales son necesarios para la colocación de las cargas de trabajo.	Función de administrador de IaaS
2	Arquitecto de infraestructura	Como arquitecto de blueprint que trabaja directamente con los tipos de componentes de las máquinas virtuales, asigna las políticas de reserva a las máquinas virtuales cuando se crea un blueprint. Especifica la política de reserva como una propiedad del componente de la máquina en el blueprint.	Arquitecto de infraestructura

Tabla 2-18. Usuarios y funciones para aprovisionar blueprints (continuación)

Paso	Administración	Acción	Función necesaria
3	Arquitecto de infraestructura, arquitecto de aplicaciones, arquitecto de software y arquitecto de XaaS	<p>Crea y publica el blueprint para aprovisionar las máquinas virtuales. Solo el arquitecto de infraestructura trabaja directamente con componentes de máquina. El resto de funciones de arquitecto puede reutilizar blueprints de infraestructura en anidamiento, aunque no pueden editar la configuración de los componentes de la máquina.</p> <p>El blueprint puede incluir un solo componente, o puede incluir blueprints anidados, componentes de XaaS, varias máquinas virtuales en una aplicación de varios niveles, etc.</p> <p>vRealize Automation ubica las máquinas virtuales en función de la configuración de las reservas y, opcionalmente, incluye la política de reserva en el nivel de componente de máquina para el blueprint. Por ejemplo, el blueprint puede incluir dos máquinas y en cada una de ellas se puede aplicar una política distinta.</p> <p>vRealize Automation también optimiza las máquinas virtuales de acuerdo con los datos de los análisis operativos que proporciona vRealize Operations Manager.</p>	Arquitecto de infraestructura
4	Administrador de la nube o administrador de la infraestructura virtual	<p>Selecciona las políticas que determinan la colocación inicial de las máquinas virtuales que aprovisiona vRealize Automation.</p> <p>El administrador puede:</p> <ul style="list-style-type: none"> ■ Seleccionar las políticas mediante una API. ■ Usar la política de colocación predeterminada, en la que se utiliza cada servidor de vRealize Automation por turnos para equilibrar las cargas de trabajo. Este enfoque no requiere entradas de vRealize Operations Manager. 	Función de administrador de IaaS, arquitecto de infraestructura
5	Administrador de la infraestructura virtual	Crea el centro de datos personalizado y los grupos personalizados en vRealize Operations Manager. A continuación, el administrador de la infraestructura virtual aplica la política utilizada para consolidar y equilibrar las cargas de trabajo a esos centros de datos personalizados.	Función de administrador de IaaS, arquitecto de infraestructura
6	Administrador de tejido	<p>Selecciona la política de colocación de vRealize Automation.</p> <p>Utilizar la política de colocación de cargas de trabajo para que vRealize Automation determine el lugar donde se pueden colocar las máquinas cuando se implementan blueprints nuevos. La política de colocación requiere que vRealize Operations Manager aporte información.</p>	Función de administrador de tejido

Tabla 2-18. Usuarios y funciones para aprovisionar blueprints (continuación)

Paso	Administración	Acción	Función necesaria
7	Desarrollador	Solicita un blueprint para aprovisionar las máquinas virtuales. El blueprint puede contener varias máquinas para ejecutar una aplicación de tres niveles.	
8	Desarrollador	Cuando el desarrollador implementa el blueprint, vRealize Operations Manager busca una política de colocación que se ajuste a los clústeres pertinentes para la solicitud.	

Para obtener más información sobre la política de colocación, consulte [política de colocación](#).

Para configurar la colocación de cargas de trabajo, consulte [Configurar colocación de cargas de trabajo](#).

Se requiere Distributed Resource Scheduler (DRS) para colocar máquinas virtuales

vSphere DRS es el motor de colocación que utilizan vRealize Automation y vRealize Operations Manager para aprovisionar y colocar máquinas virtuales.

Para que vRealize Automation pueda sugerir la mejor ubicación para las máquinas virtuales, es necesario habilitar DRS en el clúster y establecerlo como totalmente automatizado. Tras ello, vRealize Automation usa las API de vSphere DRS para determinar la ubicación correcta de las máquinas virtuales.

vRealize Automation se integra con el servicio de colocación de vRealize Operations Manager. vRealize Operations Manager solo proporciona recomendaciones de colocación para los clústeres con DRS habilitado y totalmente automatizados.

Efecto de las políticas de reserva de almacenamiento de vRealize Automation

La presencia de políticas de reserva de almacenamiento de vRealize Automation afecta a la colocación de las cargas de trabajo con vRealize Operations Manager.

Cuando se habilita la colocación de cargas de trabajo con vRealize Operations Manager, vRealize Automation pasa una lista de reservas disponibles a vRealize Operations Manager; luego vRealize Operations Manager las evalúa para la colocación de almacenamiento en función del análisis operativo.

Cuando un blueprint contiene políticas de reserva de almacenamiento, las recomendaciones de colocación de cargas de trabajo de vRealize Operations Manager pueden cambiar de las siguientes maneras.

Nota La colocación de cargas de trabajo con vRealize Operations Manager solo es compatible con máquinas virtuales que tengan uno o varios discos y donde solo hay una política de reserva de almacenamiento. No se pueden combinar varias políticas para la colocación de discos, ya que no es posible colocar discos individualmente.

- Máquinas virtuales con uno o varios discos, ninguno de los cuales especifica una política de reserva de almacenamiento:

La colocación se realiza como de costumbre. vRealize Operations Manager evalúa la lista completa y sin filtrar de las reservas de candidatos.

- Máquinas virtuales con uno o varios discos, cada uno de los cuales especifica la misma política de reserva de almacenamiento:

Las reservas de candidatos se filtran en el nivel de almacenamiento para que vRealize Operations Manager evalúe solo los almacenes de datos que coincidan con dicha política de reserva de almacenamiento.

- Máquinas virtuales con varios discos, algunos de los cuales especifican la misma política de almacenamiento, pero otros no especifican ninguna política de reserva de almacenamiento:

- Cuando el tipo de asignación de almacenamiento es RECOPIADO (el valor predeterminado), todos los discos se tratan como si compartieran esa misma política. vRealize Operations Manager evalúa los almacenes de datos que coinciden con esa política de reserva de almacenamiento.

- Cuando el tipo de asignación de almacenamiento es DISTRIBUIDO, las máquinas virtuales no se pueden colocar según las recomendaciones de vRealize Operations Manager, ya que no es posible colocar discos individualmente. En su lugar, la colocación utiliza de forma predeterminada los algoritmos de colocación de vRealize Automation.

Puede establecer el tipo de asignación de almacenamiento mediante una propiedad personalizada.

- Máquinas virtuales con varios discos, los cuales especifican distintas políticas de reserva de almacenamiento:

Como las máquinas virtuales tienen requisitos de políticas de reserva de almacenamiento en conflicto, no es posible colocarlas según las recomendaciones de vRealize Operations Manager. En su lugar, la colocación utiliza de forma predeterminada los algoritmos de colocación de vRealize Automation.

- Máquinas virtuales que requieren una ruta de almacenamiento específica:

Estas máquinas virtuales no se colocan mediante una recomendación de vRealize Operations Manager, puesto que ya se ha especificado una ruta de almacenamiento. La colocación puede coincidir o no con lo que recomendaría vRealize Operations Manager.

Puede establecer la ruta de almacenamiento mediante una propiedad personalizada.

Errores de colocación: cuando la colocación basada en vRealize Operations Manager no se puede producir, un error describe el motivo. Entre los motivos se pueden incluir las condiciones no admitidas que se describen en la lista anterior o factores ambientales como errores de comunicación entre vRealize Operations Manager y vRealize Automation.

Para revisar los errores, vaya a **Solicitudes > Ejecución**. Cerca de la parte superior derecha, haga clic en **Ver errores de colocación**.

Limitaciones de la ubicación de cargas de trabajo

Cuando se utiliza la política de colocación en la ubicación de cargas de trabajo para colocar máquinas cuando se implementan nuevos blueprints, tenga en cuenta las limitaciones.

- En vRealize Operations Manager, la solución vRealize Automation identifica los clústeres y las máquinas virtuales que administra vRealize Automation.
- Cuando vRealize Automation administra los objetos secundarios de un centro de datos o un contenedor de centro de datos personalizado en vRealize Operations Manager, la capacidad para volver a equilibrar o mover los objetos no está disponible. No se puede activar o desactivar la exclusión de acciones en objetos administrados de vRealize Automation.
- Para los objetos que administra vRealize Automation, el comportamiento de la ubicación de las cargas de trabajo es el siguiente:
 - Cuando un centro de datos personalizado o un centro de datos incluye un clúster que administra vRealize Automation, la ubicación de las cargas de trabajo no permite volver a equilibrar el clúster.
 - Cuando un clúster incluye máquinas virtuales que administra vRealize Automation, la ubicación de las cargas de trabajo no permite mover esas máquinas virtuales.
- vRealize Operations Manager no admite la ubicación de cargas de trabajo en los grupos de recursos de vCenter Server.
- vRealize Operations Manager no admite vSAN en la versión actual.

Permisos para configurar la colocación de cargas de trabajo

Debe tener permisos en vRealize Automation y vRealize Operations Manager para configurar la colocación de cargas de trabajo y la política de colocación.

En vRealize Automation, para configurar la colocación de cargas de trabajo debe tener la función de administrador de tejido. Consulte la descripción general de funciones de usuario en el Centro de información de vRealize Automation.

En vRealize Operations Manager, debe crear una función de usuario para la ubicación de cargas de trabajo, así como asignar permisos a la función.

- En la cuenta de usuario, asigne el permiso de solo lectura a los hosts y clústeres de vSphere, y el almacenamiento de vSphere, en la jerarquía de objetos.

- Para que la función de usuario pueda usar las llamadas de API en la ubicación de cargas de trabajo, asigne permisos de lectura y escritura en las API. Seleccione **Administración > Control de acceso > Permisos** y seleccione **API de REST > Otras API de lectura, escritura**.

vRealize Automation utiliza la función vRealize Operations Manager cuando se registra el endpoint y al solicitar recomendaciones de colocación durante el aprovisionamiento en nombre de los usuarios que solicitan elementos de catálogo.

Para obtener más información, consulte Control de acceso en el Centro de información de vRealize Operations Manager.

política de colocación

Puede utilizar la política de ubicación para que vRealize Automation determine dónde colocar las máquinas cuando se implementan nuevos blueprints. La política de ubicación utiliza los análisis de vRealize Operations Manager para identificar las cargas de trabajo en los clústeres para que pueda sugerir destinos de ubicación.

Debe realizar varios pasos antes de poder utilizar la política de ubicación. En vRealize Automation, cree endpoints para las instancias de vRealize Operations Manager y vCenter Server. A continuación, cree un grupo de tejidos y agregue reservas al endpoint de vCenter Server.

Para asegurarse de que vRealize Operations Manager proporciona análisis de ubicación de cargas de trabajo a vRealize Automation, debe:

- Instalar la solución vRealize Automation en la instancia de vRealize Operations Manager que se utiliza para la ubicación de las cargas de trabajo.
- Configurar vRealize Operations Manager para que supervise el vCenter Server.

Para configurar vRealize Automation y vRealize Operations Manager para la ubicación de las cargas de trabajo, consulte [Configurar colocación de cargas de trabajo](#).

Ubicación de la política de ubicación

En su instancia de vRealize Automation seleccione **Infraestructura > Reservas > Política de ubicación**.

Para utilizar los análisis de ubicación de cargas de trabajo que proporciona vRealize Operations Manager, seleccione **Utilizar vRealize Operations Manager para obtener recomendaciones de ubicación**.

Si no utiliza la política de ubicación de cargas de trabajo, vRealize Automation utiliza el método de colocación predeterminado.

Configurar colocación de cargas de trabajo

Para usar la política de colocación para colocar máquinas cuando se implementen nuevos blueprints, hay que configurar vRealize Automation para que use los análisis que vRealize Operations Manager proporciona. También hay que configurar vRealize Operations Manager para que ponga en marcha una política para consolidar y equilibrar cargas de trabajo en el clúster de recursos informáticos.

En vRealize Automation, configurará endpoints, creará un grupo de tejidos y añadirá reservas. En vRealize Operations Manager, configurará una política para dar cabida al equilibrio de la carga de trabajo y pondrá en marcha esa política en un grupo personalizado que incluya los recursos informáticos personalizados.

Requisitos previos

Para que la política de colocación pueda sugerir destinos de colocación de los blueprints, debe realizar varios pasos.

- Comprenda la política de colocación. Consulte [política de colocación](#).
- Compruebe que existe un endpoint de vRealize Automation para la instancia de vRealize Operations Manager que se usa para la colocación de cargas de trabajo. Consulte [Crear un endpoint de vRealize Operations Manager](#).
- Compruebe que existe un endpoint de vRealize Automation para la instancia de vCenter Server. Consulte [Crear un endpoint de vSphere](#).
- Añada reservas al endpoint de vCenter Server. Consulte [Reservas](#).
- Añada un grupo de tejidos y compruebe que su usuario es un administrador de ese grupo de tejidos. Consulte [Crear un grupo de tejidos](#).
- Compruebe que vRealize Operations Manager supervisa la misma infraestructura que vRealize Automation supervisa a fin de asegurarse de que ambos incluyen las mismas instancias de vCenter Server. Consulte [Solución de VMware vSphere en vRealize Operations Manager](#) en el centro de información de vRealize Operations Manager.
- Conozca las reservas, la reserva de almacenamiento, los blueprints y los proveedores de delegados. Consulte el centro de información de vRealize Automation.
- Comprenda y defina la configuración de relleno y equilibrio de la política de vRealize Operations Manager que se usa para la colocación de cargas de trabajo. Consulte [Detalles de la automatización de cargas de trabajo](#) en el centro de información de vRealize Operations Manager.

Procedimiento

1 [Configurar vRealize Automation para la colocación de carga de trabajo](#)

Si quiere utilizar análisis de colocación de cargas de trabajo para colocar máquinas cuando implemente nuevos blueprints, debe preparar la instancia de vRealize Automation.

2 [Configurar vRealize Operations Manager para la colocación de cargas de trabajo en vRealize Automation](#)

Para proporcionar análisis de colocación de cargas de trabajo para que vRealize Automation coloque máquinas cuando implemente nuevos blueprints, debe preparar la instancia de vRealize Operations Manager.

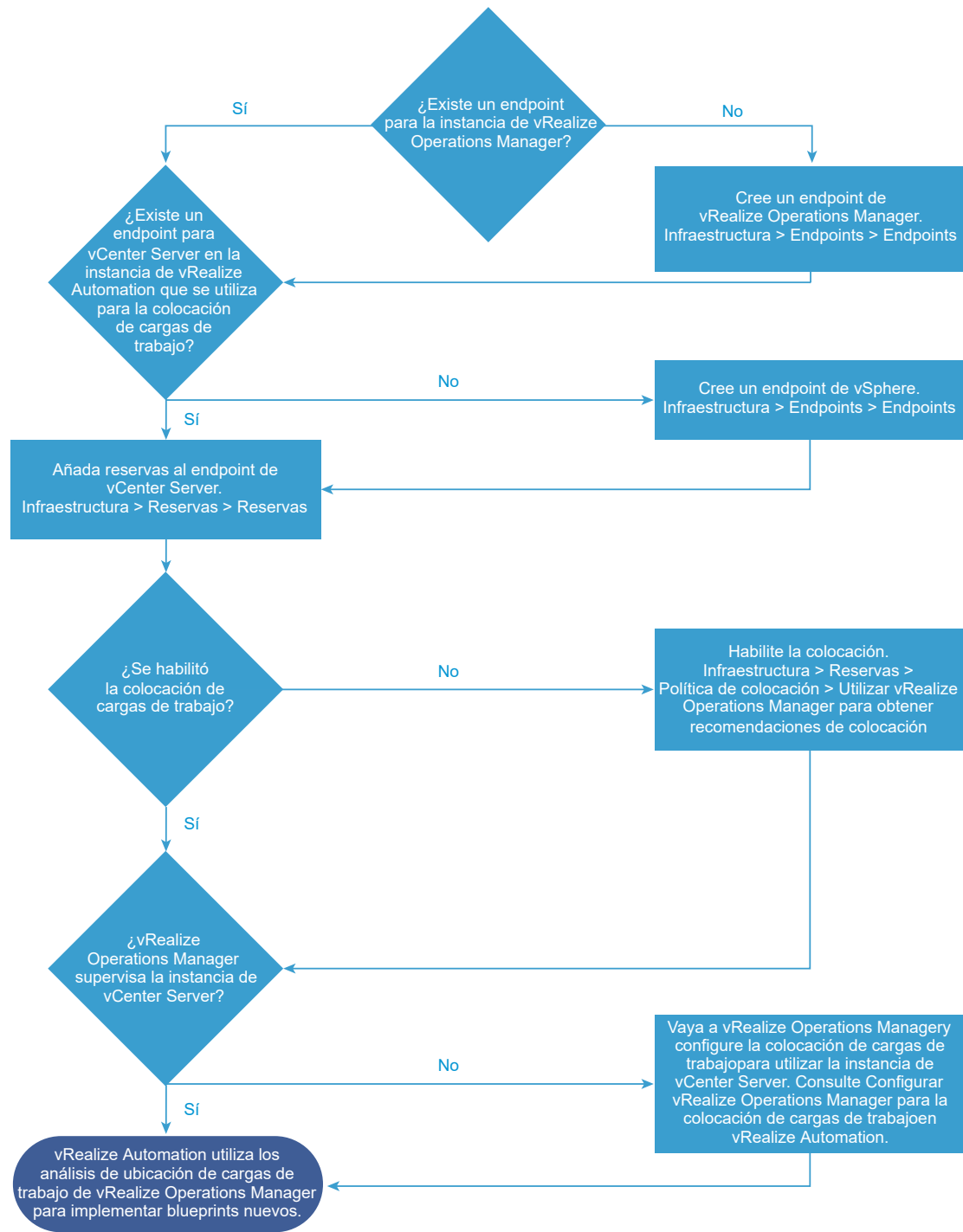
Resultados

Ha configurado vRealize Automation y vRealize Operations Manager de forma que usen análisis de colocación de cargas de trabajo para sugerir destinos de colocación de los nuevos blueprints.

Configurar vRealize Automation para la colocación de carga de trabajo

Si quiere utilizar análisis de colocación de cargas de trabajo para colocar máquinas cuando implemente nuevos blueprints, debe preparar la instancia de vRealize Automation.

Para preparar la instancia de vRealize Automation de forma que use la directiva de colocación, hay que configurar endpoints, crear un grupo de tejidos y añadir reservas.



Requisitos previos

- Para usar la colocación de cargas de trabajo, debe conocer los requisitos. Consulte [Configurar colocación de cargas de trabajo](#).
- En vRealize Automation, añada una función de usuario específica y permisos para que vRealize Operations Manager valide las credenciales. Consulte la descripción general de funciones de usuario en el Centro de información de vRealize Automation.

Procedimiento

- 1 En la instancia de vRealize Automation, añada un endpoint relativo a la instancia de vRealize Operations Manager y haga clic en **Aceptar**.
 - a Seleccione **Infraestructura > Endpoint > Endpoints**.
 - b Seleccione **Nuevo > Administración > vRealize Operations Manager**.
 - c Introduzca la información general del endpoint de **vRealize Operations Manager**.

No es necesario especificar las propiedades del endpoint.

- 2 En la instancia de vRealize Automation, añada un endpoint relativo a la instancia de vCenter Server y haga clic en **Aceptar**.
 - a Seleccione **Infraestructura > Endpoint > Endpoints**.
 - b Seleccione **Nuevo > Virtual > vSphere (vCenter)**.
 - c Introduzca la información general, las propiedades y las asociaciones del endpoint de vCenter Server.

Después de haber añadido los endpoints y de que vRealize Automation haya recopilado datos de ellos, habrá disponibles recursos informáticos para esos endpoints. Estos recursos informáticos se pueden añadir al grupo de tejidos que va a crear.

- 3 Cree un grupo de tejidos para que otros usuarios puedan crear reservas y habilitar la política de colocación.
 - a Seleccione **Infraestructura > Endpoint > Grupos de tejidos**.
 - b Haga clic en **Nuevo** e introduzca la información del grupo de tejidos.

Opción	Descripción
Nombre	Escriba un nombre con sentido para el grupo de tejidos.
Descripción	Escriba una descripción práctica.
Administradores de tejido	Escriba la dirección de correo electrónico de cada persona que se vaya a designar como administrador de tejido.
Recursos informáticos	Seleccione los clústeres de recursos informáticos que los administradores pueden gestionar.

Después de haber añadido recursos informáticos a un grupo de tejidos y de que vRealize Automation haya recopilado datos de ellos, los administradores de tejido pueden crear reservas de los recursos informáticos.

4 Cree reservas de los recursos informáticos en la instancia de vCenter Server.

- a Seleccione **Infraestructura > Reservas > Reservas**.
- b Seleccione **Nuevo > vSphere (vCenter)**.
- c En cada pestaña, introduzca la información de la reserva.

Opción	Acción
General	Seleccione una política de reserva y la prioridad de la política y haga clic en Habilitar esta reserva .
Recursos	Seleccione la cuota de máquinas, la memoria y el almacenamiento. No es necesario seleccionar un grupo de recursos.
Red	Seleccione el adaptador de red. No es necesario seleccionar un perfil de red.
Propiedades	Si procede, añada propiedades personalizadas a la reserva.
Alerta	Si procede, seleccione Alertas de capacidad para notificar a los destinatarios cuando la capacidad supere el umbral de la reserva.

5 Habilite la política de colocación.

- a Seleccione **Infraestructura > Reservas > Política de colocación**.
- b Active la casilla de verificación denominada **Usar vRealize Operations Manager para recomendaciones de colocación**.

Resultados

Ha configurado vRealize Automation para que use los análisis de vRealize Operations Manager para colocar máquinas cuando los usuarios implementen blueprints.

Pasos siguientes

Configure vRealize Operations Manager para que supervise la instancia de vCenter Server y aplique una política de colocación de cargas de trabajo en los recursos informáticos del clúster. Consulte [Configurar vRealize Operations Manager para la colocación de cargas de trabajo en vRealize Automation](#).

Configurar vRealize Operations Manager para la colocación de cargas de trabajo en vRealize Automation

Para proporcionar análisis de colocación de cargas de trabajo para que vRealize Automation coloque máquinas cuando implemente nuevos blueprints, debe preparar la instancia de vRealize Operations Manager.

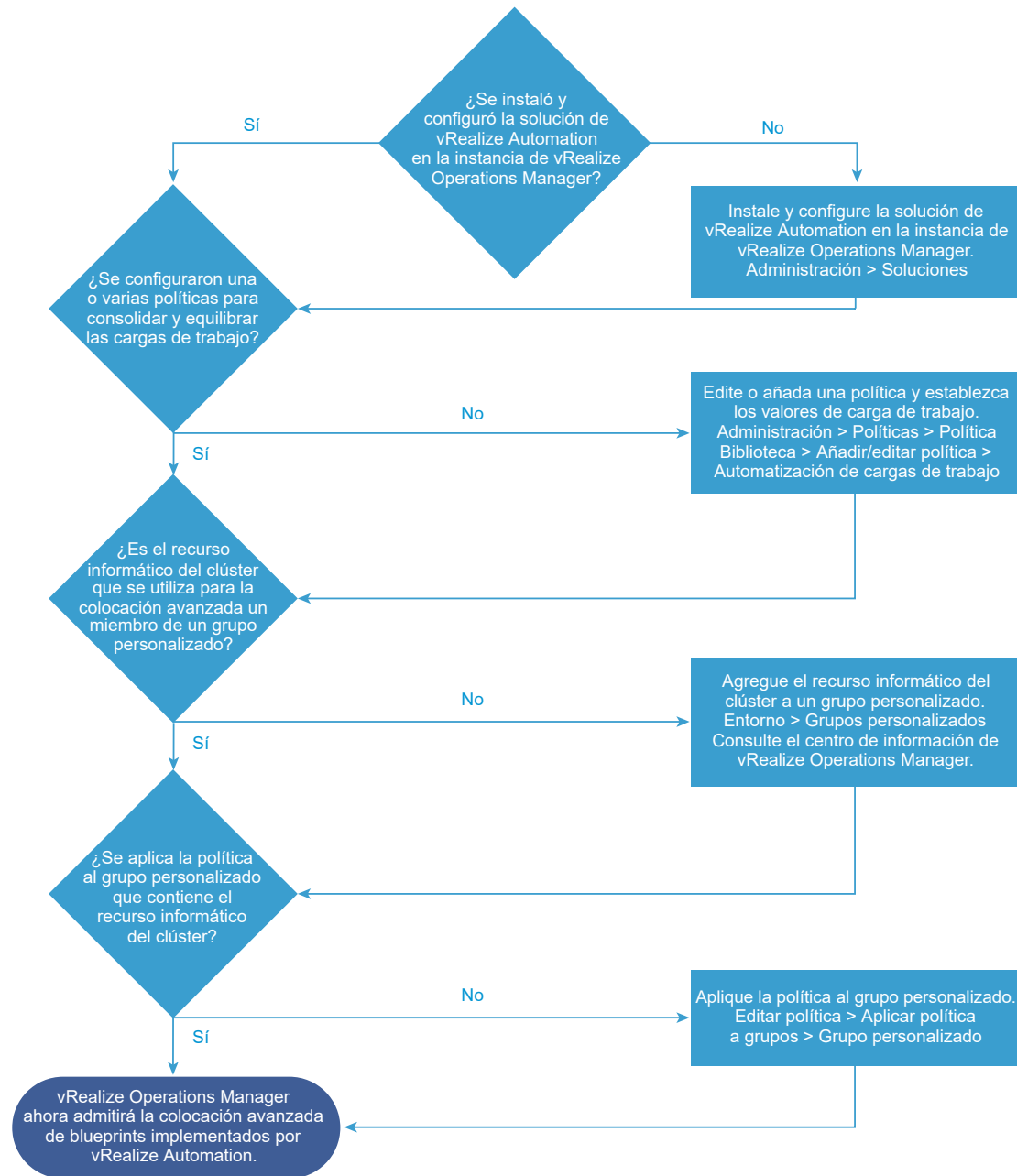
Precaución Es necesario instalar la solución de vRealize Automation (que incluye el paquete de administración) en una sola instancia de vRealize Operations Manager.

Para preparar la instancia de vRealize Operations Manager para que proporcione análisis a vRealize Automation, instale y configure la solución vRealize Automation. También debe configurar una política y aplicarla en los recursos informáticos del clúster.

Después de configurar la solución de vRealize Automation, no podrá trasladar ni volver a equilibrar ninguna máquina virtual que vRealize Automation administre.

Si la solución de vRealize Automation no se instala en la instancia de vRealize Operations Manager, la colocación de cargas de trabajo puede trasladar o volver a equilibrar las máquinas virtuales que administra vRealize Automation.

Para permitir que la colocación de cargas de trabajo mueva las máquinas virtuales, esas máquinas virtuales deben residir en un centro de datos o en un centro de datos personalizado.



Requisitos previos

- Configure vRealize Automation para que use análisis de colocación de cargas de trabajo. Consulte [Configurar vRealize Automation para la colocación de carga de trabajo](#).
- Confirme que la solución de vRealize Automation está instalada y configurada en la instancia de vRealize Operations Manager que se usa para la colocación de cargas de trabajo. Para obtener información detallada sobre esta solución, consulte el tema sobre [Management Pack for vRealize Automation en Solution Exchange](#). Para obtener información sobre cómo funciona la colocación de cargas de trabajo en vRealize Operations Manager, consulte el tema de [detalles de la automatización de cargas de trabajo](#) y otros temas relacionados en la documentación de vRealize Operations Manager.

Procedimiento

- 1 En la instancia de vRealize Operations Manager que administra la colocación de cargas de trabajo, instale y configure la solución de vRealize Automation.

Es probable que la solución ya esté instalada.

- a Para ver las soluciones que hay instaladas en vRealize Operations Manager, haga clic en **Administración > Soluciones**.

- b Compruebe que la solución de vRealize Automation ya está instalada.

Si la solución de vRealize Automation no figura en la lista, descárguela e instálela.

Consulte el tema de [Management Pack for vRealize Automation en Solution Exchange](#).

- c Si la solución figura en la lista, seleccione la **solución de VMware vRealize Automation** y haga clic en **Configurar**.

- d Configure la solución de vRealize Automation y guarde la configuración.

Para obtener más información sobre la forma de configurar la solución, consulte [Soluciones de vRealize Operations Manager](#) en el centro de información de vRealize Operations Manager.

- 2 Si no utiliza la política predeterminada de vRealize Operations Manager, debe crear un grupo personalizado. A continuación, debe añadir los recursos informáticos del clúster al grupo personalizado.

Para usar una política distinta de la política predeterminada en los clústeres, añada un grupo personalizado. Luego, aplique la política en el grupo personalizado. Si usa la política predeterminada, no es necesario crear un grupo personalizado, ya que la política predeterminada se aplica a todos los objetos.

- a Haga clic en **Entorno > Grupos personalizados**.

- b Si no existe un grupo personalizado para los clústeres, créelo.

Para obtener detalles, consulte [Escenario de usuario: Crear grupos de objetos personalizados](#) en el centro de información de vRealize Operations Manager.

- c Añada el clúster al grupo personalizado y guarde el grupo personalizado.

- 3 Configure una política para consolidar y equilibrar las cargas de trabajo en los clústeres y póngala en marcha en el grupo personalizado.

En vRealize Operations Manager se configuran políticas para establecer las opciones de consolidación, equilibrio, relleno, CPU, memoria y espacio en disco. Por ejemplo, la opción Consolidar cargas de trabajo se modifica para determinar la mejor colocación de nuevas cargas de trabajo administradas en función de la capacidad y el estado del clúster. Igualmente, también modificamos la opción de umbral para equilibrar cargas de trabajo en el nivel de intensidad necesario para colocar cargas de trabajo. Se pueden configurar una o varias políticas y aplicarlas en los recursos informáticos del clúster.

- a Para encontrar las políticas, haga clic en **Administración > Políticas > Biblioteca de políticas**.
- b Para establecer los valores de carga de trabajo, haga clic en **Agregar/editar política** y, luego, haga clic en **Automatización de carga de trabajo**.

Las opciones de configuración denominadas Consolidar cargas de trabajo y Capacidad de aumento de clúster se aplican a la colocación inicial de máquinas virtuales.

- Cuando Consolidar cargas de trabajo se establece en **Ninguna**, la colocación de cargas de trabajo equilibra la carga de trabajo en todos los clústeres a los que se aplica la política. Cuando Consolidar cargas de trabajo se establece en un valor distinto a Ninguna, la colocación de cargas de trabajo rellena el clúster más ocupado primero.
 - El valor de Capacidad de aumento de clúster es el espacio de búfer reservado en un clúster, como un porcentaje de la capacidad total. Por ejemplo, si se establece la capacidad de aumento de clúster en 20%, ese búfer podría impedir que la colocación de cargas de trabajo coloque máquinas virtuales en ese clúster. El motivo por el que se impide la colocación es que el clúster tiene un 20% menos de la capacidad libre para CPU, memoria o espacio de disco.
- c En el área de trabajo de política, haga clic en **Aplicar política a grupos**.
 - d Seleccione el grupo personalizado.
 - e Guarde la política.

Resultados

Ha configurado vRealize Operations Manager de forma que vRealize Automation use los análisis de colocación de cargas de trabajo para sugerir destinos de colocación de máquinas cuando los usuarios implementen blueprints.

Pasos siguientes

Espere a que vRealize Automation y vRealize Operations Manager recopilen datos de los endpoints y los objetos de su entorno. Así, cuando implemente nuevos blueprints, vRealize Automation mostrará las recomendaciones de colocación de cargas de trabajo, los candidatos de destino y la ubicación seleccionada para que los confirme.

Solución de problemas con la colocación de cargas de trabajo

Si experimenta problemas con la colocación de cargas de trabajo, utilice la información de solución de problemas para resolverlos.

La solución de vRealize Automation se necesita para que la colocación de cargas de trabajo funcione correctamente

La colocación de cargas de trabajo se basa en las máquinas individuales y se realiza en el nivel de máquina. Cuando se instalan juntos vRealize Automation y vRealize Operations Manager, la solución vRealize Automation también debe instalarse.

La solución, que incluye el paquete de administración y el adaptador, identifica los clústeres en los que las acciones **volver a equilibrar contenedor** o **mover máquina virtual** están desactivadas. La acción de volver a equilibrar está desactivada en el centro de datos personalizado al que pertenece el clúster.

- En el caso de los clústeres de vRealize Automation no administrados que pertenecen a un centro de datos personalizado que no tiene ningún clúster de vRealize Automation administrado, las acciones **mover máquina virtual** y **volver a equilibrar contenedor** están habilitadas. En los clústeres de vRealize Automation administrados, estas acciones están desactivadas.
- En vRealize Operations Manager, el adaptador de vRealize Automation provoca que las máquinas virtuales en los clústeres que asignan las reservas no estén disponibles para moverlas o volver a equilibrarlas.

Precaución La solución de vRealize Automation debe instalarse únicamente en una sola instancia de vRealize Operations Manager.

High Availability está habilitado, pero debe estar desactivado

Cuando HA está habilitado, si vRealize Operations Manager está inactivo, se puede producir un error en el tiempo de espera utilizado para la llamada de colocación de cargas de trabajo a vRealize Operations Manager.

vRealize Automation registra errores de ubicación de la carga de trabajo en el archivo de log `catalina.out`.

Los endpoints de vSphere en vRealize Automation no están supervisados

vRealize Operations Manager no supervisa la instancia de vSphere vCenter Server que contiene los clústeres de reserva.

Si vRealize Operations Manager no reconoce las reservas de candidatos de vRealize Automation para un clúster, un almacén de datos o un clúster de almacén de datos cuando intente colocarlos, los omite. En la respuesta de colocación, vRealize Operations Manager comunica a vRealize Automation que no los reconoce.

Como resultado, en los detalles de colocación de la ejecución de la solicitud, vRealize Automation muestra un icono de advertencia en la reserva de candidatos para indicar que no se reconoce.

Cuando se producen errores de coincidencia, vRealize Automation aparece en la parte superior de la lista

vRealize Automation y vRealize Operations Manager administran diferentes vistas de la infraestructura. Pero ambos deben administrar las mismas instancias de vCenter Server en la misma infraestructura.

Deben identificar las desconexiones y los errores de coincidencia, y mostrar los detalles.

Qué hacer si el adaptador de vRealize Automation está inactivo

La colocación inicial siempre respeta la lista de candidatos de destino que recibe desde vRealize Operations Manager, por ejemplo, cuando un usuario añade un clúster inmediatamente después de la instalación.

Si la solución de vRealize Automation, que incluye el paquete de administración y el adaptador, no se encuentra disponible en vRealize Operations Manager, las acciones `mover máquina virtual` y `volver a equilibrar contenedor` se vuelven disponibles.

Administrar pares de claves

Los pares de claves sirven para aprovisionar y conectarse a una instancia en la nube. Un par de claves se usa para descifrar contraseñas de Windows o para iniciar sesión en una máquina de Linux.

Los pares de claves son necesarios para el aprovisionamiento con Amazon AWS. En el caso de Red Hat OpenStack, los pares de claves son opcionales.

Los pares de claves existentes se importan como parte de la recopilación de datos cuando se añade un endpoint de nube. Un administrador de tejido también puede crear y administrar pares de claves con la consola de vRealize Automation. Si se elimina un par de claves de la consola de vRealize Automation, también se eliminará de la cuenta del servicio de nube.

Aparte de administrar pares de claves manualmente, también puede configurar vRealize Automation para que las genere automáticamente por máquina o grupo empresarial.

- Un administrador de tejido puede configurar la generación automática de pares de claves en el nivel de reserva.
- Si el par de claves se va a controlar en el nivel de blueprint, el administrador de tejido deberá seleccionar **Sin especificar** en la reserva.
- Un administrador de tenant o administrador de grupo empresarial puede configurar la generación automática de pares de claves en el nivel de blueprint.
- Si la generación de pares de claves está configurada en los niveles tanto de reserva como de blueprint, el valor del nivel de reserva reemplaza al de blueprint.

Crear un par de claves

Puede crear pares de claves para usarlos con endpoints mediante vRealize Automation.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Cree un endpoint de nube y añada sus recursos informáticos de nube a un grupo de tejidos. Consulte [Elegir un escenario de endpoint](#) y [Crear un grupo de tejidos](#).

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Pares de claves**.
- 2 Haga clic en **Nuevo**.
- 3 Escriba un nombre en el cuadro de texto **Nombre**.
- 4 Seleccione una región de nube en el menú desplegable **Recurso informático**.
- 5 Haga clic en el icono **Guardar** (✓).

Resultados

El par de claves podrá utilizarse cuando la columna Clave secreta tenga el valor *****.

Cargar la clave privada de un par de claves

Puede cargar la clave privada de un par de claves en formato PEM.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Debe contar previamente con un par de claves. Consulte [Crear un par de claves](#).

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Pares de claves**.
- 2 Busque el par de claves en el que desea cargar una clave privada.
- 3 Haga clic en el icono **Editar** (✎).
- 4 Utilice uno de los siguientes métodos para cargar la clave.
 - Busque un archivo con codificación PEM y haga clic en **Cargar**.
 - Pegue el texto de la clave privada, que comienza con -----BEGIN RSA PRIVATE KEY----- y termina con -----END RSA PRIVATE KEY-----.
- 5 Haga clic en el icono **Guardar** (✓).

Exportar la clave privada de un par de claves

La clave privada de un par de claves se puede exportar a un archivo con codificación PEM.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.

- Debe haber un par de claves con una clave privada. Consulte [Cargar la clave privada de un par de claves](#).

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Pares de claves**.
- 2 Busque el par de claves del que va a exportar la clave privada.
- 3 Haga clic en el icono **Exportar** (📎).
- 4 Vaya a la ubicación en la que quiera guardar el archivo y haga clic en **Guardar**.

Escenario: Aplicar una ubicación a un recurso informático para implementaciones entre regiones

Como administrador de tejido, debe etiquetar los recursos informáticos como pertenecientes al centro de datos de Londres o de Boston para que admitan las implementaciones entre las regiones. Cuando los arquitectos de blueprint habiliten la opción de ubicaciones en sus blueprints, los usuarios podrán elegir entre aprovisionar las máquinas en el centro de datos de Boston o de Londres.



Tiene un centro de datos en Londres y otro en Boston, y no quiere que los usuarios de Boston aprovisionen máquinas en la infraestructura de Londres y viceversa. Para asegurarse de que los usuarios de Boston aprovisionan en la infraestructura de Boston, y los usuarios de Londres aprovisionan en la infraestructura de Londres, le interesa permitir a los usuarios que seleccionen una ubicación adecuada para el aprovisionamiento cuando estos soliciten máquinas.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tejido**.
- Como administrador del sistema, defina las ubicaciones de los centros de datos. Consulte [Escenario: Añadir ubicaciones de centros de datos para implementaciones en varias regiones](#).

Procedimiento

- 1 Seleccione **Infraestructura > Recursos informáticos > Recursos informáticos**.
- 2 Apunte al recurso informático ubicado en el centro de datos de Boston y haga clic en **Editar**.
- 3 Seleccione Boston en el menú desplegable de **Ubicaciones**.

4 Haga clic en **Aceptar**.

5 Repita este procedimiento según sea necesario para asociar los recursos informáticos a las ubicaciones de Boston y Londres.

Resultados

Los arquitectos de IaaS pueden habilitar la característica de ubicaciones para que los usuarios puedan optar por aprovisionar máquinas en Boston o Londres cuando rellenen sus formularios de solicitud de elementos del catálogo. Consulte [Escenario: Permitir a los usuarios seleccionar ubicaciones de centros de datos para implementaciones entre regiones](#).

Aprovisionamiento de una implementación de vRealize Automation con un proveedor de IPAM de terceros

Es posible obtener rangos y direcciones IP para usar en un perfil de red de vRealize Automation de algún proveedor de la solución IPAM de terceros compatible, como Infoblox.

Los rangos de direcciones IP del perfil de red se usan en la reserva asociada que se especifique en un blueprint. Cuando un usuario autorizado solicita el aprovisionamiento de una máquina mediante el elemento del catálogo del blueprint, se obtiene una dirección IP del rango de direcciones IP que especifica el proveedor de IPAM de terceros. Después de implementar la máquina, puede enviar una consulta a la página de detalles del elemento vRealize Automation para detectar la dirección IP en uso.

Tabla 2-19. Preparar el aprovisionamiento de una implementación de vRealize Automation con la lista de comprobación de Infoblox IPAM

Tarea	Descripción	Detalles
Obtener, importar y configurar el paquete o el complemento del proveedor de la solución IPAM de terceros.	<p>Obtenga e importe el complemento vRealize Orchestrator, ejecute los flujos de configuración de vRealize Orchestrator y registre el tipo de endpoint del proveedor de IPAM en vRealize Orchestrator.</p> <p>Si VMware Solution Exchange en https://marketplace.vmware.com/vsx no contiene el paquete del proveedor de IPAM que usted necesita, podrá crear uno propio con el SDK del proveedor de la solución IPAM y con la documentación complementaria. Consulte la página Paquete de IPAM de terceros de ejemplo de vRealize Automation en code.vmware.com/web/sdk.</p>	Consulte Lista de comprobación para proporcionar soporte técnico del proveedor de IPAM de terceros .
Crear un endpoint del proveedor de la solución IPAM de terceros.	Cree un nuevo endpoint de IPAM en vRealize Automation.	Consulte Crear un endpoint de proveedor de IPAM de terceros .
Especificar la configuración de endpoint del proveedor de la solución IPAM de terceros en un perfil de red externa.	Cree un perfil de red externa y especifique el endpoint de IPAM definido en vRealize Automation.	Consulte Crear un perfil de red externa mediante un proveedor de IPAM de terceros .

Tabla 2-19. Preparar el aprovisionamiento de una implementación de vRealize Automation con la lista de comprobación de Infoblox IPAM (continuación)

Tarea	Descripción	Detalles
Opcionalmente, especificar la configuración de endpoint del proveedor de la solución IPAM de terceros en un perfil de red enrutada.	Cree un perfil de red a petición y especifique el endpoint de IPAM definido en vRealize Automation.	Consulte Crear un perfil de red enrutada mediante un endpoint de IPAM de terceros o Crear un perfil de red NAT mediante un endpoint de IPAM de terceros .
Definir una reserva para usar el perfil de red.	Cree una reserva que llame al perfil de red en vRealize Automation.	Consulte Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer .
Definir un blueprint que use el perfil de red.	Cree un blueprint que utilice la reserva en vRealize Automation.	Consulte Capítulo 3 Proporcionar blueprints de servicio a los usuarios .
Publicar el blueprint en el catálogo para que esté disponible para su uso.	Publique el blueprint en el catálogo en vRealize Automation. Añada las autorizaciones necesarias.	Consulte Publicar un blueprint .
Solicitar el aprovisionamiento de la máquina con el elemento del catálogo del blueprint.	Use el elemento del catálogo del blueprint para solicitar el aprovisionamiento de la máquina en vRealize Automation.	Consulte Administrar el catálogo de servicios .

Configurar recursos de XaaS

Necesita configurar los endpoints de XaaS para poder conectar vRealize Automation a su entorno. Cuando configure los complementos de vRealize Orchestrator como endpoints, utilice la interfaz de usuario de vRealize Automation en lugar de la interfaz de configuración de vRealize Orchestrator para configurar los complementos.

Si desea utilizar las capacidades de vRealize Orchestrator y los plug-ins de vRealize Orchestrator para exponer la tecnología de VMware y de terceros a vRealize Automation, puede configurar los plug-ins de vRealize Orchestrator añadiéndolos como endpoints. De este modo, se crean conexiones a distintos hosts y servidores, como instancias de vCenter Server, un host de Microsoft Active Directory, etc.

Cuando se añade un plug-in de vRealize Orchestrator como endpoint mediante la interfaz de usuario de vRealize Automation, se ejecuta un flujo de trabajo de configuración en el servidor vRealize Orchestrator predeterminado. Los flujos de trabajo de configuración se encuentran en la carpeta de flujos de trabajo en **vRealize Automation > XaaS > Configuración de endpoints**.

Importante No está permitido configurar un único plug-in en vRealize Orchestrator y en la consola de vRealize Automation, por lo que se genera un error.

Configurar el complemento Active Directory como un endpoint

Añada un endpoint y configure el complemento Active Directory para conectarlo con una instancia de Active Directory en ejecución, y administre usuarios y grupos de usuarios, equipos con Active Directory, unidades organizativas, etc.

Después de añadir un endpoint de Active Directory, podrá actualizarlo en cualquier momento.

Requisitos previos

- Compruebe que tiene acceso a una instancia de Active Directory de Microsoft. Consulte la documentación de Active Directory de Microsoft.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Configuración de vRO > Endpoints**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 En el menú desplegable **Complemento**, seleccione **Active Directory**.
- 4 Haga clic en **Siguiente**.
- 5 Especifique un nombre y, opcionalmente, una descripción.
- 6 Haga clic en **Siguiente**.
- 7 Configure los detalles del servidor de Active Directory.
 - a Escriba la dirección IP o el nombre DNS del host en el que se ejecuta Active Directory en el cuadro de texto **IP/URL del host de Active Directory**.
 - b Especifique el puerto de búsqueda del servidor de Active Directory en el cuadro de texto **Puerto**.

vRealize 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. Además de los puertos 389 y 3268, puede usar 636 para LDAPS.
 - c Especifique el elemento raíz del servicio Active Directory en el cuadro de texto **Raíz**.

Por ejemplo, si el nombre del dominio es *mycompany.com*, el Active Directory raíz es **dc=mycompany,dc=com**.

Este nodo se usa para examinar el directorio de servicios después de introducir las credenciales adecuadas. Para directorios de servicios más grandes, al especificar un nodo en el árbol se limita la búsqueda y se mejora el rendimiento. Por ejemplo, en lugar de buscar en todo el directorio, puede especificar **ou=empleados,dc=miempresa,dc=com**. Este elemento raíz muestra todos los usuarios del grupo Empleados.
 - d (opcional) Para activar la certificación cifrada para la conexión entre vRealize Orchestrator y Active Directory, seleccione **Sí** en el menú desplegable **Usar SSL**.

El certificado SSL se importa automáticamente sin solicitar confirmación, incluso aunque esté autofirmado.
 - e (opcional) Introduzca el dominio en el cuadro de texto **Dominio predeterminado**.

Por ejemplo, si el nombre del dominio es *mycompany.com*, escriba **@mycompany.com**.

8 Ajuste la configuración de la sesión compartida.

vRealize Orchestrator utiliza las credenciales para ejecutar todas las acciones y los flujos de trabajo de Active Directory.

- a Escriba el nombre de usuario para la sesión compartida en el cuadro de texto **Nombre de usuario para la sesión compartida**.
- a Escriba la contraseña para la sesión compartida en el cuadro de texto **Contraseña para la sesión compartida**.

9 Haga clic en **Finalizar**.**Resultados**

Añadió una instancia de Active Directory como endpoint. Los arquitectos de XaaS pueden usar XaaS para publicar flujos de trabajo del complemento Active Directory como elementos de catálogo y acciones personalizadas.

Pasos siguientes

- Para utilizar blueprints de vRealize Automation y administrar sus usuarios de Active Directory en su entorno, cree un blueprint de XaaS basado en Active Directory. Para ver un ejemplo, consulte [Crear un blueprint y acción de XaaS para crear y modificar un usuario](#).
- Para usar vRealize Automation y crear registros de Active Directory cuando una máquina se implementa, puede crear diferentes políticas de Active Directory y aplicarlas en diferentes grupos empresariales y blueprints. Consulte [Crear y aplicar políticas de Active Directory](#).

Configurar el complemento de HTTP-REST como un endpoint

Puede añadir un endpoint y configurar el complemento de HTTP-REST para conectarse a un host de REST.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants**.
- Compruebe que tiene acceso a un host de REST.

Procedimiento

- 1** Seleccione **Administración > Configuración de vRO > Endpoints**.
- 2** Haga clic en el icono **Nuevo** (+).
- 3** Seleccione **HTTP-REST** en el menú desplegable **Complemento**.
- 4** Haga clic en **Siguiente**.
- 5** Especifique un nombre y, opcionalmente, una descripción.
- 6** Haga clic en **Siguiente**.

7 Proporcione información sobre el host de REST.

- a Escriba el nombre del host en el cuadro de texto **Nombre**.
- b Escriba la dirección del host en el cuadro de texto **URL**.

Nota Si usa la autenticación de acceso Kerberos, debe proporcionar la dirección del host en formato FDQN.

- c (opcional) Escriba el número de segundos que transcurrirán antes de que se agote el tiempo de espera de una conexión en el cuadro de texto **Tiempo de espera de la conexión (segundos)**.

El valor predeterminado es 30 segundos.

- d (opcional) Escriba el número de segundos que transcurrirán antes de que se agote el tiempo de espera de una operación en el cuadro de texto **Tiempo de espera de la operación (segundos)**.

El valor predeterminado es 60 segundos.

8 (opcional) Configure los ajustes de proxy.

- a Seleccione **Sí** para usar un proxy en el menú desplegable **Usar proxy**.
- b Escriba la IP del servidor proxy en el cuadro de texto **Dirección de proxy**.
- c Escriba el número de puerto para comunicarse con el servidor proxy en el cuadro de texto **Puerto del proxy**.

9 Haga clic en **Siguiente**.**10** Seleccione el tipo de autenticación.

Opción	Acción
Ninguno	No se necesita autenticación.
OAuth 1.0	<p>Usa el protocolo OAuth 1.0. Debe proporcionar los parámetros de autenticación obligatorios para OAuth 1.0.</p> <ul style="list-style-type: none"> a Escriba la clave usada para identificar al consumidor como proveedor de servicios en el cuadro de texto Clave del consumidor. b Escriba el secreto para establecer propiedad de la clave de consumidor en el cuadro de texto Secreto del consumidor. c (opcional) Escriba el token de acceso que el consumidor usa para obtener acceso a los recursos protegidos en el cuadro de texto Token de acceso. d (opcional) Escriba el secreto que el consumidor usa para establecer propiedad de un token en el cuadro de texto Secreto del token de acceso.
OAuth 2.0	<p>Usa el protocolo OAuth 2.0.</p> <p>Especifique el token de autenticación en el cuadro de texto Token.</p>

Opción	Acción
Básico	<p>Proporciona autenticación de acceso básica. La comunicación con el host se realiza en modo de sesión compartida.</p> <ol style="list-style-type: none"> Escriba el nombre de usuario para la sesión compartida en el cuadro de texto Nombre de usuario de autenticación. Escriba la contraseña para la sesión compartida en el cuadro de texto Contraseña de autenticación.
Implícita	<p>Proporciona autenticación de acceso implícita que usa cifrado. La comunicación con el host se realiza en modo de sesión compartida.</p> <ol style="list-style-type: none"> Escriba el nombre de usuario para la sesión compartida en el cuadro de texto Nombre de usuario de autenticación. Escriba la contraseña para la sesión compartida en el cuadro de texto Contraseña de autenticación.
NTLM	<p>Proporciona autenticación de acceso con NT LAN Manager (NTLM) dentro del marco de Proveedor de compatibilidad para seguridad de Windows (SSP). La comunicación con el host se realiza en modo de sesión compartida.</p> <ol style="list-style-type: none"> Proporcione las credenciales de usuario para la sesión compartida. <ul style="list-style-type: none"> Escriba el nombre de usuario para la sesión compartida en el cuadro de texto Nombre de usuario de autenticación. Escriba la contraseña para la sesión compartida en el cuadro de texto Contraseña de autenticación. Configure los detalles de NTLM <ul style="list-style-type: none"> (opcional) Especifique el nombre de la estación de trabajo en el cuadro de texto Estación de trabajo para autenticación NTLM. Especifique el nombre del dominio en el cuadro de texto Dominio para autenticación NTLM.
Kerberos	<p>Proporciona autenticación de acceso Kerberos. La comunicación con el host se realiza en modo de sesión compartida.</p> <ol style="list-style-type: none"> Escriba el nombre de usuario para la sesión compartida en el cuadro de texto Nombre de usuario de autenticación. Escriba la contraseña para la sesión compartida en el cuadro de texto Contraseña de autenticación.

11 Haga clic en **Finalizar**.

Resultados

Ha configurado el endpoint y ha añadido un host de REST. Los arquitectos de XaaS pueden usar XaaS para publicar flujos de trabajo del complemento de HTTP-REST como elementos del catálogo y acciones personalizadas.

Configurar el complemento de PowerShell como un endpoint

Puede añadir un endpoint y configurar el complemento de PowerShell para conectarse a un host de PowerShell en ejecución, de manera que pueda llamar a los scripts de PowerShell y cmdlets desde flujos de trabajo y acciones de vRealize Orchestrator, y trabajar con el resultado.

Requisitos previos

- Compruebe que tiene acceso a un host de Windows PowerShell. Para obtener más información acerca de Microsoft Windows PowerShell, consulte la documentación de Windows PowerShell.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Configuración de vRO > Endpoints**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Seleccione **PowerShell** en el menú desplegable **Complemento**.
- 4 Haga clic en **Siguiente**.
- 5 Especifique un nombre y, opcionalmente, una descripción.
- 6 Haga clic en **Siguiente**.
- 7 Especifique los detalles del host de PowerShell.
 - a Escriba el nombre del host en el cuadro de texto **Nombre**.
 - b Escriba la dirección IP o el FDQN del host en el cuadro de texto **Host/IP**.
- 8 Seleccione el tipo de host de PowerShell al que se conecta el complemento.

Opción	Acción
WinRM	<ol style="list-style-type: none"> a Escriba el número de puerto que desea utilizar para la comunicación con el host en el cuadro de texto Puerto en los detalles del host de PowerShell. b Seleccione un protocolo de transporte en el menú desplegable Protocolo de transporte. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Nota Si utiliza el protocolo de transporte HTTPS, el certificado del host remoto de PowerShell se importa en el almacén de claves de vRealize Orchestrator.</p> </div> c Seleccione un tipo de autenticación en el menú desplegable Autenticación. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Nota Para utilizar la autenticación Kerberos, habilítela en el servicio WinRM. Para obtener información acerca de la configuración de la autenticación Kerberos, consulte <i>Utilizar el complemento PowerShell</i>.</p> </div>
SSH	Ninguno.

- 9 Escriba las credenciales para una comunicación de sesión compartida con el host PowerShell en los cuadros de texto **Nombre de usuario** y **Contraseña**.
- 10 Haga clic en **Finalizar**.

Resultados

Ha añadido un host Windows PowerShell como endpoint. Los arquitectos de XaaS pueden usar XaaS para publicar flujos de trabajo del complemento PowerShell como elementos del catálogo y acciones personalizadas.

Configurar el complemento de SOAP como un endpoint

Puede añadir un endpoint y configurar el complemento de SOAP para definir un servicio de SOAP como objeto de inventario, así como realizar operaciones de SOAP en los objetos definidos.

Requisitos previos

- Compruebe que tiene acceso a un host de SOAP. El complemento es compatible con las versiones de SOAP 1.1 y 1.2 y WSDL 1.1 y 2.0.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Configuración de vRO > Endpoints**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 En el menú desplegable **Complemento**, seleccione **SOAP**.
- 4 Haga clic en **Siguiente**.
- 5 Especifique un nombre y, opcionalmente, una descripción.
- 6 Haga clic en **Siguiente**.
- 7 Proporcione los detalles acerca del host de SOAP.
 - a Escriba el nombre del host en el cuadro de texto **Nombre**.
 - b Seleccione si el contenido de WSDL se proporcionará como texto en el menú desplegable **Proporcionar contenido de WSDL**.

Opción	Acción
Sí	Escriba el texto WSDL en el cuadro de texto Contenido WSDL .
No	Escriba la ruta correcta en el cuadro de texto URL de WSDL .

- c (opcional) Escriba el número de segundos que transcurrirán antes de que se agote el tiempo de espera de una conexión en el cuadro de texto **Tiempo de espera de la conexión (en segundos)**.

El valor predeterminado es 30 segundos.

- d (opcional) Escriba el número de segundos que transcurrirán antes de que se agote el tiempo de espera de una operación en el cuadro de texto **Tiempo de espera de la solicitud (en segundos)**.

El valor predeterminado es 60 segundos.

8 (opcional) Especifique la configuración proxy.

- a Para utilizar un proxy, seleccione **Sí** en el menú desplegable **Proxy**.
- b Escriba la dirección IP del servidor proxy en el cuadro de texto **Proxy**.
- c Escriba el número de puerto para comunicarse con el servidor proxy en el cuadro de texto **Puerto**.

9 Haga clic en **Siguiente**.

10 Seleccione el tipo de autenticación.

Opción	Acción
Ninguno	No se necesita autenticación.
Básico	<p>Proporciona autenticación de acceso básica. La comunicación con el host se realiza en modo de sesión compartida.</p> <ul style="list-style-type: none"> a Escriba el nombre de usuario para la sesión compartida en el cuadro de texto Nombre de usuario. b Escriba la contraseña para la sesión compartida en el cuadro de texto Contraseña.
Implícita	<p>Proporciona autenticación de acceso implícita que usa cifrado. La comunicación con el host se realiza en modo de sesión compartida.</p> <ul style="list-style-type: none"> a Escriba el nombre de usuario para la sesión compartida en el cuadro de texto Nombre de usuario. b Escriba la contraseña para la sesión compartida en el cuadro de texto Contraseña.

Opción	Acción
NTLM	<p>Proporciona autenticación de acceso con NT LAN Manager (NTLM) en el marco de Proveedor de compatibilidad para seguridad de Windows (SSP). La comunicación con el host se realiza en modo de sesión compartida.</p> <ol style="list-style-type: none"> Proporcione las credenciales de usuario. <ul style="list-style-type: none"> ■ Escriba el nombre de usuario para la sesión compartida en el cuadro de texto Nombre de usuario. ■ Escriba la contraseña para la sesión compartida en el cuadro de texto Contraseña. Proporcione la configuración de NTLM. <ul style="list-style-type: none"> ■ Especifique el nombre del dominio en el cuadro de texto Dominio NTLM. ■ (opcional) Especifique el nombre del dominio en el cuadro de texto Estación de trabajo NTLM.
Negotiate	<p>Proporciona autenticación de acceso Kerberos. La comunicación con el host se realiza en modo de sesión compartida.</p> <ol style="list-style-type: none"> Proporcione las credenciales de usuario. <ol style="list-style-type: none"> 1 Escriba el nombre de usuario para la sesión compartida en el cuadro de texto Nombre de usuario. 2 Escriba la contraseña para la sesión compartida en el cuadro de texto Contraseña. Escriba el servicio Kerberos SPN en el SPN de servicio Kerberos.

11 Haga clic en **Finalizar**.

Resultados

Ha añadido un servicio de SOAP. Los arquitectos de XaaS pueden usar XaaS para publicar flujos de trabajo del complemento de SOAP como elementos del catálogo y acciones personalizadas.

Configurar el complemento de vCenter Server como un endpoint

Puede añadir un endpoint y configurar el complemento de vCenter Server para conectarse a una instancia de vCenter Server en ejecución y crear blueprints de XaaS con el fin de administrar objetos de inventario de vSphere.

Requisitos previos

- Instale y configure vCenter Server. Consulte *Instalación y configuración de vSphere*.
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Configuración de vRO > Endpoints**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Seleccione **vCenter Server** en el menú desplegable **Complemento**.
- 4 Haga clic en **Siguiente**.

- 5 Especifique un nombre y, opcionalmente, una descripción.
- 6 Haga clic en **Siguiente**.
- 7 Proporcione información sobre la instancia de vCenter Server.
 - a Escriba la dirección IP o el nombre DNS de la máquina en el cuadro de texto **IP o nombre del host de la instancia de vCenter Server que añadir**.

Se trata de la dirección IP o el nombre DNS de la máquina donde está instalada la instancia de vCenter Server que desea añadir.
 - b Especifique el puerto para comunicarse con la instancia de vCenter Server en el cuadro de texto **Puerto de la instancia de vCenter Server**.

El puerto predeterminado es 443.
 - c Escriba la ubicación del SDK que se usará para conectarse a la instancia de vCenter Server en el cuadro de texto **Ubicación del SDK que usa para conectarse a la instancia de vCenter Server**.

Por ejemplo, `/sdk`.
- 8 Haga clic en **Siguiente**.
- 9 Defina los parámetros de conexión.
 - a Especifique el puerto HTTP de la instancia de vCenter Server en el cuadro de texto **Puerto HTTP de la instancia de vCenter Server, aplicable para el complemento de VC versión 5.5.2 o anterior**.
 - b Escriba las credenciales de vRealize Orchestrator que se usarán para establecer conexión con la instancia de vCenter Server en los cuadros de texto **Nombre del usuario que Orchestrator utilizará para conectarse a la instancia de vCenter Server** y **Contraseña del usuario que Orchestrator utilizará para conectarse a la instancia de vCenter Server**.

El usuario que seleccione debe ser válido y poseer privilegios para administrar extensiones de vCenter Server y un conjunto de privilegios definidos personalizados.
- 10 Haga clic en **Finalizar**.

Resultados

Ha añadido una instancia de vCenter Server como endpoint. Los arquitectos de XaaS pueden usar XaaS para publicar flujos de trabajo del complemento de vCenter Server como elementos del catálogo y acciones personalizadas.

Crear un endpoint de Microsoft Azure

Puede crear un endpoint de Microsoft Azure para facilitar una conexión con credenciales entre vRealize Automation y una implementación de Azure.

Un endpoint establece una conexión a un recurso (en este caso, una instancia de Azure) que puede utilizar para crear blueprints de máquina virtual. Debe tener un endpoint de Azure para usar como base de los blueprints para aprovisionar máquinas virtuales de Azure. Si cuenta con varias suscripciones a Azure, necesita endpoints para cada identificador de suscripción.

Opcionalmente, puede crear una conexión de Azure directamente desde vRealize Orchestrator utilizando el comando Agregar una conexión de Azure que se encuentra en **Biblioteca > Azure > Configuración** en el árbol de flujo de trabajo de vRealize Orchestrator. En la mayoría de los casos, la opción preferida es la creación de una conexión mediante la configuración del endpoint, tal como se describe en este documento.

Los endpoints de Azure son compatibles con la funcionalidad XaaS y vRealize Orchestrator. Puede crear, eliminar o editar un endpoint de Azure. Tenga en cuenta que si realiza cambios en un endpoint existente y no ejecuta ninguna actualización en el portal de Azure a través de la conexión actualizada por varias horas, debe reiniciar el servicio vRealize Orchestrator mediante el comando `service vco-service restart`. Si no reinicia el servicio, pueden producirse errores.

Requisitos previos

- Configure una instancia de Microsoft Azure y obtenga una suscripción válida a Microsoft Azure a partir de la que pueda usar el identificador de suscripción. Consulte <http://www.vaficionado.com/2016/11/using-new-microsoft-azure-endpoint-vrealize-automation-7-2/> para obtener más información sobre cómo configurar Azure y obtener un identificador de suscripción.
- Compruebe que la implementación de vRealize Automation tenga al menos un tenant y un grupo empresarial.
- Cree una aplicación de Active Directory tal como se describe en <https://azure.microsoft.com/es-es/documentation/articles/resource-group-create-service-principal-portal>.
- Tome nota de la siguiente información relacionada con Azure, ya que la necesitará durante la configuración del endpoint y el blueprint.
 - ID de suscripción
 - ID de tenant
 - nombre de la cuenta de almacenamiento
 - nombre del grupo de recursos
 - ubicación
 - nombre de la red virtual
 - identificador de la aplicación cliente
 - clave secreta de aplicación cliente
 - URN de imagen de la máquina virtual

- Existen ajustes exclusivos necesarios para crear e implementar las aplicaciones de nube de Azure en el entorno de China. Para obtener información relacionada, consulte <https://docs.microsoft.com/en-us/azure/china/china-get-started-developer-guide>. Al crear un endpoint de Azure de vRealize Automation para China, la URL del servicio, la URL de inicio de sesión y la URL de almacenamiento se deben especificar de la siguiente manera:

- URL de servicio: `https://management.chinacloudapi.cn`
- URL de inicio de sesión: `https://login.chinacloudapi.cn/`
- URL de almacenamiento: `https://storage_account_name.blob.core.chinacloudapi.cn/`

La implementación de Azure de vRealize Automation admite un subconjunto de regiones admitidas de Microsoft Azure. Consulte [Regiones admitidas de Azure](#).

- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Configuración de vRO > Endpoints**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 En la pestaña **Complemento**, haga clic en el menú desplegable **Complemento** y seleccione **Complemento Azure**.
- 4 Haga clic en **Siguiente**.
- 5 Especifique un nombre y, opcionalmente, una descripción.
- 6 Haga clic en **Siguiente**.
- 7 Rellene los cuadros de texto de la pestaña **Detalles** según corresponda para el endpoint.

Parámetro	Descripción
Configuración de conexión	
Conexión de Azure	
Nombre de la conexión	Nombre único para la nueva conexión de endpoint. Este nombre aparece en la interfaz de vRealize Orchestrator para ayudarle a identificar una conexión determinada.
Identificador de suscripción de Azure	Identificador de la suscripción de Azure. El identificador define las cuentas de almacenamiento, las máquinas virtuales y otros recursos de Azure a los que puede acceder.
Configuración del administrador de recursos	
URI del servicio Azure	El URI a través del cual obtiene acceso a la instancia de Azure. El valor predeterminado de <code>https://management.azure.com/</code> es apropiado para muchas implementaciones típicas.
URI de almacenamiento de Azure	El URI a través del cual se obtiene acceso a la instancia de almacenamiento de Azure.

Parámetro	Descripción
Identificador de tenant	El identificador de tenant de Azure que desea que use el endpoint.
Identificador del cliente	El identificador de cliente de Azure que desea que use el endpoint. Se asigna al crear una aplicación de Active Directory.
Secreto de cliente	La clave que se utiliza con un identificador de cliente de Azure. Esta clave se asigna al crear una aplicación de Active Directory.
URL de inicio de sesión	La URL que se usa para acceder a la instancia de Azure. El valor predeterminado de <code>https://login.windows.net/</code> es apropiado para muchas implementaciones típicas.
Configuración de proxy	
Host de proxy	Si su empresa utiliza un servidor web proxy, introduzca el nombre de host de dicho servidor.
Puerto de proxy	Si su empresa utiliza un servidor web proxy, introduzca el número de puerto de dicho servidor.

- 8 (opcional) Haga clic en **Propiedades** y agregue las propiedades personalizadas proporcionadas, los grupos de propiedades o sus propias definiciones de propiedades personalizadas.

- 9 Haga clic en **Finalizar**.

Pasos siguientes

Cree los grupos de recursos, las cuentas de almacenamiento y los grupos de seguridad de red adecuados en Azure. También debe crear equilibradores de carga si son apropiados para su implementación.

Acción	Opciones
Crear un grupo de recursos de Azure	<ul style="list-style-type: none"> ■ Cree el grupo de recursos desde el portal de Azure. Consulte la documentación de Azure para obtener instrucciones específicas. ■ Use el flujo de trabajo adecuado de vRealize Orchestrator, que se encuentra en <code>Library/Azure/Resource/Create resource group</code>. ■ En vRealize Automation, cree y publique un blueprint XaaS que contenga el flujo de trabajo de vRealize Orchestrator. Puede solicitar el grupo de recursos después de adjuntarlo al servicio y las autorizaciones. Tenga en cuenta que vRealize Automation no admite ni administra el tipo de recurso Grupo de recursos.
Crear una cuenta de almacenamiento de Azure	<ul style="list-style-type: none"> ■ Use Azure para crear una cuenta de almacenamiento. Consulte la documentación de Azure para obtener instrucciones específicas. ■ Use el flujo de trabajo adecuado de vRealize Orchestrator, que se encuentra en <code>Library/Azure/Storage/Create storage account</code>. ■ En vRealize Automation, cree y publique un blueprint XaaS que contenga el flujo de trabajo de vRealize Orchestrator. Puede solicitar la cuenta de almacenamiento después de adjuntarla al servicio y las autorizaciones.
Crear un grupo de seguridad de red de Azure	<ul style="list-style-type: none"> ■ Use Azure para crear un grupo de seguridad. Consulte la documentación de Azure para obtener instrucciones específicas. ■ Use el flujo de trabajo adecuado de vRealize Orchestrator, que se encuentra en <code>Library/Azure/Network/Create Network security group</code>. ■ En vRealize Automation, cree y publique un blueprint XaaS que contenga el flujo de trabajo de vRealize Orchestrator. Puede solicitar el grupo de seguridad después de adjuntarlo al servicio y las autorizaciones.

Regiones admitidas de Azure

La implementación de Azure de vRealize Automation admite un subconjunto de regiones admitidas de Microsoft Azure.

Las siguientes regiones de Azure son compatibles con la implementación de Azure en vRealize Automation.

■ Asia del Este	■ Este de Australia
■ Sudeste de Asia	■ Sudeste de Australia
■ Región Central de EE. UU.	■ Sur de India
■ Este de EE. UU.	■ Centro de India
■ Este de EE. UU. 2	■ Oeste de India
■ Oeste de EE. UU.	■ Centro de Canadá
■ Oeste de EE. UU. 2	■ Este de Canadá
■ Centro-norte de EE. UU.	■ Centro-oeste de EE. UU.
■ Centro-sur de EE. UU.	■ Centro de Corea
■ Europa del Norte	■ Sur de Corea
■ Europa Occidental	■ Oeste de Reino Unido
■ Oeste de Japón	■ Sur de Reino Unido
■ Este de Japón	■ Este de China
■ Sur de Brasil	■ Norte de China

Crear y configurar contenedores

Puede usar la pestaña Contenedores de vRealize Automation para abrir la aplicación integrada Contenedores para vRealize Automation y crear y ajustar la configuración de los contenedores y la red de contenedor a fin de que estén disponibles para los arquitectos de blueprint de vRealize Automation.

Puede definir contenedores usando plantillas e imágenes nuevas y existentes en la aplicación integrada Contenedores. A continuación, puede añadir tanto los componentes de contenedor como su configuración de red asociada a los blueprints de vRealize Automation.

Administrar hosts y clústeres de contenedor

Puede ver y administrar los hosts que añada desde la página Clústeres. En el contexto de Contenedores, el host es una máquina virtual o una infraestructura que le permite ejecutar contenedores.

La página Clústeres, la cual se encuentra en la pestaña Infraestructura, contiene los controles para añadir clústeres y hosts nuevos. Para añadir un host a un entorno de contenedores, debe añadirlo a un clúster. Puede supervisar el estado de las solicitudes de aprovisionamiento de los hosts existentes y ver los logs de eventos de los contenedores de cualquier página en las pestañas Biblioteca e Implementaciones. Los paneles Solicitudes y Log de eventos están situados en la parte derecha de las páginas.

Añadir un host de contenedor a un nuevo clúster

Para implementar contenedores, debe añadir un host a un clúster.

Requisitos previos

Seleccione un grupo empresarial en la parte superior izquierda de la pestaña Contenedores.

Procedimiento

- 1 Inicie sesión en la consola de vRealize Automation como **administrador de contenedores**.

- 2 Haga clic en la pestaña **Contenedores**.
- 3 Haga clic en **Infraestructura > Clústeres**.
- 4 Haga clic en **Nuevo**.
- 5 Introduzca un nombre para el clúster.
- 6 Introduzca una descripción para el clúster.
- 7 En **Tipo**, seleccione si ha introducido la dirección de un host de Docker o un host de contenedor virtual (Virtual Container Host, VCH).

Nota Solo los hosts VCH que tengan la versión 1.2 y 1.3 se admiten en los contenedores de vRealize Automation 7.4.

- 8 Introduzca la dirección IP o el nombre del host con el formato **http(s)://<nombre del host>:<puerto>**.
- 9 Seleccione las credenciales de inicio de sesión de la lista.

Contenedores admite la autenticación con credenciales y la autenticación con clave pública o privada. Puede añadir las credenciales desde la página **Administración de identidades**.
- 10 Haga clic en **Guardar**.

Resultados

Ha creado un nuevo clúster y ha añadido un host a él correctamente.

Usar políticas de implementación de contenedores

Puede vincular políticas de implementación con definiciones de hosts y de contenedores. Las políticas de implementación se utilizan en Contenedores para vRealize Automation para definir una preferencia por hosts y cuotas concretos al implementar un contenedor.

Las políticas de implementación que se aplican a un contenedor tienen mayor prioridad que las colocaciones que se aplican a los hosts de contenedor.

Nota Las políticas de implementación ya no se admiten y se quitarán de una versión futura de vRealize Automation.

Establecer una política de colocación en un host

Defina una preferencia por hosts y cuotas concretos al implementar un contenedor.

Nota Las políticas de implementación ya no se admiten y se quitarán de una versión futura de vRealize Automation.

Requisitos previos

Añada un host a un clúster.

Procedimiento

- 1 Inicie sesión en la consola de vRealize Automation como **administrador de contenedores**.
- 2 Haga clic en la pestaña **Contenedores**.
- 3 Haga clic en **Infraestructura > Clústeres**.
- 4 Haga clic en el clúster que contiene el host que desea editar.
- 5 Haga clic en **Recursos**.
- 6 Haga clic en el icono de opciones en el host que desea configurar y, a continuación, en **Editar**.
- 7 Seleccione la política de implementación y haga clic en **Actualizar**.

Establecer una política de implementación para una definición de contenedor

Establezca una política de implementación para una definición de contenedor.

Nota Las políticas de implementación ya no se admiten y se quitarán de una versión futura de vRealize Automation.

Procedimiento

- 1 Haga clic en la pestaña **Contenedores**.
- 2 Haga clic en **+Contenedor** para iniciar el aprovisionamiento del contenedor.
- 3 En las opciones de aprovisionamiento, haga clic en **Política**.
- 4 Seleccione una política existente de la lista desplegable **Política de implementación**.
- 5 Aprovisione el contenedor o guárdelo como una plantilla.

Configurar las opciones de contenedor

Puede definir una aplicación de varios contenedores o un solo contenedor utilizando propiedades y opciones de configuración de contenedor nuevas y existentes.

Además de la configuración básica de Contenedores para vRealize Automation, están disponibles las siguientes opciones de configuración de vRealize Automation para las implementaciones que emplean componentes de contenedor:

- Configuración del estado
- Vínculos
- Servicios expuestos
- Tamaño de clúster y parámetros de escalado vertical y horizontal

Configurar las comprobaciones de estado en Contenedores

Puede configurar un método de comprobación de estado para actualizar el estado de un contenedor según criterios personalizados.

Puede usar los protocolos HTTP o TCP al ejecutar un comando en el contenedor. También puede especificar un método de comprobación de estado.

Requisitos previos

- Compruebe que Contenedores para vRealize Automation esté activado en su implementación de vRealize Automation compatible.
- Compruebe que dispone de privilegios de función de **administrador de contenedores** o de **arquitecto de contenedores**.

Procedimiento

- 1 Inicie sesión en vRealize Automation.
- 2 Haga clic en la pestaña **Contenedores**.
- 3 Seleccione **Biblioteca > Plantillas** en el panel izquierdo.
- 4 Edite la plantilla o imagen.

Opción	Descripción
Para editar una plantilla	<ol style="list-style-type: none">a Haga clic en Editar en la parte superior derecha de la plantilla que desea abrir.b Haga clic en Editar en la parte superior derecha del contenedor que desea abrir.
Para editar una imagen.	Haga clic en la flecha situada junto al botón Aprovisionar de la imagen y, a continuación, haga clic en Introducir información adicional .

- 5 Haga clic en la pestaña **Configuración de estado**.

6 Seleccione un modo de estado.

Tabla 2-20. Modos de configuración de estado

Modo	Descripción
Ninguno	Predeterminado. No se configura ninguna comprobación de estado.
HTTP	<p>Si selecciona HTTP, debe proporcionar una API para acceder, así como el método y la versión de HTTP que se utilizarán. La API es relativa y no es necesario que introduzca la dirección del contenedor. También puede especificar un período de tiempo de espera para la operación y definir umbrales de estado.</p> <p>Por ejemplo, un umbral de buen estado con un valor de 2 significa que deben producirse dos llamadas consecutivas con éxito para que se considere que el contenedor está en buen estado y en ejecución (estado RUNNING). Un umbral de mal estado con un valor de 2 significa que deben producirse errores en dos llamadas para que se considere que el contenedor está en mal estado y en situación de error (estado ERROR). Para todos los casos intermedios entre los umbrales de buen estado y mal estado, el estado del contenedor es DEGRADED.</p>
Conexión TCP	Si selecciona Conexión TCP , solo debe especificar un puerto para el contenedor. La comprobación de estado intenta establecer una conexión TCP con el contenedor en el puerto indicado. También puede especificar un valor de tiempo de espera para la operación y definir umbrales de buen estado o de mal estado, al igual que con HTTP.
Comando	Si selecciona Comando , debe introducir el comando que se ejecutará en el contenedor. El estado de salida del comando determina el éxito de la comprobación de estado.
Omitir comprobación de estado en aprovisionamiento	Desactive esta opción para forzar la comprobación del estado durante el aprovisionamiento. Al hacerlo, no se considerará que un contenedor está aprovisionado hasta que supere correctamente una comprobación de estado.
AutoDeploy	Reimplementación automática de los contenedores cuando se encuentran en el estado ERROR.

7 Haga clic en **Guardar**.

Configurar vínculos en Contenedores

Los vínculos y los servicios expuestos dirigen la comunicación entre los servicios de contenedor y el equilibrio de carga entre hosts. Puede ajustar la configuración de los vínculos para los contenedores en Contenedores.

Puede utilizar vínculos para activar la comunicación entre varios servicios en la aplicación. Los vínculos de Contenedores son similares a los vínculos de Docker, pero conectan contenedores entre hosts. Un vínculo consta de dos partes: un nombre de servicio y un alias. El nombre de servicio es el nombre de la plantilla o del servicio invocados. El alias es el nombre de host que se utiliza para establecer una comunicación con ese servicio.

Por ejemplo, si dispone de una aplicación que contiene un servicio web y de base de datos, y define un vínculo del servicio web al servicio de base de datos mediante un alias de **my-db**, la aplicación de servicio web abre una conexión TCP a `my-db:{PORT_OF_DB}`. `PORT_OF_DB` es el puerto al que escucha la base de datos, independientemente del puerto público que la configuración del contenedor asigna al host. Si MySQL está buscando actualizaciones en el puerto predeterminado 3306, y el puerto publicado del host de contenedor es el 32799, la aplicación web accede a la base de datos en `my-db:3306`.

Nota Se recomienda utilizar redes en vez de vínculos. Los vínculos son ahora una característica antigua de Docker, con limitaciones significativas para vincular clústeres de contenedores, incluyendo las siguientes:

- Docker no admite varios vínculos con el mismo alias. Se recomienda permitir que Contenedores para vRealize Automation genere alias de vínculos por usted.
 - No es posible actualizar los vínculos de un tiempo de ejecución de contenedor. Al aumentar o reducir la escala de un clúster vinculado, los vínculos del contenedor dependiente no se actualizan.
-

Requisitos previos

- Compruebe que Contenedores para vRealize Automation esté activado en su implementación de vRealize Automation compatible.
- Compruebe que dispone de privilegios de función de **administrador de contenedores** o de **arquitecto de contenedores**.
- Compruebe que una red de puente esté disponible para vincular servicios.
- Compruebe que el puerto interno del servicio de destino esté publicado. Para comunicaciones cruzadas, el servicio puede asignarse a cualquier otro puerto, pero debe ser accesible desde fuera del host.
- Compruebe que los hosts de servicio tengan acceso mutuo.

Procedimiento

- 1 Inicie sesión en vRealize Automation.
- 2 Seleccione **Biblioteca > Plantillas** en el panel izquierdo.

3 Edite la plantilla o imagen.

Opción	Descripción
Para editar una plantilla	a Haga clic en Editar en la parte superior derecha de la plantilla que desea abrir. b Haga clic en Editar en la parte superior derecha del contenedor que desea abrir.
Para editar una imagen.	Haga clic en la flecha situada junto al botón Aprovisionar de la imagen y, a continuación, haga clic en Introducir información adicional .

4 Haga clic en la pestaña **Básica**.

5 En el cuadro de texto **Servicios**, escriba una lista de servicios separados por comas de los que depende el contenedor.

6 En el cuadro de texto **Alias**, escriba un nombre descriptivo del servicio o de la lista de servicios separados por comas.

7 Haga clic en **Guardar**.

Configurar servicios expuestos en Contenedores

Puede utilizar un nombre de host exclusivo para un equilibrador de carga indicando una dirección y un marcador de posición en la configuración del contenedor.

El marcador de posición determina la ubicación de una parte de la URL que se genera de manera automática. Este valor es único para cada nombre de host. La dirección admite el carácter de formato %s para especificar dónde se encuentra el marcador de posición.

Nota Si no se utiliza el marcador de posición, se coloca como prefijo o sufijo del nombre de host, en función de la configuración del sistema.

Si crea una aplicación que incluye un servicio que deba estar expuesto públicamente y que, de igual manera, deba escalarse de forma vertical y horizontal, se recomienda que emplee un equilibrador de carga que pueda dirigir solicitudes a cada nodo. Después de aprovisionar la aplicación, la configuración del equilibrador de carga se actualiza cada vez que vRealize Automation escala el servicio de manera vertical u horizontal.

Requisitos previos

- Compruebe que Contenedores para vRealize Automation esté activado en su implementación de vRealize Automation compatible.
- Compruebe que dispone de privilegios de función de **administrador de contenedores** o de **arquitecto de contenedores**.

Procedimiento

1 Inicie sesión en vRealize Automation.

2 Haga clic en la pestaña **Contenedores**.

3 Seleccione **Biblioteca > Plantillas** en el panel izquierdo.

4 Edite la plantilla o imagen.

Opción	Descripción
Para editar una plantilla	<p>a Haga clic en Editar en la parte superior derecha de la plantilla que desea abrir.</p> <p>b Haga clic en Editar en la parte superior derecha del contenedor que desea abrir.</p>
Para editar una imagen.	Haga clic en la flecha situada junto al botón Aprovisionar de la imagen y, a continuación, haga clic en Introducir información adicional .

5 Haga clic en la pestaña **Red**.

6 En el cuadro de texto **Dirección**, escriba la ubicación del marcador de posición.

El host de direcciones actúa como host virtual. Para acceder al host de direcciones, puede añadir información de asignación al archivo etc/hosts o utilizar un DNS que asigne la dirección del contenedor al nombre del host.

7 En el cuadro de texto **Puerto de contenedor**, escriba el número de puerto utilizado para exponer el servicio.

Utilice el formato de muestra que se proporciona en el formulario. Si su aplicación de contenedor expone más de un puerto, especifique los puertos internos que podrán exponer el servicio.

8 Haga clic en **Guardar**.

Configurar el tamaño de clúster y el escalado en Contenedores

Puede crear clústeres de contenedores mediante la configuración de colocación de Contenedores para especificar el tamaño de clúster.

Cuando configura un clúster, Contenedores aprovisiona el número especificado de contenedores. Las cargas de las solicitudes se equilibran entre todos los contenedores del clúster.

Puede modificar el tamaño de clúster en un contenedor o una aplicación aprovisionados para aumentar o reducir el tamaño del clúster en una unidad. Cuando modifica el tamaño de clúster en tiempo de ejecución, se tienen en cuenta todos los filtros de afinidad y las reglas de colocación.

Requisitos previos

- Compruebe que Contenedores para vRealize Automation esté activado en su implementación de vRealize Automation compatible.
- Compruebe que dispone de privilegios de función de **administrador de contenedores** o de **arquitecto de contenedores**.

Procedimiento

1 Inicie sesión en vRealize Automation.

- 2 Haga clic en la pestaña **Contenedores**.
- 3 Seleccione **Biblioteca > Plantillas** en el panel izquierdo.
- 4 Edite la plantilla o imagen.

Opción	Descripción
Para editar una plantilla	<ol style="list-style-type: none"> a Haga clic en Editar en la parte superior derecha de la plantilla que desea abrir. b Haga clic en Editar en la parte superior derecha del contenedor que desea abrir.
Para editar una imagen.	Haga clic en la flecha situada junto al botón Aprovisionar de la imagen y, a continuación, haga clic en Introducir información adicional .

- 5 Haga clic en la pestaña **Política**.
- 6 Defina el tamaño del clúster del contenedor.
- 7 Haga clic en **Guardar**.

Configurar y usar plantillas e imágenes en Contenedores

Contenedores utiliza plantillas para aprovisionar contenedores.

Una plantilla es una configuración reutilizable para aprovisionar un contenedor o un conjunto de contenedores. En una plantilla, puede definir una aplicación de varios niveles que consta de servicios vinculados.

Un servicio se define como uno o varios contenedores del mismo tipo o imagen.

Puede crear una plantilla de contenedores personalizada con base en una plantilla existente en la página **Plantillas** o importar un archivo YAML con el formato correcto. También puede aprovisionar una imagen o una plantilla de contenedores.

Crear una plantilla de contenedor personalizada

Puede crear una plantilla personalizada y utilizarla para definir un contenedor.

Una plantilla es una configuración reutilizable que puede utilizar para aprovisionar un contenedor o un conjunto de contenedores.

La página Plantillas muestra imágenes de plantilla disponibles de acuerdo con los registros que ha definido. Puede crear una plantilla personalizada a partir de una imagen de plantilla existente, o bien puede importar un archivo de plantilla o de Docker Compose. Consulte [Importar una plantilla de contenedor o un archivo de Docker Compose](#).

También puede crear una plantilla o una imagen personalizadas usando la opción **Aprovisionar > Introducir información adicional** que se describe en [Aprovisionar un contenedor desde una plantilla o una imagen](#).

Requisitos previos

- Compruebe que dispone de privilegios de función de **administrador de contenedores**.

Procedimiento

- 1 Inicie sesión en la consola de vRealize Automation como **administrador de contenedores**.
- 2 Haga clic en la pestaña **Contenedores**.
- 3 Seleccione **Biblioteca > Plantillas** en el panel izquierdo.

En una lista se muestran las plantillas y las imágenes disponibles para el aprovisionamiento.

- Plantillas configuradas en la vista **Imágenes**.
- Plantillas existentes o personalizadas en la vista **Plantilla**.
- Todas las plantillas y las imágenes disponibles basadas en los registros que haya especificado en la vista **Todo**.

Las opciones **Importar** y **Exportar** también están disponibles para la importación o la exportación de plantillas e imágenes.

- 4 Haga clic en la flecha situada junto al botón **Aprovisionar** de una imagen que desee incluir en la plantilla.
- 5 Haga clic en **Introducir información adicional**.
- 6 Haga clic en **Guardar como plantilla** para guardar los cambios como una nueva plantilla de contenedor en Contenedores para vRealize Automation.

Pasos siguientes

Puede editar una plantilla para un futuro aprovisionamiento. Las aplicaciones existentes que se han aprovisionado a partir de la plantilla no se ven afectadas por los cambios que realice en la plantilla después del aprovisionamiento.

Importar una plantilla de contenedor o un archivo de Docker Compose

Puede usar una plantilla de contenedor de Docker importada o un archivo YAML de Docker Compose como plantilla personalizada en Contenedores para vRealize Automation.

Si utiliza un archivo YAML, especifique el contenido del archivo YAML como texto, o busque y cargue el archivo YAML. El archivo YAML representa la plantilla, la configuración de los diferentes contenedores y sus conexiones. Los tipos de formato admitidos son Docker Compose YAML y YAML de Contenedores para vRealize Automation.

El archivo YAML de Contenedores para vRealize Automation es similar a Docker Compose, pero utiliza el formato YAML del blueprint de vRealize Automation visible en la API de REST de vRealize Automation o en vRealize CloudClient. El archivo YAML de Contenedores para vRealize Automation permite importar las aplicaciones de Docker Compose existentes y modificarlas, aprovisionarlas y administrarlas utilizando Contenedores.

Requisitos previos

- Compruebe que Contenedores para vRealize Automation esté activado en su implementación de vRealize Automation compatible.

- Inicie sesión en vRealize Automation como **administrador de contenedores**.

Para obtener información sobre el formato YAML utilizado por las REST API de servicio de vRealize Automation, consulte *Referencia de la API de vRealize Automation*.

Procedimiento

- 1 Haga clic en la pestaña **Contenedores**.

- 2 Seleccione **Biblioteca > Plantillas** en el panel izquierdo.

En una lista se muestran las plantillas y las imágenes disponibles para el aprovisionamiento.

- Plantillas configuradas en la vista Imágenes.
- Plantillas existentes o personalizadas en la vista **Plantilla**.
- Todas las plantillas y las imágenes disponibles basadas en los registros que haya especificado en la vista **Todo**.

Las opciones **Importar** y **Exportar** también están disponibles para la importación o la exportación de plantillas e imágenes.

- 3 Haga clic en el icono **Importar plantilla o Docker Compose**.

Se abrirá la página Importar plantilla.

- 4 Indique el contenido del archivo YAML.

Opción	Descripción
Cargar desde archivo	Haga clic en Cargar desde archivo para buscar y seleccionar el archivo YAML en un directorio.
Introducir plantilla o Docker Compose	Pegue el contenido de un archivo YAML con el formato correcto en el cuadro de texto Introducir plantilla o Docker Compose .

- 5 Haga clic en **Importar**.

La nueva plantilla aparecerá en la vista **Plantillas**.

Aprovisionar un contenedor desde una plantilla o una imagen

Puede aprovisionar un contenedor desde una plantilla o una imagen en la vista Plantillas.

El proceso de aprovisionamiento crea un contenedor basado en la configuración que existe en la plantilla o la imagen a partir de las que aprovisiona.

Para aprovisionar un contenedor desde una plantilla o una imagen, puede utilizar la configuración existente o editar la configuración y, a continuación, realizar el aprovisionamiento.

También puede editar y guardar la configuración para crear nuevas plantillas o imágenes de contenedor personalizadas.

Requisitos previos

- Compruebe que Contenedores para vRealize Automation esté activado en su implementación de vRealize Automation compatible.
- Inicie sesión en vRealize Automation como **administrador de contenedores**.

Procedimiento

- 1 Haga clic en la pestaña **Contenedores**.

- 2 Seleccione **Biblioteca > Plantillas** en el panel izquierdo.

En una lista se muestran las plantillas y las imágenes disponibles para el aprovisionamiento.

- Plantillas configuradas en la vista **Imágenes**.
- Plantillas existentes o personalizadas en la vista **Plantilla**.
- Todas las plantillas y las imágenes disponibles basadas en los registros que haya especificado en la vista **Todo**.

Las opciones **Importar** y **Exportar** también están disponibles para la importación o la exportación de plantillas e imágenes.

- 3 Use las opciones de vista **Todo**, **Imágenes** o **Plantillas** para ver la imagen o la plantilla que se aprovisionará.
- 4 Aprovisione la plantilla o la imagen.

Opción	Descripción
Aprovisionar la configuración existente.	<p>a Haga clic en Aprovisionar.</p> <p>La vista Solicitudes de aprovisionamiento muestra información sobre el aprovisionamiento correcto.</p>
Aprovisionamiento por edición de configuración.	<p>a Haga clic en la flecha que se encuentra junto al botón Aprovisionar.</p> <p>b Haga clic en Introducir información adicional.</p> <p>c Introduzca la información adicional del contenedor en el formulario Aprovisionar un contenedor.</p> <p>d Cuando haya completado las actualizaciones del formulario, haga clic en Aprovisionar para realizar el aprovisionamiento mediante la configuración modificada.</p> <p>e Haga clic en Guardar como plantilla para guardar los cambios como una nueva plantilla de contenedor en Contenedores para vRealize Automation.</p> <p>La vista Solicitudes de aprovisionamiento muestra información sobre el aprovisionamiento correcto.</p>

Exportar una plantilla de contenedor o un archivo de Docker Compose

Puede exportar una plantilla de contenedor como un archivo YAML de Docker Compose o un archivo YAML de Contenedores para vRealize Automation.

Puede importar una plantilla, modificarla mediante programación utilizando la API de REST de vRealize Automation o vRealize CloudClient, o modificarla de forma gráfica en Contenedores. A continuación, puede exportar el archivo modificado. Por ejemplo, puede importar un formato de Docker Compose y exportarlo en el formato YAML de blueprint utilizado en la API de servicio de composición de vRealize Automation. Sin embargo, algunas configuraciones específicas de Contenedores, como la configuración de estado y las restricciones de afinidad, no se incluyen si exporta la plantilla en formato de Docker Compose.

Requisitos previos

- Compruebe que Contenedores para vRealize Automation esté activado en su implementación de vRealize Automation compatible.
- Inicie sesión en vRealize Automation como **administrador de contenedores**.

Para obtener información sobre el formato YAML utilizado por las REST API de servicio de vRealize Automation, consulte *Referencia de la API de vRealize Automation*.

Procedimiento

1 Haga clic en la pestaña **Contenedores**.

2 Seleccione **Biblioteca > Plantillas** en el panel izquierdo.

En una lista se muestran las plantillas y las imágenes disponibles para el aprovisionamiento.

- Plantillas configuradas en la vista Imágenes.
- Plantillas existentes o personalizadas en la vista **Plantilla**.
- Todas las plantillas y las imágenes disponibles basadas en los registros que haya especificado en la vista **Todo**.

Las opciones **Importar** y **Exportar** también están disponibles para la importación o la exportación de plantillas e imágenes.

3 Coloque el puntero sobre una plantilla y haga clic en el icono **Exportar**.

4 Cuando se le solicite, seleccione un tipo de formato de salida:

- **Blueprint con formato YAML**

Este formato es compatible con el formato YAML de blueprint utilizado en la API de servicio de composición de vRealize Automation.

- **Docker Compose**

Este formato es compatible con el formato YAML utilizado en la aplicación Docker Compose.

5 Haga clic en **Exportar**.

6 Guarde el archivo o ábralo con una aplicación adecuada cuando se le solicite.

Usar registros de contenedor

Un registro de Docker es una aplicación sin estado del lado servidor. Puede utilizar los registros en Contenedores para vRealize Automation para almacenar y distribuir imágenes de Docker.

Para configurar un registro, debe proporcionar su dirección, un nombre de registro personalizado y, de forma opcional, credenciales. Para establecer si el registro es seguro o no, la dirección debe comenzar por HTTP o HTTPS. Si no se indica el tipo de conexión, se utiliza HTTPS de forma predeterminada.

Nota Para HTTP se debe declarar el puerto 80, mientras que para HTTPS se debe declarar el 443. Si no se especifica ningún puerto, el motor de Docker espera el puerto 5000, lo que puede causar interrupciones en la conexión.

Nota Ya que este protocolo no se considera seguro, no es recomendable que utilice registros HTTP. Si desea utilizar HTTP, debe modificar la propiedad `DOCKER_OPTS` en cada host del modo siguiente:

```
DOCKER_OPTS="--insecure-registry myregistrydomain.com:5000".
```

Para obtener más información, consulte la documentación de Docker en <https://docs.docker.com/registry/insecure/>.

Contenedores puede relacionarse con registros HTTP API V1 y V2 de Docker de la siguiente manera:

V1 en HTTP (registro HTTP simple y no seguro)

Puede realizar búsquedas en esta clase de registro libremente, pero debe configurar de forma manual cada host Docker con la marca `--insecure-registry` para aprovisionar contenedores basados en imágenes desde registros inseguros. Debe reiniciar el daemon de Docker después de establecer la propiedad.

V1 en HTTPS

Utilícelo detrás de un proxy inverso, como NGINX. La implementación estándar está disponible mediante código abierto en <https://github.com/docker/docker-registry>.

V2 en HTTPS

La implementación estándar se ofrece como código abierto en <https://github.com/docker/distribution>.

V2 en HTTPS con autenticación básica

La implementación estándar se ofrece como código abierto en <https://github.com/docker/distribution>.

V2 en HTTPS con autenticación mediante un servicio central

Puede ejecutar un registro de Docker en modo independiente, en el cual no se realizan comprobaciones de autorización. JFrog Artifactory y Harbor son registros de terceros

compatibles. Docker Hub está habilitado de manera predeterminada para todos los tenants y no está presente en la lista de registros, pero se puede desactivar con una propiedad del sistema.

Nota Normalmente, Docker no interactúa con registros seguros que se han configurado con certificados firmados por una autoridad desconocida. El servicio de contenedor resuelve esta situación cargando de forma automática los certificados que no son de confianza en todos los hosts Docker y habilitando los hosts para que se conecten con estos registros. Si no se puede cargar un certificado en un host concreto, el host se desactiva automáticamente.

Crear y administrar registros de contenedores

Puede configurar varios registros para acceder tanto a imágenes públicas como a imágenes privadas.

Los registros son almacenes públicos o privados en los cuales se cargan imágenes o bien desde los que se descargan. Puede desactivar, editar o eliminar los registros que haya creado. Las imágenes que se muestran en la pestaña **Plantillas** se basan en los registros que haya definido.

Al crear o administrar registros en la página Registros existentes, puede hacer clic en los botones **Credenciales** o **Certificado** para añadir o administrar credenciales y certificados.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de contenedores**.
- Compruebe que exista al menos un host configurado y que esté disponible para la configuración de red de contenedor.

Procedimiento

- 1 Haga clic en la pestaña **Contenedores**.
- 2 Haga clic en **Registros**.
Se abrirá la página Registros existentes.
- 3 Haga clic en **+Registro**.
- 4 Introduzca la dirección del registro.
- 5 Escriba un nombre para el registro.
- 6 Seleccione las credenciales de inicio de sesión de la lista desplegable.
- 7 (opcional) Haga clic en **Verificar** para confirmar que los parámetros configurados son válidos.
- 8 Haga clic en **Guardar** para añadir el registro.

Configurar recursos de red para contenedores

Puede crear, modificar y adjuntar configuraciones de red para contenedores y plantillas de contenedores en la aplicación Contenedores para vRealize Automation.

Cuando aprovisiona un contenedor, la configuración de red está integrada y disponible. Puede personalizar la configuración de red para los componentes de contenedor que ha añadido a un blueprint de vRealize Automation.

Crear una nueva red para los contenedores

Si ninguna configuración de red adecuada está disponible, puede crear una nueva en vRealize Automation.

Requisitos previos

- Compruebe que dispone de privilegios de función de **administrador de contenedores**, de **arquitecto de contenedores** o de **administrador de IaaS**.
- Compruebe que exista al menos un host configurado y que esté disponible para la configuración de red de contenedor.

Procedimiento

- 1 Inicie sesión en vRealize Automation.
- 2 Haga clic en la pestaña **Contenedores**.
- 3 Seleccione **Implementaciones > Redes** en el panel izquierdo.

El panel principal muestra las configuraciones de red existentes que pueden aprovisionarse como parte de la implementación de contenedores. Las configuraciones de red incluyen tanto las que se han recopilado a partir de hosts Docker añadidos como las que se han creado en vRealize Automation. Los iconos que representan las configuraciones de red muestran los controladores de red y de IPAM, la información de subred, la puerta de enlace y el rango de IP, el número de contenedores que usan la configuración de la red, y el número de hosts.

- 4 Haga clic en **+Red**.
- 5 Escriba un nombre para la red.

Cuando termine de crear la nueva configuración, se adjuntará un identificador único al valor de nombre.

- 6 (opcional) Para añadir ajustes de configuración más detallados, active la casilla **Avanzado**. Aparecen opciones de configuración de red adicionales en el panel Añadir red.

7 Configure las opciones de configuración avanzada de red.

Opción	Descripción
Configuración de IPAM	<p>Subred</p> <p>Proporcione direcciones de subred y puerta de enlace exclusivos de esta configuración de red. No deben superponerse con los de ninguna otra red del mismo host de contenedor.</p>
Propiedades personalizadas	<p>Opcionalmente, especifique propiedades personalizadas para la nueva configuración de red.</p> <p>containers.ipam.driver</p> <p>Solo se puede utilizar con contenedores. Especifica el controlador de IPAM que se usará cuando se añada un componente de red de Contenedores a un blueprint. Los valores admitidos dependen de los controladores que están instalados en el entorno de host de contenedor en el que se utilizan. Por ejemplo, según los complementos de IPAM que estén instalados en el host de contenedor, un valor admitido podría ser <code>infoblox</code> o <code>calico</code>.</p> <p>El nombre y el valor de la propiedad distinguen mayúsculas de minúsculas. El valor de la propiedad no está validado cuando lo añade. Si el controlador especificado no existe en el host de contenedor al realizar el aprovisionamiento, aparecerá un mensaje de error y el aprovisionamiento no se realizará correctamente.</p> <p>containers.network.driver</p> <p>Solo se puede utilizar con contenedores. Especifica el controlador de red que se empleará cuando se añada un componente de red de Contenedores a un blueprint. Los valores admitidos dependen de los controladores que están instalados en el entorno de host de contenedor en el que se utilizan. De forma predeterminada, los controladores de red suministrados por Docker incluyen <code>bridge</code>, <code>overlay</code> y <code>macvlan</code>, mientras que los controladores de red proporcionados por el host de contenedor virtual (Virtual Container Host, VCH) incluyen el controlador <code>bridge</code>. También puede que estén disponibles controladores de red de terceros, como <code>weave</code> y <code>calico</code>, en función de los complementos de red que estén instalados en el host de contenedor.</p> <p>El nombre y el valor de la propiedad distinguen mayúsculas de minúsculas. El valor de la propiedad no está validado cuando lo añade. Si el controlador especificado no existe en el host de contenedor al realizar el aprovisionamiento, aparecerá un mensaje de error y el aprovisionamiento no se realizará correctamente.</p>

Nota Si crea la red sin usar la configuración avanzada, vRealize Automation proporciona la configuración automáticamente.

8 En el menú desplegable, seleccione el host al que desea conectar la red.

9 Haga clic en **Crear**.

Añadir una red a una plantilla de contenedor

Puede añadir una configuración de red a una plantilla de contenedor para conectar los contenedores entre sí. Esta configuración de red se implementa automáticamente para todas las aplicaciones que usan la plantilla. Puede añadir una red existente, o bien configurar y añadir una nueva red como corresponda.

Requisitos previos

- Compruebe que haya una plantilla disponible. Si no es así, primero debe crear una.
- Compruebe que dispone de privilegios de función de **administrador de contenedores**, de **arquitecto de contenedores** o de **administrador de IaaS**.
- Compruebe que exista al menos un host configurado y que esté disponible para la configuración de red de contenedor.

Procedimiento

- 1 Inicie sesión en vRealize Automation.
- 2 Haga clic en la pestaña **Contenedores**.
- 3 Haga clic en **Plantillas** en el panel izquierdo.
Una matriz de iconos muestra las plantillas y las imágenes disponibles para el aprovisionamiento.
- 4 (opcional) Modifique la vista de manera que solo se muestren las plantillas haciendo clic en **Vista: Plantillas** en el encabezado superior derecho que se encuentra sobre los iconos.
- 5 Haga clic en **Editar** en la parte superior derecha de la plantilla que desea personalizar.
Se abrirá la página Editar plantilla, que muestra los iconos del contenedor y un icono en blanco con el signo más.
- 6 Apunte al icono en blanco.
Aparece el icono **Añadir red**.
- 7 Haga clic en el icono **Añadir red**.
Se abrirá el panel Añadir red.

8 Agregue una red existente, o bien cree y añada una red nueva.

Opción	Descripción
Añada una red existente.	<ul style="list-style-type: none"> a Haga clic en la casilla de verificación Existente. b Haga clic dentro del campo Nombre para mostrar una lista con las redes existentes. c Seleccione la red que quiera utilizar y haga clic en Guardar.
Configure y añada una nueva red.	<ul style="list-style-type: none"> a Escriba un nombre para la red. b Para añadir ajustes de configuración más detallados, haga clic en la casilla de verificación Avanzado. c Haga clic en Guardar.

El panel Añadir configuración de red desaparece y la red añadida se muestra como un icono horizontal bajo los iconos del contenedor de la página Editar plantilla. También se muestra un icono de red en el borde inferior de los iconos del contenedor.

9 Conecte la red a un contenedor. Para ello, arrastre el icono del conector de red del contenedor a un punto del icono horizontal que representa la red.

Configuración de volúmenes para contenedores

Puede crear, modificar y adjuntar volúmenes para contenedores y plantillas de contenedores en la aplicación Contenedores para vRealize Automation.

Contenedores para vRealize Automation usa volúmenes de Docker para la administración de datos persistentes. Con los volúmenes, puede realizar las siguientes tareas:

- Compartir volúmenes entre diferentes contenedores dentro del mismo host.
- Actualizar datos al instante.
- Guardar los datos de volumen después de eliminar el contenedor.

Crear un nuevo volumen para los contenedores

Para ampliar el almacenamiento de contenedores, primero debe crear un volumen de datos.

Requisitos previos

- Compruebe que dispone de privilegios de función de **administrador de contenedores**, de **arquitecto de contenedores** o de **administrador de IaaS**.
- Compruebe que hay al menos un host configurado y que está disponible para la configuración de volumen de contenedor.

Procedimiento

- 1 Inicie sesión en vRealize Automation.
- 2 Haga clic en la pestaña **Contenedores**.

3 Seleccione **Implementaciones > Volúmenes** en el panel izquierdo.

El panel principal muestra las configuraciones de volumen existentes que se pueden conectar a los contenedores implementados. Estas configuraciones de volumen incluyen tanto las que se han recopilado a partir de hosts de Docker añadidos como las que se han creado en vRealize Automation. Las instancias de volumen muestran el controlador, el ámbito y las opciones de controlador.

4 Haga clic en **+Volumen**.

5 Escriba un nombre para el volumen.

Cuando se completa la creación de la configuración, se adjunta un identificador único al valor de nombre.

6 En el cuadro de texto **Controlador**, introduzca el controlador del complemento de volumen que desea utilizar. Si no introduce nada, se utiliza local como el valor predeterminado.

7 (opcional) Para añadir ajustes de configuración más detallados, haga clic en la casilla de verificación **Avanzado**.

Se muestran opciones de configuración adicionales.

8 (opcional) Establezca la configuración avanzada de volúmenes.

Opción	Descripción
Opciones del controlador	Especifique las opciones de controlador que desea utilizar. Las opciones varían según el complemento de volumen que se está utilizando.
Propiedades personalizadas	Especifique propiedades personalizadas para la nueva configuración.

9 En el menú desplegable, seleccione el host al que desea conectar el volumen.

10 Haga clic en **Crear**.

El panel Crear volumen desaparecerá y el volumen añadido aparecerá en la pestaña Volúmenes.

Pasos siguientes

[Añadir un volumen a una plantilla de contenedor](#)

Añadir un volumen a una plantilla de contenedor

Agregue un volumen a una plantilla para conectarlo a un contenedor.

Requisitos previos

- Compruebe que haya una plantilla disponible. Si no es así, primero debe crear una.
- Compruebe que dispone de privilegios de función de **administrador de contenedores**, de **arquitecto de contenedores** o de **administrador de IaaS**.
- Compruebe que hay al menos un host configurado y que está disponible para la configuración de volumen de contenedor.

Procedimiento

1 Inicie sesión en vRealize Automation.

2 Haga clic en la pestaña **Contenedores**.

3 Haga clic en **Plantillas** en el panel izquierdo.

Una matriz de iconos muestra las plantillas y las imágenes disponibles para el aprovisionamiento.

4 (opcional) Modifique la vista de manera que solo se muestren las plantillas haciendo clic en **Vista: Plantillas** en el encabezado superior derecho que se encuentra sobre los iconos.

5 Haga clic en **Editar** en la parte superior derecha de la plantilla que desea personalizar.

Se abrirá la página Editar plantilla, que muestra los iconos del contenedor, incluido un icono en blanco con el signo más.

6 Coloque el cursor sobre el icono en blanco con el signo más hasta que se muestre el icono **Añadir volumen**.

7 Haga clic en el icono **Añadir volumen**.

8 Añada un volumen existente, o bien cree y añada un volumen nuevo.

Opción	Descripción
Añada un volumen existente.	<p>a Haga clic en la casilla de verificación Existente.</p> <p>b Haga clic dentro del campo Nombre para ver una lista de los volúmenes existentes.</p> <p>c Seleccione el volumen que desee utilizar y haga clic en Guardar.</p>
Configure y añada un nuevo volumen.	<p>a Escriba un nombre para el volumen.</p> <p>b En el cuadro de texto Controlador, introduzca el controlador del complemento de volumen que desea utilizar. Si no utiliza un sistema de almacenamiento externo, escriba local.</p> <p>c Para añadir ajustes de configuración más detallados, haga clic en la casilla de verificación Avanzado.</p> <p>d Haga clic en Guardar.</p>

El panel Añadir volumen desaparece y el volumen añadido se muestra como un icono horizontal bajo los iconos del contenedor en la página Editar plantilla. También se muestra un icono de volumen en el borde inferior de los iconos del contenedor.

9 Conecte el volumen a un contenedor. Para ello, arrastre el icono del conector de volumen desde el contenedor hasta un punto del icono horizontal que representa el volumen.

10 (opcional) Haga clic en la ruta de acceso del contenedor para cambiar la ubicación donde se encuentra montado el volumen.

Pasos siguientes

[Aprovisionar un contenedor desde una plantilla o una imagen](#)

Instalar complementos adicionales en el servidor predeterminado de vRealize Orchestrator

Puede instalar complementos y paquetes adicionales en el servidor de vRealize Orchestrator predeterminado mediante la interfaz de configuración de vRealize Orchestrator.

Puede instalar complementos adicionales en el servidor de vRealize Orchestrator predeterminado y utilizar los flujos de trabajo con XaaS.

También puede importar paquetes adicionales en el servidor de vRealize Orchestrator predeterminado para configurarlos como tipos de endpoints de proveedores de IPAM externos de vRealize Automation. Para obtener información sobre cómo obtener, importar y configurar el paquete Infoblox IPAM, consulte [Lista de comprobación para proporcionar soporte técnico del proveedor de IPAM de terceros](#).

Los archivos de paquete (.package) y los archivos de instalación de complementos (.vmoapp o .dar) están disponibles en VMware Solution Exchange en https://solutionexchange.vmware.com/store/category_groups/cloud-management. Para obtener información sobre los archivos de complemento, consulte la documentación sobre complementos de vRealize Orchestrator en https://www.vmware.com/support/pubs/vco_plugins_pubs.html.

Para obtener más información sobre cómo instalar nuevos complementos, consulte el tema de *instalación y configuración de VMware vCenter Orchestrator*.

Trabajar con políticas de Active Directory

Las políticas de Active Directory definen las propiedades de un registro de máquina; por ejemplo, un dominio, así como la unidad organizativa en la que el registro se crea mediante un blueprint de vRealize Automation.

Si aplica una política a un grupo empresarial, todas las solicitudes de máquinas que provengan de los miembros de ese grupo se añaden a la unidad organizativa especificada. Puede crear diferentes políticas para diversas unidades organizativas y, después, aplicar las diferentes políticas a diversos grupos empresariales.

Utilizar propiedades personalizadas para reemplazar una política de Active Directory

Al utilizar las propiedades personalizadas de Active Directory que se proporcionan, puede reemplazar la política de Active Directory, el dominio, la unidad organizativa y otros valores en un blueprint particular cuando se implemente.

La lista de las propiedades personalizadas de Active Directory que se proporcionan se incluye en la *Referencia de propiedades personalizadas*. El prefijo de las propiedades personalizadas es `ext.policy.activedirectory`.

Además de las propiedades proporcionadas, puede crear las suyas propias personalizadas. Debe añadir el prefijo a las propiedades personalizadas con `ext.policy.activedirectory`. Por ejemplo, `ext.policy.activedirectory.domain.extension` o `ext.policy.activedirectory.yourproperty`. Las propiedades pasan a sus flujos de trabajo personalizados de Active Directory de vRealize Orchestrator.

Para obtener más información sobre las propiedades personalizadas, consulte *Referencia de propiedades personalizadas*. Según cuáles sean los valores que está reemplazando, podría necesitar crear una definición de propiedades. Por ejemplo, podría crear una definición de propiedades que recupere las políticas de Active Directory disponibles desde vRealize Automation. Igualmente, podría crear una definición que permita al usuario solicitante seleccionar entre dos o más unidades organizativas alternativas. Consulte *Referencia de propiedades personalizadas*.

Crear y aplicar políticas de Active Directory

Cree una o varias políticas de Active Directory para que pueda asignarlas a diferentes grupos empresariales. Puede utilizar las diferentes políticas para añadir registros de máquinas a diversas unidades empresariales basadas en la pertenencia a estos.

En caso necesario, puede reemplazar la política de Active Directory asignada.

Procedimiento

1 Crear una política de Active Directory

Puede crear una política de Active Directory para definir dónde se van a añadir los registros en una instancia de Active Directory cuando los usuarios implementen máquinas. Puede asignar una política a un grupo empresarial de manera que todas las máquinas que implementen los miembros de ese grupo resulten en un registro creado en la unidad organizativa especificada.

2 Escenario: Añadir una propiedad personalizada a blueprints para reemplazar una política de Active Directory

Como arquitecto de blueprints para el grupo empresarial de desarrollo, tiene un blueprint que incluye una máquina de aplicaciones y una máquina de bases de datos, y desea que el registro de la máquina de bases de datos se añada a una unidad organizativa que sea diferente a la política de Active Directory aplicada.

Crear una política de Active Directory

Puede crear una política de Active Directory para definir dónde se van a añadir los registros en una instancia de Active Directory cuando los usuarios implementen máquinas. Puede asignar una política a un grupo empresarial de manera que todas las máquinas que implementen los miembros de ese grupo resulten en un registro creado en la unidad organizativa especificada.

Cree diferentes políticas de Active Directory cuando quiera que las máquinas que implementen distintos grupos empresariales tengan diferentes dominios o que se añadan a diferentes instancias de Active Directory.

Requisitos previos

- Compruebe que ha creado un endpoint de Active Directory. Consulte [Configurar el complemento Active Directory como un endpoint](#).
- Si usa un servidor de vRealize Orchestrator externo, verifique que esté configurado correctamente. Consulte [Configurar un servidor de vRealize Orchestrator externo](#).
- Inicie sesión en vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Seleccione **Administración > Políticas de AD**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Configure los detalles de las políticas de Active Directory.

Opción	Descripción
ID	<p>Introduzca el valor permanente.</p> <p>El valor no puede incluir espacios ni caracteres especiales.</p> <p>No podrá cambiar este valor más adelante. Solo podrá recrear la política con otro identificador.</p>
Descripción	Describa la política.
Endpoint de Active Directory	Seleccione el endpoint de Active Directory para el cual se crea esta política.
Dominio	Introduzca el dominio raíz. El formato es <i>mycompany.com</i> .
Unidad organizativa	<p>Introduzca el nombre distintivo de la unidad organizativa para esta política.</p> <p>Se debe introducir la jerarquía como una lista separada por comas. Por ejemplo, <i>ou=development,dc=corp,dc=domain,dc=com</i>.</p>

- 4 Haga clic en **Aceptar**.

Resultados

El endpoint de Active Directory de vRealize Orchestrator se añade a la lista. Puede aplicar la política en grupos empresariales o utilizar la política en blueprints o grupos empresariales.

Pasos siguientes

- Para proporcionar varias opciones de políticas, cree más políticas.
- Para añadir registros a Active Directory con base en la pertenencia a grupos empresariales cuando un blueprint se implementa, añada la política de Active Directory apropiada a un grupo empresarial. Consulte [Crear un grupo empresarial](#). Puede aplicar la política cuando cree el grupo empresarial, o bien puede hacerlo más adelante.
- Para reemplazar la política de Active Directory para el grupo empresarial de un blueprint particular, añada las propiedades personalizadas de Active Directory al blueprint. Consulte [Escenario: Añadir una propiedad personalizada a blueprints para reemplazar una política de Active Directory](#).

Escenario: Añadir una propiedad personalizada a blueprints para reemplazar una política de Active Directory

Como arquitecto de blueprints para el grupo empresarial de desarrollo, tiene un blueprint que incluye una máquina de aplicaciones y una máquina de bases de datos, y desea que el registro de la máquina de bases de datos se añada a una unidad organizativa que sea diferente a la política de Active Directory aplicada.

Tiene una política actual que se aplica al grupo empresarial de desarrollo. La política añade registros de máquina a `ou=development,dc=corp,dc=domain,dc=com`. Quiere que todas las máquinas de bases de datos se añadan a `ou=databases,dc=corp,dc=domain,dc=com`. En un blueprint que incluye un servidor de bases de datos, se reemplaza la unidad organizativa de Active Directory para añadir el registro de máquina de bases de datos a `ou=databases,dc=corp,dc=domain,dc=com`.

En este escenario se asumen los siguientes puntos:

- Active Directory incluye unidades organizativas para el desarrollo y las bases de datos.
- Tiene un blueprint de prueba incluido en un servicio que está autorizado.

Además de este sencillo ejemplo sobre cómo puede reemplazar la política, puede utilizar propiedades personalizadas con la política de Active Directory para hacer otros cambios a Active Directory cuando implemente blueprints. Consulte [Trabajar con políticas de Active Directory](#).

Requisitos previos

- Compruebe que tiene al menos una política de Active Directory. Consulte [Crear una política de Active Directory](#). Por ejemplo, cree una política de desarrollo que añada registros a `ou=development,dc=corp,dc=domain,dc=com`.
- Compruebe que tiene un grupo empresarial al que aplicó una política de Active Directory. Consulte [Crear un grupo empresarial](#). Por ejemplo, su grupo empresarial de desarrollo utiliza la política de desarrollo.

Procedimiento

- 1 En el blueprint de prueba, seleccione la máquina de bases de datos en el lienzo.
- 2 Haga clic en la pestaña **Propiedades**.
- 3 Haga clic en la pestaña **Propiedades personalizadas**.
- 4 Haga clic en el icono **Nuevo** (+).
- 5 Añada la propiedad personalizada para cambiar la unidad organizativa predeterminada.
 - a En el cuadro de texto **Nombre**, escriba **ext.policy.activedirectory.orgunit**.
 - b En el cuadro de texto **Valor**, escriba **ou=databases,dc=corp,dc=domain,dc=com**.
 - c Anule la selección de **Reemplazable**.
 - d Haga clic en **Aceptar**.

6 Haga clic en **Finalizar**.

Resultados

El blueprint de prueba incluye la propiedad personalizada, pero los usuarios no ven esta propiedad en el formulario de solicitud.

Pasos siguientes

Solicite el blueprint de prueba. Compruebe que el registro de la máquina de bases de datos se haya añadido a la unidad organizativa de bases de datos, y que el registro de la máquina de aplicaciones se haya añadido a la unidad organizativa de desarrollo. Cuando esté satisfecho con los resultados, podrá añadir la propiedad personalizada a sus blueprints de producción.

Preferencias del usuario para notificaciones y delegados

La preferencia del usuario se utiliza para reemplazar individualmente la configuración predeterminada para las notificaciones del aprobador del sistema y las preferencias de idioma de notificación.

Para acceder a las preferencias del usuario, haga clic en **Preferencias** en la barra de herramientas que aparece junto a su nombre.

Las siguientes opciones son específicas para el usuario que ha iniciado sesión.

Tabla 2-21. Opciones de preferencias de usuario

Opción	Descripción
Asignar delegados	Le permite reasignar las solicitudes de aprobación a otros usuarios. Por ejemplo, el usuario es un aprobador de solicitudes de catálogo, pero se va de vacaciones. Delega todas las notificaciones de aprobación a uno o varios aprobadores. Esta asignación reenvía inmediatamente las solicitudes al delegado. Los delegados están activos hasta que se les quita de la lista.
Notificaciones	Le permite cambiar el idioma de notificación de manera que reciba los mensajes de correo electrónico en el idioma que prefiera en lugar de en el idioma predeterminado. Seleccione el idioma y añada la suscripción de notificación que admite la preferencia de idioma.

Proporcionar blueprints de servicio a los usuarios

3

Los servicios a petición se ofrecen a los usuarios mediante la creación de acciones y elementos de catálogo; después se controla estrictamente quién puede solicitar dichos servicios mediante autorizaciones y aprobaciones.

Este capítulo incluye los siguientes temas:

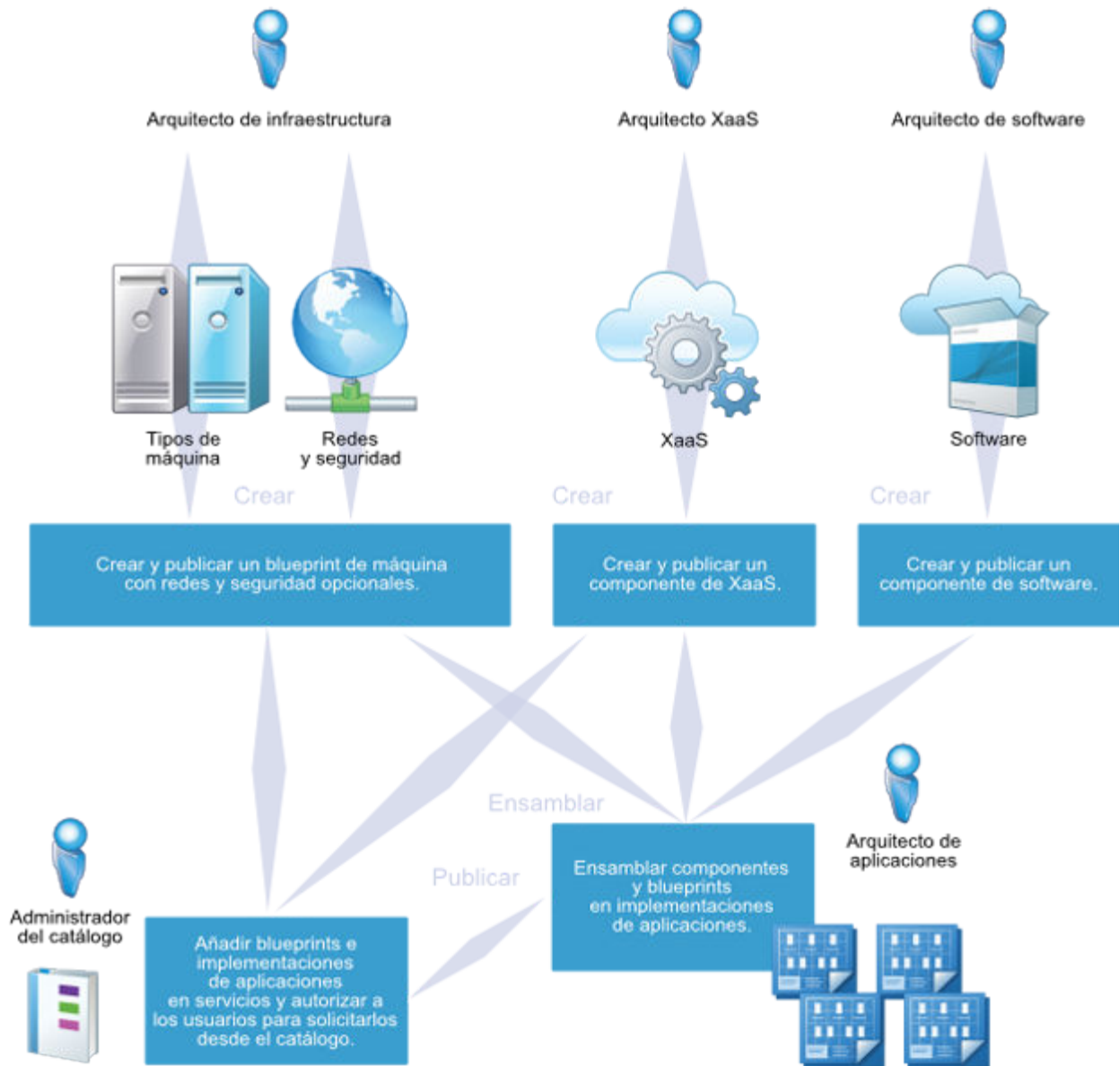
- [Diseñar blueprints](#)
- [Crear la biblioteca de diseño](#)
- [Trabajar con blueprints de desarrollador](#)
- [Ensamblar blueprints compuestos](#)
- [Personalizar formularios de solicitud de blueprint](#)
- [Administrar el catálogo de servicios](#)
- [Administrar los elementos de catálogo implementados](#)

Diseñar blueprints

Los arquitectos de blueprints crean componentes de Software, blueprints de máquinas y blueprints de XaaS personalizados, y ensamblan estos componentes en los blueprints que definen los elementos que los usuarios solicitan del catálogo. El catálogo puede mostrar un formulario de solicitud predeterminado, o bien se puede crear un formulario personalizado para cada blueprint publicado.

Puede crear y publicar blueprints para una sola máquina, o un solo blueprint de XaaS personalizado, pero también puede combinar componentes de máquina y blueprints de XaaS con otros bloques de creación para diseñar blueprints de elementos del catálogo que incluyan varias máquinas, conexiones de red y seguridad, software con soporte durante el ciclo de vida completo y funcionalidad de XaaS personalizada.

En función del elemento del catálogo que desee definir, el proceso puede ser sencillo, como cuando un solo arquitecto de infraestructura publica en un componente de máquina como un blueprint; o puede ser más complejo, como cuando varios arquitectos crean muchos tipos de componentes distintos para diseñar una pila de aplicación completa para que la soliciten los usuarios.



Componentes de Software

Puede crear y publicar componentes de software para instalar software durante el proceso de aprovisionamiento de la máquina y ofrecer soporte al ciclo de vida del software. Por ejemplo, puede crear un blueprint para que los desarrolladores soliciten una máquina que tenga ya instalado y configurado el entorno de desarrollo. Los componentes de software no son elementos del catálogo en sí mismos y deben combinarse con un componente de máquina para crear un blueprint de elemento del catálogo. Consulte [Diseñar componentes de Software](#).

Blueprints de máquinas

Puede crear y publicar blueprints simples para aprovisionar máquinas individuales, o puede crear blueprints más complejos que contengan componentes de máquinas adicionales y, opcionalmente, cualquier combinación de los siguientes tipos de componentes:

- Componentes de Software
- Blueprints existentes
- Red NSX y componentes de seguridad
- Componentes de XaaS
- Componentes de Contenedores
- Componentes personalizados u otros componentes

Consulte [Diseñar blueprints de máquinas](#).

Blueprints de XaaS

Puede publicar flujos de trabajo de vRealize Orchestrator como blueprints de XaaS. Por ejemplo, puede crear un recurso personalizado para usuarios de Active Directory y diseñar un blueprint de XaaS que permita a los administradores aprovisionar nuevos usuarios en su grupo de Active Directory. Puede crear y administrar componentes de XaaS fuera de la pestaña de diseño. Puede reutilizar los blueprints de XaaS publicados para crear blueprints de aplicaciones, pero solo en combinación con al menos un componente de máquina. Consulte [Diseñar acciones personalizadas y blueprints XaaS](#).

Blueprints de aplicaciones con componentes de varias máquinas, de XaaS y de Software

Puede añadir cualquier número de componentes de máquina, componentes de Software y blueprints de XaaS a un blueprint de máquina para ofrecer una funcionalidad avanzada a los usuarios.

Por ejemplo, puede crear un blueprint para que los administradores aprovisionen una configuración relativa a una nueva contratación. Puede combinar componentes de varias máquinas, componentes de software y un blueprint de XaaS para aprovisionar a nuevos usuarios de Active Directory. El administrador de calidad puede solicitar el elemento del catálogo Nueva contratación para aprovisionar al nuevo empleado de ingeniería de calidad en Active Directory y proporcionarle dos máquinas virtuales de trabajo (una para Windows y otra para Linux), cada una de ellas con todo el software necesario para ejecutar casos de pruebas en sus entornos.

Crear la biblioteca de diseño

Puede crear una biblioteca de componentes de blueprint reutilizables que los arquitectos puedan ensamblar en blueprints de aplicación para prestar elaborados servicios a petición a sus usuarios.

Cree una biblioteca de los componentes de diseño de blueprints más pequeños: blueprints de una sola máquina, componentes de Software y blueprints de XaaS; después, combine estos elementos básicos de formas nuevas y diferentes para crear elementos de catálogo complejos que proporcionen niveles de funcionalidad cada vez mayores a sus usuarios.

Tenga en cuenta que hay blueprints de ejemplo en VMware Solution Exchange en <https://solutionexchange.vmware.com> y en <https://code.vmware.com>.

Tabla 3-1. Crear la biblioteca de diseño

Elemento del catálogo	Función	Componentes	Descripción	Detalles
Máquinas	Arquitecto de infraestructura	Cree blueprints de máquina en la pestaña Blueprints .	<p>Puede crear blueprints de máquina para proporcionar rápidamente a los usuarios máquinas en nubes virtuales privadas, públicas o híbridas.</p> <p>Los blueprints de máquina publicados están disponibles para que los administradores del catálogo los incluyan en el catálogo como blueprints independientes, aunque también es posible combinar blueprints de máquina con otros componentes para crear elementos del catálogo más complejos que incluyan varios blueprints de máquina, Software o blueprints de XaaS.</p>	Configurar un blueprint de máquina
Red y seguridad de NSX en las máquinas	Arquitecto de infraestructura	Añada componentes de red y seguridad de NSX a los blueprints de máquina de vSphere en la pestaña Blueprints .	<p>Puede configurar componentes de red y seguridad, como perfiles de red y grupos de seguridad, para permitir que las máquinas virtuales se comuniquen entre sí a través de redes físicas y virtuales de forma segura y eficiente.</p> <p>Debe combinar los componentes de red y seguridad con al menos un componente de máquina de vSphere para que los administradores del catálogo puedan incluirlos en el catálogo. Solo puede aplicar componentes de red y seguridad de NSX a blueprints de máquina de vSphere.</p>	Diseñar blueprints con la configuración de NSX

Tabla 3-1. Crear la biblioteca de diseño (continuación)

Elemento del catálogo	Función	Componentes	Descripción	Detalles
Software en máquinas	Arquitecto de software Para añadir componentes de software correctamente al lienzo de diseño, también debe ser miembro del grupo empresarial, ser administrador del grupo empresarial, o bien tener acceso de función de administrador de tenant en el catálogo de destino.	Cree y publique los componentes de Software en la pestaña Software y, a continuación, combínelos con blueprints de máquina en la pestaña Blueprints .	Añada componentes de Software a los blueprints de máquina para estandarizar, implementar, configurar, actualizar y escalar aplicaciones complejas en entornos de nube. Estas aplicaciones van desde sencillas aplicaciones web hasta complejas aplicaciones personalizadas y aplicaciones empaquetadas. Los componentes de Software no pueden aparecer únicamente en el catálogo. Debe crear y publicar los componentes de Software y, a continuación, ensamblar un blueprint de aplicación que contenga al menos una máquina.	Crear un componente de Software

Tabla 3-1. Crear la biblioteca de diseño (continuación)

Elemento del catálogo	Función	Componentes	Descripción	Detalles
Servicios de TI personalizados	Arquitectos XaaS	Cree y publique blueprints de XaaS en la pestaña XaaS .	Puede crear elementos del catálogo de XaaS que amplíen la funcionalidad de vRealize Automation más allá del aprovisionamiento de máquinas, redes, seguridad y software. Puede automatizar la entrega de cualquier servicio de TI mediante el uso de flujos de trabajo y complementos de vRealize Orchestrator existentes o scripts personalizados desarrollados en vRealize Orchestrator. Los blueprints de XaaS publicados están disponibles para que los administradores del catálogo los incluyan en el catálogo como blueprints independientes, aunque también es posible combinarlos con otros componentes de la pestaña Blueprints para crear elementos del catálogo más elaborados.	Diseñar acciones personalizadas y blueprints XaaS
Ensamblar los bloques de creación de blueprints publicados en nuevos elementos del catálogo	<ul style="list-style-type: none"> ■ Arquitecto de aplicaciones ■ Arquitecto de infraestructura ■ Arquitecto de software 	Combine más blueprints de máquina, blueprints de XaaS y componentes de Software con al menos un componente de máquina o blueprint de máquina en la pestaña Blueprints .	Puede reutilizar componentes y blueprints publicados, combinándolos de nuevas formas para crear paquetes de servicios de TI que proporcionen funciones complejas a los usuarios.	Ensamblar blueprints compuestos

Diseñar blueprints de máquinas

Los blueprints de máquinas constituyen la especificación completa de una máquina; en ellos se determinan los atributos de una máquina, la forma en la que esta se aprovisiona y su configuración de administración y políticas. Según cuál sea la complejidad del elemento de catálogo que esté creando, puede combinar uno o varios componentes de máquina del blueprint con otros componentes en el lienzo de diseño a fin de obtener elementos de catálogo más elaborados que incluyan redes y seguridad, componentes de Software, componentes de XaaS y otros componentes de blueprint.

Almacenamiento con un uso eficaz del espacio para el aprovisionamiento virtual

La tecnología de almacenamiento que hace un uso eficiente del espacio elimina las ineficacias de los métodos de almacenamiento tradicionales, ya que solo utiliza el almacenamiento que en realidad se requiere para las operaciones de una máquina. Normalmente, solo se trata de una fracción del almacenamiento que se asigna a las máquinas realmente. vRealize Automation es compatible con dos métodos de aprovisionamiento con tecnología que usa el espacio de forma eficiente: aprovisionamiento fino y aprovisionamiento de FlexClone.

Cuando se utiliza el almacenamiento estándar, el almacenamiento que se asigna a una máquina aprovisionada se reserva para esa única máquina, aunque esté apagada. Esto puede constituir un desperdicio de recursos de almacenamiento, debido a que hay muy pocas máquinas virtuales que realmente usan todo el almacenamiento que se les asigna; solo unas pocas máquinas físicas funcionan con un disco completo al 100 %. Cuando se emplea una tecnología que hace un uso eficiente del espacio, el almacenamiento asignado y el almacenamiento utilizado se registran por separado, y solo el almacenamiento utilizado se reserva completamente para la máquina aprovisionada.

Aprovisionamiento fino

El aprovisionamiento fino es compatible con todos los métodos de aprovisionamiento virtual. En función de la plataforma de virtualización, el tipo de almacenamiento y la configuración de almacenamiento predeterminada, el aprovisionamiento fino se puede usar de forma continua durante el aprovisionamiento de máquinas. Por ejemplo, para las integraciones del servidor de vSphere ESX que usan almacenamiento NFS, siempre se usa el aprovisionamiento fino. No obstante, para las integraciones del servidor de vSphere ESX que usan almacenamiento local o de iSCSI, el aprovisionamiento fino solo se usa para aprovisionar máquinas si la propiedad personalizada `VirtualMachine.Admin.ThinProvision` se especifica en el blueprint. Para obtener más información sobre el aprovisionamiento fino, consulte la documentación que acompaña a la plataforma de virtualización.

Aprovisionamiento de Net App FlexClone

Puede crear un blueprint para el aprovisionamiento de NetApp FlexClone si trabaja en un entorno de vSphere que utiliza el almacenamiento Network File System (NFS) y la tecnología de FlexClone.

Solo se puede usar el almacenamiento NFS, de lo contrario se producirá un error de aprovisionamiento de máquinas. Puede especificar una ruta de almacenamiento de FlexClone para otros tipos de aprovisionamiento de máquinas, pero la ruta de almacenamiento de FlexClone se comportará como el almacenamiento estándar.

A continuación encontrará una descripción de alto nivel de la secuencia de pasos necesarios para aprovisionar máquinas que usan la tecnología de FlexClone:

- 1 Un administrador de IaaS crea un endpoint de NetApp ONTAP. Consulte [Referencia de la configuración de un endpoint](#).
- 2 Un administrador de IaaS ejecuta la recopilación de datos en el endpoint para permitir que este sea visible en las páginas de recursos informáticos y de reservas.

La opción FlexClone estará disponible en una página de reservas en la columna de endpoint si hay un endpoint de NetApp ONTAP y si el host es virtual. Si hay un endpoint de NetApp ONTAP, la página de reservas mostrará el endpoint asignado a la ruta de almacenamiento.

- 3 Un administrador de tejido crea una reserva de vSphere, habilita el almacenamiento de FlexClone y especifica una ruta de almacenamiento NFS que utiliza la tecnología de FlexClone. Consulte [Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer](#).
- 4 Un arquitecto de infraestructura u otro usuario autorizado crea un blueprint para el aprovisionamiento de FlexClone.

Descripción y el uso de la parametrización de blueprints

Los perfiles de componente se pueden usar para parametrizar blueprints. En lugar de crear un blueprint pequeño, mediano y grande independiente destinado a un tipo de implementación determinado, puede crear un único blueprint donde se pueda elegir una máquina virtual de tamaño pequeño, mediano o grande. Los usuarios seleccionarán uno de estos tamaños cuando implementen el elemento del catálogo.

Con los perfiles de componente se minimiza la infrautilización de los blueprints y se simplifican las ofertas del catálogo. Los perfiles de componente se usan para definir los componentes de máquina de vSphere en un blueprint. Los tipos de perfil de componente disponibles son **Size** y **Image**. Al agregar perfiles de componente a un componente de máquina, la configuración de perfil de componente reemplaza otras opciones del componente de máquina, como el número de CPU o la cantidad de almacenamiento.

Los perfiles de componente solo están disponibles para los componentes de máquina de vSphere.

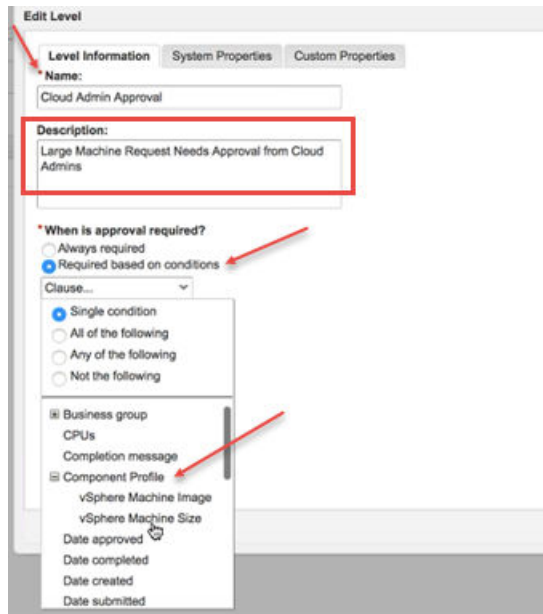
Si desea obtener información sobre cómo definir los conjuntos de valores para los perfiles de componente **Size** y **Image**, consulte en *Referencia de propiedades personalizadas*

Para obtener información sobre cómo agregar los perfiles de componente y los conjuntos de valores seleccionados para un componente de máquina de vSphere en un blueprint, consulte [Configuración de los componentes de máquina de vSphere](#).

Para obtener información sobre cómo añadir información de perfiles de componente mediante la configuración importada de un OVF, consulte [Configurar un blueprint para aprovisionar desde un OVF](#).

En el caso de necesitar información sobre el uso de los perfiles de componente cuando se solicita el aprovisionamiento de máquinas, consulte [Solicitar el aprovisionamiento de máquinas a través de un blueprint parametrizado](#).

Nota Se pueden crear políticas de aprobación que requieran la aprobación previa al solicitar el aprovisionamiento de máquinas de blueprints en relación con las condiciones del conjunto de valores del perfil de componente **Size** y **Image**. Para obtener más información, consulte [Ejemplos de políticas de aprobación basadas en el tipo de política de máquina virtual](#)



Si desea más información sobre cómo usar la parametrización de blueprints al solicitar el aprovisionamiento de máquinas del catálogo, consulte [Solicitar el aprovisionamiento de máquinas a través de un blueprint parametrizado](#).

Configurar un blueprint de máquina

Configure y publique un componente de máquina como un blueprint independiente que otros arquitectos puedan reutilizar como componente en blueprints de aplicaciones y los administradores del catálogo puedan incluir en los servicios de catálogo.

Este procedimiento proporciona una visión general sencilla del proceso de creación de blueprints. Para obtener información adicional, consulte lo siguiente:

- [Diseñar blueprints con la configuración de NSX](#)
- [Descripción y el uso de la parametrización de blueprints](#)
- [Configurar un blueprint para aprovisionar desde un OVF](#)
- [Exportar e importar blueprints y contenido](#)
- [Crear blueprints de Microsoft Azure e incorporar acciones personalizadas](#)
- [Crear blueprints de vSphere habilitados para Puppet](#)

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Complete las preparaciones externas para el aprovisionamiento (como crear plantillas, WinPE e ISO) o recopile la información sobre las preparaciones externas de los administradores.
- Configure el tenant. Consulte [Configurar las opciones de tenant](#).
- Configure los recursos de IaaS. Consulte [Lista de comprobación para la configuración de recursos de IaaS](#).

- Consulte *Configuración de vRealize Automation*.

Procedimiento

- 1 Seleccione **Diseño > Blueprints**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Siga los mensajes del cuadro de diálogo **Nuevo blueprint** para realizar la configuración general.
- 4 Haga clic en **Aceptar**.
- 5 Haga clic en **Tipos de máquina** en el área Categorías para ver una lista de los tipos de máquina disponibles.
- 6 Arrastre hasta el lienzo de diseño el tipo de máquina que quiera aprovisionar.
- 7 Siga las indicaciones de cada una de las pestañas para configurar los detalles de aprovisionamiento de la máquina.
- 8 Haga clic en **Finalizar**.
- 9 Seleccione el blueprint y haga clic en **Publicar**.

Resultados

De este modo, ha configurado y publicado un componente de máquina como un blueprint independiente. Los administradores del catálogo pueden incluir este blueprint de máquina en los servicios de catálogo y autorizar a los usuarios a que puedan solicitar este blueprint. Por su parte, otros arquitectos pueden reutilizar este blueprint de máquina para crear blueprints de aplicación más elaborados que incluyan componentes de Software, blueprints de XaaS o más blueprints de máquina.

Pasos siguientes

Un blueprint de máquina se puede combinar con componentes de Software, con blueprints de XaaS o con más blueprints de máquina para crear blueprints de aplicación más elaborados. Consulte [Ensamblar blueprints compuestos](#) y [Información sobre el comportamiento de blueprint anidado](#).

Configuración de blueprint de máquina

Puede definir valores de configuración y propiedades personalizadas para todo el blueprint.

Configuración de las propiedades de blueprint

La configuración que se aplica en todo el blueprint se puede especificar en la página **Propiedades de blueprint** cuando este se crea. Después de crear el blueprint, edite estas opciones en la página Propiedades de blueprint.

Pestaña **General**

Aplique las opciones de configuración en todo el blueprint, incluidos todos los componentes que desea añadir en este momento o posteriormente.

Tabla 3-2. Configuración de la pestaña **General**

Configuración	Descripción
Nombre	Escriba un nombre para el blueprint.
Identificador	El campo de identificador se rellena automáticamente en función del nombre que haya introducido. Si desea editar este campo, hágalo ahora, pues en cuanto guarde el blueprint ya no podrá cambiarlo. Dado que los identificadores son permanentes y únicos en el tenant, puede usarlos para interactuar con los blueprints mediante programación y para crear enlaces de propiedades.
Descripción	Incluya un resumen del blueprint para proporcionar información a otros arquitectos. Además, los usuarios verán esta descripción en el formulario de solicitud.
Límite de implementaciones	Especifique el número máximo de implementaciones que pueden crearse cuando se usa este blueprint para aprovisionar máquinas.
Días de concesión: Mínimo y Máximo	Establezca un valor mínimo y un valor máximo para permitir a los usuarios elegir entre un rango de duraciones de concesión. Cuando finaliza la concesión, la implementación se destruye o se archiva. Si no especifica un valor mínimo o un valor máximo, la concesión nunca caducará.
Días de archivado	Puede especificar un período de archivado para conservar las implementaciones de forma temporal en lugar de destruirlas cuando caduque su concesión. Especifique 0 (valor predeterminado) para destruir la implementación cuando caduque su concesión. El período de archivado comienza el día que caduca la concesión. Cuando finaliza el período de archivado, la implementación se destruye.
Propagar actualizaciones a implementaciones existentes	<p>Cuando se activa, especifica que cualquier ampliación de los límites de los valores máximos o mínimos de la CPU, la memoria y el almacenamiento del blueprint se insertarán en todas las implementaciones activas aprovisionadas desde el blueprint. Por ejemplo, si especifica un mínimo de 2 y un máximo de 4 (2,4) en un principio, un cambio a (1,4) o (2,5) surte efecto tras la reconfiguración, pero un cambio a (3,4) o (2,3) no se aplica.</p> <p>Los cambios surten efecto después de la siguiente acción de reconfiguración. Para obtener información relacionada con las acciones de reconfiguración, consulte Comandos del menú Acción en recursos aprovisionados.</p>

Pestaña **Configuración de NSX**

Si ha configurado NSX, puede especificar la configuración de la zona de transporte, la política de reserva de puerta de enlace enrutada y de Edge, y el aislamiento de aplicaciones de NSX cuando cree o edite un blueprint. Estas opciones de configuración están disponibles en la pestaña **Configuración de NSX** de las páginas **Blueprint** y **Propiedades de blueprint**.

Para obtener información sobre la configuración de NSX, consulte [Configuración de las páginas Nuevo blueprint y Propiedades de blueprint con NSX](#).

Pestaña **Propiedades**

Las propiedades personalizadas que añada al blueprint se aplican a todo el blueprint, incluidos todos sus componentes. Sin embargo, pueden reemplazarse con propiedades personalizadas asignadas posteriormente en la cadena de prioridad. Para obtener más información sobre el orden de prioridad de las propiedades personalizadas, consulte *Referencia de propiedades personalizadas*.

Tabla 3-3. Configuración de la pestaña **Propiedades**

Pestaña	Configuración	Descripción
Grupos de propiedades	Los grupos de propiedades son grupos reutilizables de propiedades que se han diseñado para simplificar el proceso de adición de propiedades personalizadas a los blueprints. Los administradores de tenant y de tejido pueden agrupar las propiedades que se suelen utilizar juntas para poder añadir el grupo de propiedades a un blueprint en lugar de insertar propiedades personalizadas una por una.	
	Añadir	<p>Añada uno o varios grupos de propiedades existentes y aplíquelos a todo el blueprint.</p> <p>Se proporcionan los siguientes grupos de propiedades relacionados con contenedores:</p> <ul style="list-style-type: none"> ■ Propiedades del host de contenedor con autenticación con certificado ■ Propiedades del host de contenedor con autenticación con usuario/contraseña
	Subir /Bajar	Establezca una prioridad de los grupos para controlar el orden de prioridad de cada grupo de propiedades con respecto de los demás. El primer grupo de la lista es el que tiene mayor prioridad y sus propiedades personalizadas ocupan el primer puesto en el orden de prioridad. Si desea cambiar el orden, solo tiene que arrastrar y soltar.
	Ver propiedades	Visualice las propiedades personalizadas en el grupo de propiedades seleccionado.
	Ver propiedades combinadas	Si la propiedad personalizada está incluida en más de un grupo de propiedades, tendrá prioridad el valor incluido en el grupo de propiedades cuya prioridad sea mayor. Puede ver estas propiedades combinadas para establecer el orden de prioridad de los grupos de propiedades.
Propiedades personalizadas	Puede añadir propiedades personalizadas individuales en lugar de grupos de propiedades.	

Tabla 3-3. Configuración de la pestaña **Propiedades** (continuación)

Pestaña	Configuración	Descripción
	Nuevo	Añada una propiedad personalizada individual y aplíquela a todo el blueprint.
	Nombre	Escriba el nombre de la propiedad. Para obtener una lista de las propiedades personalizadas y sus definiciones, consulte <i>Referencia de propiedades personalizadas</i> .
	Valor	Introduzca el valor de la propiedad personalizada.
	Cifrado	Puede optar por cifrar el valor de la propiedad si, por ejemplo, el valor es una contraseña.
	Reemplazable	Puede especificar que la próxima persona u otra más adelante que utilice la propiedad pueda reemplazar el valor de la propiedad. Por lo general, suele ser otro arquitecto, pero, si selecciona Mostrar en solicitud , los usuarios empresariales podrán ver y editar valores de propiedades cuando soliciten elementos del catálogo.
	Mostrar en solicitud	Si desea mostrar el nombre y el valor de la propiedad a los usuarios finales, puede seleccionar la opción para mostrar la propiedad en el formulario de solicitud cuando se solicite el aprovisionamiento de la máquina. También debe seleccionar Reemplazable si desea que los usuarios proporcionen un valor.

Configuración de los componentes de máquina de vSphere

Conozca los ajustes y las opciones que puede configurar para un componente de máquina de vSphere en el lienzo de diseño de blueprints de vRealize Automation. vSphere es el único tipo de componente de máquina que puede usar la configuración de red y seguridad de NSX en el lienzo de diseño.

Pestaña **General**

Configure los ajustes generales para un componente de máquina de vSphere.

Tabla 3-4. Configuración de la pestaña **General**

Configuración	Descripción
ID	Escriba el nombre del componente de máquina o acepte el nombre predeterminado.
Descripción	Incluya un resumen del componente de máquina para proporcionar información a otros arquitectos.

Tabla 3-4. Configuración de la pestaña **General** (continuación)

Configuración	Descripción
Mostrar ubicación al solicitar	<p>En un entorno de nube, como vCloud Air, esto permite que los usuarios seleccionen una región para sus máquinas aprovisionadas.</p> <p>Para un entorno virtual, como vSphere, puede configurar la función de ubicaciones para permitir a los usuarios seleccionar una ubicación de centro de datos concreta para el aprovisionamiento de una máquina solicitada. Para configurar esta opción completamente, un administrador del sistema debe añadir información de la ubicación del centro de datos al archivo de ubicaciones y un administrador de tejido debe editar un recurso informático para asociarlo a dicha ubicación.</p>
Política de reserva	<p>Aplice una política de reserva a un blueprint para restringir las máquinas aprovisionadas desde ese blueprint a un subconjunto de reservas disponibles. Los administradores de tejido crean políticas de reserva como una opción útil para controlar el procesamiento de las solicitudes de reserva, por ejemplo, para recopilar recursos en grupos para niveles de servicio distintos o para facilitar que un tipo de recurso concreto esté disponible para un fin concreto. Si el administrador de tejido no configuró políticas de reserva, no verá ninguna opción disponible en este menú desplegable. Solo están disponibles las políticas de reserva que corresponden al tenant actual.</p>
Prefijo de máquina	<p>Los administradores de tejido crean prefijos de máquina para generar los nombres de las máquinas aprovisionadas. Si selecciona Usar valor predeterminado del grupo, las máquinas aprovisionadas del blueprint reciben sus nombres a partir del prefijo de máquina configurado como predeterminado en el grupo empresarial del usuario. Si no hay ningún prefijo de máquina configurado, se genera uno automáticamente basándose en el nombre del grupo empresarial. Solo están disponibles los prefijos de máquina que corresponden al tenant actual.</p> <p>Si el administrador de tejido configura otros prefijos de máquina que pueden seleccionarse, es posible aplicar un prefijo a todas las máquinas aprovisionadas del blueprint, sea quien sea el solicitante.</p>
Instancias: Mínimo y Máximo	<p>Configure el número máximo y mínimo de instancias que los usuarios pueden seleccionar para una implementación, o para una acción de escalado horizontal o vertical. Si no desea ofrecerles una opción a los usuarios, puede introducir el mismo valor en los campos Mínimo y Máximo para configurar exactamente cuántas instancias aprovisionar y desactivar las acciones de escalado en ese componente de máquina.</p> <p>Los componentes de XaaS no pueden escalarse y no se actualizan durante una operación de escalado. Si utiliza componentes de XaaS en su blueprint, podría crear una acción personalizada para que los usuarios la ejecuten después de una operación de escalado, que podría escalar o actualizar los componentes de XaaS en caso necesario. Como alternativa, podría desactivar las acciones de escalado. Para ello, debe configurar el número exacto de instancias que desea permitir en cada componente de máquina.</p>

Pestaña Información de creación

Configure los ajustes de información de compilación para un componente de máquina de vSphere.

Tabla 3-5. Pestaña Información de creación

Configuración	Descripción
Tipo de blueprint	Para mantener un registro y administrar las licencias, seleccione si las máquinas aprovisionadas desde este blueprint se clasifican como Escritorio o Servidor.
Acción	<p>Las opciones que aparecen en el menú desplegable dependen del tipo de máquina que haya seleccionado. Dispone de las siguientes acciones:</p> <ul style="list-style-type: none"> ■ Crear Cree la especificación de componente de máquina sin usar una opción de clonación. ■ Clonar Realice copias de una máquina virtual a partir de una plantilla y un objeto de personalización. ■ Clon vinculado Aprovisionar una copia con espacio eficiente de una máquina virtual llamada clon vinculado. Los clones vinculados se basan en el snapshot de una máquina virtual y usan una cadena de discos delta para realizar un seguimiento de las diferencias con respecto a una máquina principal. El snapshot de máquina virtual identificado en el blueprint debe apagarse antes de aprovisionar las máquinas virtuales de clon vinculado. ■ NetApp FlexClone Si el administrador de tejido configuró las reservas para utilizar el almacenamiento de NetApp FlexClone, puede usar esta tecnología para clonar copias de máquinas haciendo un uso eficiente del espacio.

Tabla 3-5. Pestaña **Información de creación** (continuación)

Configuración	Descripción
Flujo de trabajo de aprovisionamiento	<p>Las opciones que aparecen en el menú desplegable de flujo de trabajo de aprovisionamiento dependen del tipo de máquina y de la acción que haya seleccionado.</p> <ul style="list-style-type: none"> ■ BasicVmWorkflow <p>Aprovisione una máquina sin sistema operativo invitado.</p> ■ ExternalProvisioningWorkflow <p>Cree una máquina iniciándola desde una instancia de máquina virtual o una imagen de nube.</p> ■ ImportOvfWorkflow <p>Permite implementar una máquina virtual de vSphere a partir de una plantilla de OVF de la misma manera en la que una instancia de CloneWorkflow permite implementar una máquina virtual de vSphere a partir de una plantilla de máquina virtual. Puede importar a un componente de vSphere en un blueprint de máquina o a un perfil de componente de Image de un blueprint parametrizado.</p> ■ LinuxKickstartWorkflow <p>Aprovisionar una máquina mediante el arranque desde una imagen ISO usando un archivo de configuración Kickstart o autoYaST y una imagen de distribución Linux para instalar el sistema operativo en la máquina.</p> ■ VirtualSccmProvisioningWorkflow <p>Aprovisionar una máquina y transferir el control a una secuencia de tareas de SCCM para arrancar desde una imagen ISO, implementar un sistema operativo Windows e instalar el agente invitado de vRealize Automation.</p> ■ WIMImageWorkflow <p>Aprovisionar una máquina mediante el arranque en un entorno WinPE y la instalación de un sistema operativo usando una imagen Windows Imaging File Format (WIM) de una máquina de referencia Windows existente.</p> <p>Cuando utilice un flujo de trabajo de aprovisionamiento de WIM en un blueprint, especifique un valor de almacenamiento que tenga en cuenta el tamaño de todos los discos que se usarán en la máquina. Use el valor total de todos los discos como valor de almacenamiento mínimo del componente de máquina. Especifique además un tamaño para cada disco con capacidad suficiente para dar cabida al sistema operativo.</p>

Tabla 3-5. Pestaña **Información de creación** (continuación)

Configuración	Descripción
Clonar de	<p>Seleccione una plantilla de máquina a partir de la cual clonar. Puede refinar la lista de plantillas disponibles usando la opción Filtros disponible en todos los menús desplegables de las columnas, por ejemplo, la opción de menú Filtros en la columna Nombres.</p> <p>Para Clon vinculado, solo verá las máquinas con snapshots disponibles a partir de los que clonar y que administre como administrador de tenants o administrador de grupo empresarial.</p> <p>Solo puede clonar a partir de las plantillas existentes en las máquinas que administra como administrador de grupo empresarial o como administrador de tenants.</p>
Clonar desde snapshot	<p>Para Clon vinculado, seleccione un snapshot existente para clonarlo usando la plantilla de máquina seleccionada. Las máquinas solo aparecen en la lista si ya poseen un snapshot y si las administra como administrador de grupo empresarial o de tenant.</p> <p>Si selecciona Usar snapshot actual, el clon se define con las mismas características que el último estado de la máquina virtual. Si prefiere crear un clon relativo en lugar de un snapshot real, haga clic en la opción del menú desplegable y seleccione el snapshot en cuestión de la lista.</p> <p>Nota El uso del término snapshot (o snapshot) puede generar confusiones. Si selecciona un snapshot existente, la opción crea un disco nuevo que está subordinado al snapshot. La opción Usar snapshot actual no dispone de ningún disco base para utilizarlo como elemento principal y efectúa una acción de clonación completa de forma silenciosa. Como solución alternativa, puede crear snapshots en el disco base o utilizar un flujo de trabajo de vRealize Orchestrator para crear un snapshot y, a continuación, clonar inmediatamente a partir del snapshot.</p> <p>Esta opción solo está disponible para la acción de clon vinculado.</p>
Especificación de personalización	<p>Indique una especificación de personalización disponible. Solo se necesita una especificación de personalización si se lleva a cabo una clonación con direcciones IP estáticas.</p> <p>No es posible realizar personalizaciones de máquinas Windows sin una especificación de personalización. En clones de máquinas de Linux, puede usar una especificación de personalización, un script externo (o ambos) para realizar personalizaciones.</p>

Pestaña **Recursos de máquinas**

Especifique la configuración de CPU, memoria y almacenamiento para el componente de máquina de vSphere.

Tabla 3-6. Pestaña **Recursos de máquinas**

Configuración	Descripción
CPU: Mínimo y Máximo	Especifique un número mínimo y un número máximo de CPU que este componente de máquina pueda aprovisionar.
Memoria (MB): Mínimo y Máximo	Especifique una cantidad mínima y máxima de memoria que pueden consumir las máquinas aprovisionadas por este componente de máquina.
Almacenamiento (GB): Mínimo y Máximo	Especifique una cantidad mínima y máxima de almacenamiento que pueden consumir las máquinas aprovisionadas por este componente de máquina. Para vSphere, KVM (RHEV), SCVMM, vCloud Air y vCloud Director, el almacenamiento mínimo se establece en función de lo que indique en la pestaña Almacenamiento. Cuando utilice un flujo de trabajo de aprovisionamiento de WIM en un blueprint, especifique un valor de almacenamiento que tenga en cuenta el tamaño de todos los discos que se usarán en la máquina. Use el valor total de todos los discos como valor de almacenamiento mínimo del componente de máquina. Especifique además un tamaño para cada disco con capacidad suficiente para dar cabida al sistema operativo.

Pestaña **Almacenamiento**

Para controlar el espacio de almacenamiento, puede añadir al componente de máquina algunas opciones de volumen de almacenamiento, como una o varias políticas de reserva de almacenamiento.

Tabla 3-7. Configuración de la pestaña **Almacenamiento**

Configuración	Descripción
ID	Escriba un ID o nombre del volumen de almacenamiento.
Capacidad (GB)	Especifique la capacidad de almacenamiento del volumen de almacenamiento.
Letra de unidad/Punto de montaje	Especifique una letra de unidad o un punto de montaje del volumen de almacenamiento.
Etiqueta	Especifique una etiqueta para la letra de unidad y el punto de montaje del volumen de almacenamiento.
Política de reserva de almacenamiento	Especifique la política de reserva de almacenamiento existente que se usará con este volumen de almacenamiento. Solo están disponibles las políticas de reserva de almacenamiento que corresponden al tenant actual.
Propiedades personalizadas	Especifique las propiedades de almacenamiento que se usarán con este volumen de almacenamiento.

Tabla 3-7. Configuración de la pestaña **Almacenamiento** (continuación)

Configuración	Descripción
Máximo de volúmenes	Especifique el número máximo de volúmenes de almacenamiento permitidos que se pueden usar durante el aprovisionamiento desde el componente de máquina. Escriba 0 para evitar que otros usuarios puedan añadir volúmenes de almacenamiento. El valor predeterminado es 60.
Permitir que el usuario vea y cambie las políticas de reserva de almacenamiento	Active esta casilla para permitir que los usuarios eliminen una política de reserva asociada o especifiquen una distinta durante el aprovisionamiento.

Pestaña Red

Puede especificar la configuración de red de un componente de máquina de vSphere a partir de los ajustes de equilibrador de carga y red de NSX que se configuran fuera de vRealize Automation. Puede usar la configuración de uno o varios componentes de red de NSX a petición y existentes en el lienzo de diseño.

Para obtener información acerca de la adición y la configuración de los componentes de red y seguridad de NSX antes de usar la configuración de la pestaña de red en un componente de máquina de vSphere, consulte [Configurar opciones del componente de red y seguridad](#).

Para obtener información sobre la especificación de una configuración a nivel de blueprint de NSX que se aplique a los componentes de máquina de vSphere, consulte [Configuración de las páginas Nuevo blueprint y Propiedades de blueprint con NSX](#).

Tabla 3-8. Configuración de la pestaña **Red**

Configuración	Descripción
Red	Seleccione un componente de red del menú desplegable. Solo aparecen en la lista los componentes de red existentes en el lienzo de diseño. Solo están disponibles los perfiles de red que corresponden al tenant actual.
Tipo de asignación	Acepte la asignación predeterminada derivada del componente de red o seleccione un tipo de asignación del menú desplegable. Los valores de las opciones DHCP y Estática se derivan de la configuración del componente de red.
Dirección	Especifique la dirección IP de la red. Esta opción solo está disponible para el tipo de dirección estática.
Equilibrio de carga	Indique el servicio que se va a usar para el equilibrio de carga.
Propiedades personalizadas	Muestre las propiedades personalizadas configuradas para el perfil de red o el componente de red seleccionado.
Máximo de adaptadores de red	Especifique el número máximo de adaptadores de red (NIC) que se permitirán en este componente de máquina. El valor predeterminado es ilimitado. Establezca el valor en 0 para desactivar la adición de NIC en los componentes de máquina.

Pestaña **Seguridad**

Puede especificar la configuración de seguridad de un componente de máquina de vSphere a partir de los ajustes de NSX que se configuran fuera de vRealize Automation. También puede usar la configuración de los componentes de seguridad de NSX a petición y existentes en el lienzo de diseño.

La configuración de seguridad de los componentes de etiqueta de seguridad y grupo de seguridad a petición y existentes en el lienzo de diseño está disponible automáticamente.

Para obtener información acerca de la adición y la configuración de los componentes de red y seguridad de NSX antes de usar la configuración de la pestaña de seguridad en un componente de máquina de vSphere, consulte [Configurar opciones del componente de red y seguridad](#).

Para obtener información sobre la especificación de una información a nivel de blueprint de NSX que se aplique a los componentes de máquina de vSphere, consulte [Configuración de las páginas Nuevo blueprint y Propiedades de blueprint con NSX](#).

Tabla 3-9. Configuración de la pestaña **Seguridad**

Configuración	Descripción
Nombre	Muestre el nombre de una etiqueta o un grupo de seguridad de NSX. Los nombres se derivan de los componentes de seguridad del lienzo de diseño. Active la casilla situada junto a un grupo o una etiqueta de seguridad de la lista para usar dicha etiqueta o grupo para el aprovisionamiento desde este componente de máquina.
Tipo	Indique si el elemento de seguridad es un grupo de seguridad a petición, un grupo de seguridad existente o una etiqueta de seguridad.
Descripción	Muestre la descripción definida para el grupo o la etiqueta de seguridad.
Endpoint	Muestre el endpoint que utiliza el grupo o la etiqueta de seguridad de NSX.

Pestaña **Propiedades**

De forma opcional puede especificar la información de grupo de propiedades y de propiedad personalizada del componente de máquina de vSphere.

Puede utilizar la pestaña **Propiedades** para añadir al componente de máquina propiedades personalizadas, ya sea de forma individual o en grupos. También puede añadir propiedades personalizadas y grupos de propiedades a todo el blueprint con la pestaña **Propiedades** durante la creación o la edición de un blueprint mediante la página **Propiedades de blueprint**.

Puede utilizar la pestaña **Propiedades personalizadas** para añadir y configurar opciones para las propiedades personalizadas existentes. Las propiedades personalizadas se suministran con vRealize Automation y también se pueden crear definiciones de propiedades.

Tabla 3-10. Configuración de la pestaña **Propiedades > Propiedades personalizadas**

Configuración	Descripción
Nombre	Escriba el nombre de una propiedad personalizada o seleccione una de las propiedades personalizadas disponibles en el menú desplegable. Por ejemplo, escriba el nombre de propiedad personalizada <code>Machine.SSH</code> para especificar si las máquinas aprovisionadas mediante este blueprint permiten las conexiones SSH. Las propiedades solo aparecen en el menú desplegable si el administrador de tenants o de tejido creó definiciones de propiedades.
Valor	Escriba o edite un valor para asociarlo al nombre de propiedad personalizada. Por ejemplo, establezca el valor en <code>true</code> para permitir que los usuarios autorizados se conecten mediante SSH a las máquinas aprovisionadas con su blueprint.
Cifrado	Puede optar por cifrar el valor de la propiedad si, por ejemplo, el valor es una contraseña.
Reemplazable	Puede especificar que la próxima persona u otra más adelante que utilice la propiedad pueda reemplazar el valor de la propiedad. Por lo general, suele ser otro arquitecto, pero, si selecciona Mostrar en solicitud , los usuarios empresariales podrán ver y editar valores de propiedades cuando soliciten elementos del catálogo.
Mostrar en solicitud	Si desea mostrar el nombre y el valor de la propiedad a los usuarios finales, puede seleccionar la opción para mostrar la propiedad en el formulario de solicitud cuando se solicite el aprovisionamiento de la máquina. También debe seleccionar Reemplazable si desea que los usuarios proporcionen un valor.

Puede utilizar la pestaña **Grupos de propiedades** para añadir y configurar opciones para los grupos de propiedades personalizadas existentes. Puede crear sus propios grupos de propiedades o usar los grupos de propiedades creados para que los use.

Tabla 3-11. Configuración de la pestaña **Propiedades > Grupos de propiedades**

Configuración	Descripción
Nombre	Seleccione uno de los grupos de propiedades disponibles en el menú desplegable.
Subir y Bajar	Controle el nivel de prioridad de los grupos de propiedades de la lista en orden descendente. El primer grupo de propiedades de la lista tiene prioridad sobre el siguiente grupo de propiedades de la lista y así sucesivamente.

Tabla 3-11. Configuración de la pestaña **Propiedades > Grupos de propiedades** (continuación)

Configuración	Descripción
Ver propiedades	Visualice las propiedades personalizadas en el grupo de propiedades seleccionado.
Ver propiedades combinadas	Visualice todas las propiedades personalizadas de los grupos de propiedades de la lista en el orden en que aparecen en la lista de grupos de propiedades. Si una misma propiedad aparece en más de un grupo de propiedades, el nombre de la propiedad aparece una sola vez en la lista, según su primera aparición en la misma.

Pestaña Perfiles

Los perfiles de componente proporcionan un medio para parametrizar los blueprints. Así, por ejemplo, en lugar de crear un blueprint independiente para pequeño, medio y grande, puede crear un único blueprint con una capacidad pequeña, mediana y grande, de manera que el usuario pueda seleccionar uno de los tamaños cuando implemente el elemento de catálogo. Con los perfiles de componente se minimiza la infrautilización de los blueprints y se simplifica el catálogo.

Si ha creado conjuntos de valores para los perfiles de componente **Size** y **Image** proporcionados de vRealize Automation, puede añadir y configurar estas opciones para el componente de máquina del blueprint. También puede seleccionar distintos conjuntos de valores cuando implemente el elemento del catálogo.

Los perfiles de componente solo están disponibles para los componentes de máquina de vSphere.

Cuando se agrega un perfil de componente al componente de máquina de vSphere en un blueprint, la configuración que se define en el conjunto de valores o los conjuntos de valores seleccionados del perfil anula otras configuraciones que haya en el componente de máquina, como el número de CPU y de almacenamiento.

El conjunto de valores del perfil de componente se aplica a todas las máquinas de vSphere en un clúster.

No se pueden reconfigurar máquinas mediante los perfiles de componente **Size** o **Image**, pero el intervalo de CPU, memoria y almacenamiento que se calcula en función del perfil sigue disponible para las acciones de reconfiguración. Por ejemplo, si ha utilizado conjuntos de valores para **Size** pequeños (1 CPU, 1024 MB de memoria y 10 GB de almacenamiento) medianos (3 CPU, 2048 MB de memoria, 12 GB de almacenamiento) y grandes (5 CPU, 3072 MB de memoria, 15 GB de almacenamiento), los rangos disponibles durante la reconfiguración de máquina son 1-5 CPU, 1024-3072 MB de memoria y 1-15 GB de almacenamiento.

Para obtener más información sobre cómo definir conjuntos de valores para los perfiles de componente, consulte *Referencia de propiedades personalizadas*.

Tabla 3-12. Configuración de la pestaña **Perfiles**

Configuración	Descripción
Añadir	Agregue el perfil de componente Size o Image.
Editar conjuntos de valores	Asigne uno o varios conjuntos de valores para el perfil de componente seleccionado. Para ello, seleccione uno de ellos en una lista de conjuntos de valores definidos. Puede seleccionar uno de los conjuntos de valores como predeterminado.
Quitar	Elimine el perfil de componente Size o Image.

Configuración de los componentes de máquina de vCloud Air

Conozca los ajustes y las opciones que puede configurar para un componente de máquina de vCloud Air en el lienzo de diseño de blueprints de vRealize Automation.

Pestaña **General**

Configure los ajustes generales para un componente de máquina de vCloud Air.

Tabla 3-13. Configuración de la pestaña **General**

Configuración	Descripción
ID	Escriba el nombre del componente de máquina o acepte el nombre predeterminado.
Descripción	Incluya un resumen del componente de máquina para proporcionar información a otros arquitectos.
Mostrar ubicación al solicitar	En un entorno de nube, como vCloud Air, esto permite que los usuarios seleccionen una región para sus máquinas aprovisionadas. Para un entorno virtual, como vSphere, puede configurar la función de ubicaciones para permitir a los usuarios seleccionar una ubicación de centro de datos concreta para el aprovisionamiento de una máquina solicitada. Para configurar esta opción completamente, un administrador del sistema debe añadir información de la ubicación del centro de datos al archivo de ubicaciones y un administrador de tejido debe editar un recurso informático para asociarlo a dicha ubicación.
Política de reserva	Aplique una política de reserva a un blueprint para restringir las máquinas aprovisionadas desde ese blueprint a un subconjunto de reservas disponibles. Los administradores de tejido crean políticas de reserva como una opción útil para controlar el procesamiento de las solicitudes de reserva, por ejemplo, para recopilar recursos en grupos para niveles de servicio distintos o para facilitar que un tipo de recurso concreto esté disponible para un fin concreto. Si el administrador de tejido no configuró políticas de reserva, no verá ninguna opción disponible en este menú desplegable. Solo están disponibles las políticas de reserva que corresponden al tenant actual.

Tabla 3-13. Configuración de la pestaña **General** (continuación)

Configuración	Descripción
Prefijo de máquina	<p>Los administradores de tejido crean prefijos de máquina para generar los nombres de las máquinas aprovisionadas. Si selecciona Usar valor predeterminado del grupo, las máquinas aprovisionadas del blueprint reciben sus nombres a partir del prefijo de máquina configurado como predeterminado en el grupo empresarial del usuario. Si no hay ningún prefijo de máquina configurado, se genera uno automáticamente basándose en el nombre del grupo empresarial. Solo están disponibles los prefijos de máquina que corresponden al tenant actual.</p> <p>Si el administrador de tejido configura otros prefijos de máquina que pueden seleccionarse, es posible aplicar un prefijo a todas las máquinas aprovisionadas del blueprint, sea quien sea el solicitante.</p>
Instancias: Mínimo y Máximo	<p>Configure el número máximo y mínimo de instancias que los usuarios pueden seleccionar para una implementación, o para una acción de escalado horizontal o vertical. Si no desea ofrecerles una opción a los usuarios, puede introducir el mismo valor en los campos Mínimo y Máximo para configurar exactamente cuántas instancias aprovisionar y desactivar las acciones de escalado en ese componente de máquina.</p> <p>Los componentes de XaaS no pueden escalarse y no se actualizan durante una operación de escalado. Si utiliza componentes de XaaS en su blueprint, podría crear una acción personalizada para que los usuarios la ejecuten después de una operación de escalado, que podría escalar o actualizar los componentes de XaaS en caso necesario. Como alternativa, podría desactivar las acciones de escalado. Para ello, debe configurar el número exacto de instancias que desea permitir en cada componente de máquina.</p>

Pestaña Información de creación

Configure los ajustes de información de compilación para un componente de máquina de vCloud Air.

Tabla 3-14. Pestaña **Información de creación**

Configuración	Descripción
Tipo de blueprint	Para mantener un registro y administrar las licencias, seleccione si las máquinas aprovisionadas desde este blueprint se clasifican como Escritorio o Servidor.
Acción	<p>Las opciones que aparecen en el menú desplegable dependen del tipo de máquina que haya seleccionado. La única acción de aprovisionamiento disponible para un componente de máquina de vCloud Air es Clonar.</p> <ul style="list-style-type: none"> ■ Clonar <p>Realice copias de una máquina virtual a partir de una plantilla y un objeto de personalización.</p>

Tabla 3-14. Pestaña **Información de creación** (continuación)

Configuración	Descripción
Flujo de trabajo de aprovisionamiento	<p>Las opciones que aparecen en el menú desplegable de flujo de trabajo de aprovisionamiento dependen del tipo de máquina y de la acción que haya seleccionado.</p> <p>La única acción de aprovisionamiento disponible para un componente de máquina de vCloud Air es CloneWorkflow.</p> <p>■ CloneWorkflow</p> <p>Realice copias de una máquina virtual mediante cualquiera de las opciones: Clonar, Clon vinculado o NetApp Flexclone.</p>
Clonar de	<p>Seleccione una plantilla de máquina a partir de la cual clonar. Puede refinar la lista de plantillas disponibles usando la opción Filtros disponible en todos los menús desplegables de las columnas, por ejemplo, la opción de menú Filtros en la columna Nombres.</p> <p>Para Clon vinculado, solo verá las máquinas con snapshots disponibles a partir de los que clonar y que administre como administrador de tenants o administrador de grupo empresarial.</p> <p>Solo puede clonar a partir de las plantillas existentes en las máquinas que administra como administrador de grupo empresarial o como administrador de tenants.</p>

Pestaña **Recursos de máquinas**

Especifique la configuración de CPU, memoria y almacenamiento para el componente de máquina de vCloud Air.

Tabla 3-15. Pestaña **Recursos de máquinas**

Configuración	Descripción
CPU: Mínimo y Máximo	Especifique un número mínimo y un número máximo de CPU que este componente de máquina pueda aprovisionar.
Memoria (MB): Mínimo y Máximo	Especifique una cantidad mínima y máxima de memoria que pueden consumir las máquinas aprovisionadas por este componente de máquina.
Almacenamiento (GB): Mínimo y Máximo	Especifique una cantidad mínima y máxima de almacenamiento que pueden consumir las máquinas aprovisionadas por este componente de máquina. Para vSphere, KVM (RHEV), SCVMM, vCloud Air y vCloud Director, el almacenamiento mínimo se establece en función de lo que indique en la pestaña Almacenamiento.

Pestaña **Almacenamiento**

Para controlar el espacio de almacenamiento, puede añadir al componente de máquina algunas opciones de volumen de almacenamiento, como una o varias políticas de reserva de almacenamiento.

Tabla 3-16. Configuración de la pestaña **Almacenamiento**

Configuración	Descripción
ID	Escriba un ID o nombre del volumen de almacenamiento.
Capacidad (GB)	Especifique la capacidad de almacenamiento del volumen de almacenamiento.
Letra de unidad/Punto de montaje	Especifique una letra de unidad o un punto de montaje del volumen de almacenamiento.
Etiqueta	Especifique una etiqueta para la letra de unidad y el punto de montaje del volumen de almacenamiento.
Política de reserva de almacenamiento	Especifique la política de reserva de almacenamiento existente que se usará con este volumen de almacenamiento. Solo están disponibles las políticas de reserva de almacenamiento que corresponden al tenant actual.
Propiedades personalizadas	Especifique las propiedades de almacenamiento que se usarán con este volumen de almacenamiento.
Máximo de volúmenes	Especifique el número máximo de volúmenes de almacenamiento permitidos que se pueden usar durante el aprovisionamiento desde el componente de máquina. Escriba 0 para evitar que otros usuarios puedan añadir volúmenes de almacenamiento. El valor predeterminado es 60.
Permitir que el usuario vea y cambie las políticas de reserva de almacenamiento	Active esta casilla para permitir que los usuarios eliminen una política de reserva asociada o especifiquen una distinta durante el aprovisionamiento.

Pestaña **Propiedades**

De forma opcional puede especificar la información de grupo de propiedades y de propiedad personalizada del componente de máquina de vCloud Air.

Puede utilizar la pestaña **Propiedades** para añadir al componente de máquina propiedades personalizadas, ya sea de forma individual o en grupos. También puede añadir propiedades personalizadas y grupos de propiedades a todo el blueprint con la pestaña **Propiedades** durante la creación o la edición de un blueprint mediante la página **Propiedades de blueprint**.

Puede utilizar la pestaña **Propiedades personalizadas** para añadir y configurar opciones para las propiedades personalizadas existentes. Las propiedades personalizadas se suministran con vRealize Automation y también se pueden crear definiciones de propiedades.

Tabla 3-17. Configuración de la pestaña **Propiedades > Propiedades personalizadas**

Configuración	Descripción
Nombre	Escriba el nombre de una propiedad personalizada o seleccione una de las propiedades personalizadas disponibles en el menú desplegable. Por ejemplo, escriba el nombre de propiedad personalizada <code>Machine.SSH</code> para especificar si las máquinas aprovisionadas mediante este blueprint permiten las conexiones SSH. Las propiedades solo aparecen en el menú desplegable si el administrador de tenants o de tejido creó definiciones de propiedades.
Valor	Escriba o edite un valor para asociarlo al nombre de propiedad personalizada. Por ejemplo, establezca el valor en <code>true</code> para permitir que los usuarios autorizados se conecten mediante SSH a las máquinas aprovisionadas con su blueprint.
Cifrado	Puede optar por cifrar el valor de la propiedad si, por ejemplo, el valor es una contraseña.
Reemplazable	Puede especificar que la próxima persona u otra más adelante que utilice la propiedad pueda reemplazar el valor de la propiedad. Por lo general, suele ser otro arquitecto, pero, si selecciona Mostrar en solicitud , los usuarios empresariales podrán ver y editar valores de propiedades cuando soliciten elementos del catálogo.
Mostrar en solicitud	Si desea mostrar el nombre y el valor de la propiedad a los usuarios finales, puede seleccionar la opción para mostrar la propiedad en el formulario de solicitud cuando se solicite el aprovisionamiento de la máquina. También debe seleccionar Reemplazable si desea que los usuarios proporcionen un valor.

Puede utilizar la pestaña **Grupos de propiedades** para añadir y configurar opciones para los grupos de propiedades personalizadas existentes. Puede crear sus propios grupos de propiedades o usar los grupos de propiedades creados para que los use.

Tabla 3-18. Configuración de la pestaña **Propiedades > Grupos de propiedades**

Configuración	Descripción
Nombre	Seleccione uno de los grupos de propiedades disponibles en el menú desplegable.
Subir y Bajar	Controle el nivel de prioridad de los grupos de propiedades de la lista en orden descendente. El primer grupo de propiedades de la lista tiene prioridad sobre el siguiente grupo de propiedades de la lista y así sucesivamente.

Tabla 3-18. Configuración de la pestaña **Propiedades > Grupos de propiedades** (continuación)

Configuración	Descripción
Ver propiedades	Visualice las propiedades personalizadas en el grupo de propiedades seleccionado.
Ver propiedades combinadas	Visualice todas las propiedades personalizadas de los grupos de propiedades de la lista en el orden en que aparecen en la lista de grupos de propiedades. Si una misma propiedad aparece en más de un grupo de propiedades, el nombre de la propiedad aparece una sola vez en la lista, según su primera aparición en la misma.

Configuración de componentes de máquina de Amazon

Debe conocer los ajustes y opciones que puede configurar para un componente de máquina de Amazon en el lienzo de diseño de blueprints de vRealize Automation.

Pestaña **General**

Establezca la configuración general de un componente de máquina de Amazon.

Tabla 3-19. Configuración de la pestaña **General**

Configuración	Descripción
ID	Escriba el nombre del componente de máquina o acepte el nombre predeterminado.
Descripción	Incluya un resumen del componente de máquina para proporcionar información a otros arquitectos.
Mostrar ubicación al solicitar	En un entorno de nube, como vCloud Air, esto permite que los usuarios seleccionen una región para sus máquinas aprovisionadas. Para un entorno virtual, como vSphere, puede configurar la función de ubicaciones para permitir a los usuarios seleccionar una ubicación de centro de datos concreta para el aprovisionamiento de una máquina solicitada. Para configurar esta opción completamente, un administrador del sistema debe añadir información de la ubicación del centro de datos al archivo de ubicaciones y un administrador de tejido debe editar un recurso informático para asociarlo a dicha ubicación.
Política de reserva	Aplique una política de reserva a un blueprint para restringir las máquinas aprovisionadas desde ese blueprint a un subconjunto de reservas disponibles. Los administradores de tejido crean políticas de reserva como una opción útil para controlar el procesamiento de las solicitudes de reserva, por ejemplo, para recopilar recursos en grupos para niveles de servicio distintos o para facilitar que un tipo de recurso concreto esté disponible para un fin concreto. Si el administrador de tejido no configuró políticas de reserva, no verá ninguna opción disponible en este menú desplegable. Solo están disponibles las políticas de reserva que corresponden al tenant actual.

Tabla 3-19. Configuración de la pestaña **General** (continuación)

Configuración	Descripción
Prefijo de máquina	<p>Los administradores de tejido crean prefijos de máquina para generar los nombres de las máquinas aprovisionadas. Si selecciona Usar valor predeterminado del grupo, las máquinas aprovisionadas del blueprint reciben sus nombres a partir del prefijo de máquina configurado como predeterminado en el grupo empresarial del usuario. Si no hay ningún prefijo de máquina configurado, se genera uno automáticamente basándose en el nombre del grupo empresarial. Solo están disponibles los prefijos de máquina que corresponden al tenant actual.</p> <p>Si el administrador de tejido configura otros prefijos de máquina que pueden seleccionarse, es posible aplicar un prefijo a todas las máquinas aprovisionadas del blueprint, sea quien sea el solicitante.</p>
Instancias: Mínimo y Máximo	<p>Configure el número máximo y mínimo de instancias que los usuarios pueden seleccionar para una implementación, o para una acción de escalado horizontal o vertical. Si no desea ofrecerles una opción a los usuarios, puede introducir el mismo valor en los campos Mínimo y Máximo para configurar exactamente cuántas instancias aprovisionar y desactivar las acciones de escalado en ese componente de máquina.</p> <p>Los componentes de XaaS no pueden escalarse y no se actualizan durante una operación de escalado. Si utiliza componentes de XaaS en su blueprint, podría crear una acción personalizada para que los usuarios la ejecuten después de una operación de escalado, que podría escalar o actualizar los componentes de XaaS en caso necesario. Como alternativa, podría desactivar las acciones de escalado. Para ello, debe configurar el número exacto de instancias que desea permitir en cada componente de máquina.</p>

Pestaña Información de creación

Establezca la configuración de información de creación de un componente de máquina de Amazon.

Tabla 3-20. Pestaña Información de creación

Configuración	Descripción
Tipo de blueprint	Para mantener un registro y administrar las licencias, seleccione si las máquinas aprovisionadas desde este blueprint se clasifican como Escritorio o Servidor.
Flujo de trabajo de aprovisionamiento	<p>El único flujo de trabajo de aprovisionamiento disponible para un componente de máquina de Amazon es CloudProvisioningWorkflow.</p> <ul style="list-style-type: none"> ■ CloudProvisioningWorkflow <p>Cree una máquina iniciándola desde una instancia de máquina virtual o una imagen de nube.</p>

Tabla 3-20. Pestaña Información de creación (continuación)

Configuración	Descripción
Imagen de máquina de Amazon	<p>Seleccione una imagen de máquina de Amazon disponible. Una imagen de máquina de Amazon es una plantilla que contiene una configuración de software, incluido un sistema operativo. Las imágenes de máquina se administran mediante cuentas de Amazon Web Services. Puede refinar la lista de nombres de imágenes de máquinas de Amazon que se muestra utilizando la opción Filtros en el menú desplegable de la columna ID de AMI.</p>
Par de claves	<p>Los pares de claves son necesarios para el aprovisionamiento con Amazon Web Services.</p> <p>Los pares de claves sirven para aprovisionar y conectarse a una instancia en la nube. También se usan para descifrar contraseñas de Windows y para iniciar sesión en una máquina de Linux.</p> <p>Dispone de las siguientes opciones de pares de claves:</p> <ul style="list-style-type: none"> ■ Sin especificar <p>Controla el comportamiento del par de claves en el nivel de blueprint en vez del nivel de reserva.</p> ■ Autogenerado por cada grupo empresarial <p>Especifica que cada máquina aprovisionada del mismo grupo empresarial tiene el mismo par de claves, incluidas las máquinas aprovisionadas en otras reservas cuando la máquina tiene el mismo recurso informático y el mismo grupo empresarial. Como los pares de claves están asociados a un grupo empresarial, se eliminan cuando se elimina el grupo empresarial.</p> ■ Autogenerado por cada máquina <p>Especifica que cada máquina tiene un par de claves único. La opción Autogenerado por cada máquina es el método más seguro porque no se comparten pares de claves entre máquinas.</p>
Habilitar opciones de red de Amazon en la máquina	<p>Elija si desea permitir que los usuarios aprovisionen una máquina en una Virtual Private Cloud (VPC) o en una ubicación no de VPC cuando envíen la solicitud.</p>
Tipos de instancia	<p>Seleccione uno o más tipos de instancia de Amazon. Una instancia de Amazon es un servidor virtual que puede ejecutar aplicaciones en Amazon Web Services. Las instancias se crean a partir de una imagen de máquina de Amazon, y mediante la selección de un tipo de instancia apropiado. vRealize Automation administra los tipos de instancia de imagen de máquina disponibles para el aprovisionamiento.</p> <p>Para obtener información sobre cómo usar los tipos de instancia de Amazon en vRealize Automation, consulte Explicación de los tipos de instancia de Amazon y Añadir un tipo de instancia de Amazon.</p>

Pestaña **Recursos de máquinas**

Especifique la configuración de CPU, memoria, almacenamiento y volumen de EBS para el componente de máquina de Amazon.

También puede volver a configurar todos los volúmenes de almacenamiento de máquinas de Amazon de la implementación, a excepción del volumen raíz.

Tabla 3-21. Pestaña **Recursos de máquinas**

Configuración	Descripción
CPU: Mínimo y Máximo	Especifique un número mínimo y un número máximo de CPU que este componente de máquina pueda aprovisionar.
Memoria (MB): Mínimo y Máximo	Especifique una cantidad mínima y máxima de memoria que pueden consumir las máquinas aprovisionadas por este componente de máquina.
Almacenamiento (GB): Mínimo y Máximo	Especifique una cantidad mínima y máxima de almacenamiento que pueden consumir las máquinas aprovisionadas por este componente de máquina. Para vSphere, KVM (RHEV), SCVMM, vCloud Air y vCloud Director, el almacenamiento mínimo se establece en función de lo que indique en la pestaña Almacenamiento.
Almacenamiento de EBS (GB): Mínimo y Máximo	<p>Especifique una cantidad mínima y máxima de volumen de almacenamiento en Amazon Elastic Block Store (EBS) que pueden consumir los recursos de máquinas aprovisionadas por este componente de máquina.</p> <p>Al destruir una implementación que contiene un componente de máquina de Amazon, se desconectan todos los volúmenes de EBS que se agregaron a la máquina durante este ciclo de vida, en lugar de destruirse. vRealize Automation no proporciona una opción para destruir los volúmenes de EBS.</p>

Pestaña **Propiedades**

Si lo prefiere, especifique la información de propiedades personalizadas y grupos de propiedades para el componente de máquina de Amazon.

Puede utilizar la pestaña **Propiedades** para añadir al componente de máquina propiedades personalizadas, ya sea de forma individual o en grupos. También puede añadir propiedades personalizadas y grupos de propiedades a todo el blueprint con la pestaña **Propiedades** durante la creación o la edición de un blueprint mediante la página **Propiedades de blueprint**.

Puede utilizar la pestaña **Propiedades personalizadas** para añadir y configurar opciones para las propiedades personalizadas existentes. Las propiedades personalizadas se suministran con vRealize Automation y también se pueden crear definiciones de propiedades.

Tabla 3-22. Configuración de la pestaña **Propiedades > Propiedades personalizadas**

Configuración	Descripción
Nombre	Escriba el nombre de una propiedad personalizada o seleccione una de las propiedades personalizadas disponibles en el menú desplegable. Por ejemplo, escriba el nombre de propiedad personalizada <code>Machine.SSH</code> para especificar si las máquinas aprovisionadas mediante este blueprint permiten las conexiones SSH. Las propiedades solo aparecen en el menú desplegable si el administrador de tenants o de tejido creó definiciones de propiedades.
Valor	Escriba o edite un valor para asociarlo al nombre de propiedad personalizada. Por ejemplo, establezca el valor en <code>true</code> para permitir que los usuarios autorizados se conecten mediante SSH a las máquinas aprovisionadas con su blueprint.
Cifrado	Puede optar por cifrar el valor de la propiedad si, por ejemplo, el valor es una contraseña.
Reemplazable	Puede especificar que la próxima persona u otra más adelante que utilice la propiedad pueda reemplazar el valor de la propiedad. Por lo general, suele ser otro arquitecto, pero, si selecciona Mostrar en solicitud , los usuarios empresariales podrán ver y editar valores de propiedades cuando soliciten elementos del catálogo.
Mostrar en solicitud	Si desea mostrar el nombre y el valor de la propiedad a los usuarios finales, puede seleccionar la opción para mostrar la propiedad en el formulario de solicitud cuando se solicite el aprovisionamiento de la máquina. También debe seleccionar Reemplazable si desea que los usuarios proporcionen un valor.

Puede utilizar la pestaña **Grupos de propiedades** para añadir y configurar opciones para los grupos de propiedades personalizadas existentes. Puede crear sus propios grupos de propiedades o usar los grupos de propiedades creados para que los use.

Tabla 3-23. Configuración de la pestaña **Propiedades > Grupos de propiedades**

Configuración	Descripción
Nombre	Seleccione uno de los grupos de propiedades disponibles en el menú desplegable.
Subir y Bajar	Controle el nivel de prioridad de los grupos de propiedades de la lista en orden descendente. El primer grupo de propiedades de la lista tiene prioridad sobre el siguiente grupo de propiedades de la lista y así sucesivamente.

Tabla 3-23. Configuración de la pestaña **Propiedades > Grupos de propiedades** (continuación)

Configuración	Descripción
Ver propiedades	Visualice las propiedades personalizadas en el grupo de propiedades seleccionado.
Ver propiedades combinadas	Visualice todas las propiedades personalizadas de los grupos de propiedades de la lista en el orden en que aparecen en la lista de grupos de propiedades. Si una misma propiedad aparece en más de un grupo de propiedades, el nombre de la propiedad aparece una sola vez en la lista, según su primera aparición en la misma.

Configuración de componentes de máquina de OpenStack

Conozca los ajustes y las opciones que puede configurar para un componente de máquina de OpenStack en el lienzo de diseño de blueprints de vRealize Automation.

Pestaña **General**

Configure los ajustes generales para un componente de máquina de OpenStack.

Tabla 3-24. Configuración de la pestaña **General**

Configuración	Descripción
ID	Escriba el nombre del componente de máquina o acepte el nombre predeterminado.
Descripción	Incluya un resumen del componente de máquina para proporcionar información a otros arquitectos.
Mostrar ubicación al solicitar	En un entorno de nube, como vCloud Air, esto permite que los usuarios seleccionen una región para sus máquinas aprovisionadas. Para un entorno virtual, como vSphere, puede configurar la función de ubicaciones para permitir a los usuarios seleccionar una ubicación de centro de datos concreta para el aprovisionamiento de una máquina solicitada. Para configurar esta opción completamente, un administrador del sistema debe añadir información de la ubicación del centro de datos al archivo de ubicaciones y un administrador de tejido debe editar un recurso informático para asociarlo a dicha ubicación.
Política de reserva	Aplique una política de reserva a un blueprint para restringir las máquinas aprovisionadas desde ese blueprint a un subconjunto de reservas disponibles. Los administradores de tejido crean políticas de reserva como una opción útil para controlar el procesamiento de las solicitudes de reserva, por ejemplo, para recopilar recursos en grupos para niveles de servicio distintos o para facilitar que un tipo de recurso concreto esté disponible para un fin concreto. Si el administrador de tejido no configuró políticas de reserva, no verá ninguna opción disponible en este menú desplegable. Solo están disponibles las políticas de reserva que corresponden al tenant actual.

Tabla 3-24. Configuración de la pestaña **General** (continuación)

Configuración	Descripción
Prefijo de máquina	<p>Los administradores de tejido crean prefijos de máquina para generar los nombres de las máquinas aprovisionadas. Si selecciona Usar valor predeterminado del grupo, las máquinas aprovisionadas del blueprint reciben sus nombres a partir del prefijo de máquina configurado como predeterminado en el grupo empresarial del usuario. Si no hay ningún prefijo de máquina configurado, se genera uno automáticamente basándose en el nombre del grupo empresarial. Solo están disponibles los prefijos de máquina que corresponden al tenant actual.</p> <p>Si el administrador de tejido configura otros prefijos de máquina que pueden seleccionarse, es posible aplicar un prefijo a todas las máquinas aprovisionadas del blueprint, sea quien sea el solicitante.</p>
Instancias: Mínimo y Máximo	<p>Configure el número máximo y mínimo de instancias que los usuarios pueden seleccionar para una implementación, o para una acción de escalado horizontal o vertical. Si no desea ofrecerles una opción a los usuarios, puede introducir el mismo valor en los campos Mínimo y Máximo para configurar exactamente cuántas instancias aprovisionar y desactivar las acciones de escalado en ese componente de máquina.</p> <p>Los componentes de XaaS no pueden escalarse y no se actualizan durante una operación de escalado. Si utiliza componentes de XaaS en su blueprint, podría crear una acción personalizada para que los usuarios la ejecuten después de una operación de escalado, que podría escalar o actualizar los componentes de XaaS en caso necesario. Como alternativa, podría desactivar las acciones de escalado. Para ello, debe configurar el número exacto de instancias que desea permitir en cada componente de máquina.</p>

Pestaña Información de creación

Configure las opciones de información de compilación para un componente de máquina de OpenStack.

Tabla 3-25. Pestaña Información de creación

Configuración	Descripción
Tipo de blueprint	Para mantener un registro y administrar las licencias, seleccione si las máquinas aprovisionadas desde este blueprint se clasifican como Escritorio o Servidor.
Flujo de trabajo de aprovisionamiento	<p>Estos son los flujos de trabajo de aprovisionamiento disponibles para un componente de máquina de OpenStack:</p> <ul style="list-style-type: none"> ■ CloudLinuxKickstartWorkflow Aprovisionar una máquina mediante el arranque desde una imagen ISO usando un archivo de configuración Kickstart o autoYaST y una imagen de distribución Linux para instalar el sistema operativo en la máquina. ■ CloudProvisioningWorkflow Cree una máquina iniciándola desde una instancia de máquina virtual o una imagen de nube. ■ CloudWIMImageWorkflow Aprovisionar una máquina mediante el arranque en un entorno WinPE y la instalación de un sistema operativo usando una imagen Windows Imaging File Format (WIM) de una máquina de referencia Windows existente. Cuando utilice un flujo de trabajo de aprovisionamiento de WIM en un blueprint, especifique un valor de almacenamiento que tenga en cuenta el tamaño de todos los discos que se usarán en la máquina. Use el valor total de todos los discos como valor de almacenamiento mínimo del componente de máquina. Especifique además un tamaño para cada disco con capacidad suficiente para dar cabida al sistema operativo.
Imagen de OpenStack	Seleccione una imagen de OpenStack disponible. Una imagen de OpenStack es una plantilla que contiene una configuración de software, incluido un sistema operativo. Las imágenes se administran mediante cuentas de OpenStack. Puede refinar la lista de nombres de imágenes de OpenStack que se muestra utilizando la opción Filtros en el menú desplegable de la columna Nombres .

Tabla 3-25. Pestaña **Información de creación** (continuación)

Configuración	Descripción
Par de claves	<p>Los pares de claves son opcionales para el aprovisionamiento con OpenStack.</p> <p>Los pares de claves sirven para aprovisionar y conectarse a una instancia en la nube. También se usan para descifrar contraseñas de Windows y para iniciar sesión en una máquina de Linux.</p> <p>Dispone de las siguientes opciones de pares de claves:</p> <ul style="list-style-type: none"> ■ Sin especificar <p>Controla el comportamiento del par de claves en el nivel de blueprint en vez del nivel de reserva.</p> ■ Autogenerado por cada grupo empresarial <p>Especifica que cada máquina aprovisionada del mismo grupo empresarial tiene el mismo par de claves, incluidas las máquinas aprovisionadas en otras reservas cuando la máquina tiene el mismo recurso informático y el mismo grupo empresarial. Como los pares de claves están asociados a un grupo empresarial, se eliminan cuando se elimina el grupo empresarial.</p> ■ Autogenerado por cada máquina <p>Especifica que cada máquina tiene un par de claves único. La opción Autogenerado por cada máquina es el método más seguro porque no se comparten pares de claves entre máquinas.</p>
Tipos	<p>Seleccione uno o varios tipos de OpenStack. Un tipo de OpenStack es una plantilla de hardware virtual donde se definen las especificaciones de recurso de máquina de las instancias aprovisionadas en OpenStack. Los tipos se administran mediante el proveedor de OpenStack y se importan durante la recopilación de datos.</p>

Pestaña **Recursos de máquinas**

Especifique la configuración de CPU, memoria y almacenamiento para el componente de máquina de OpenStack.

Tabla 3-26. Pestaña **Recursos de máquinas**

Configuración	Descripción
CPU: Mínimo y Máximo	Especifique un número mínimo y un número máximo de CPU que este componente de máquina pueda aprovisionar.
Memoria (MB): Mínimo y Máximo	Especifique una cantidad mínima y máxima de memoria que pueden consumir las máquinas aprovisionadas por este componente de máquina.
Almacenamiento (GB): Mínimo y Máximo	Especifique una cantidad mínima y máxima de almacenamiento que pueden consumir las máquinas aprovisionadas por este componente de máquina. Para vSphere, KVM (RHEV), SCVMM, vCloud Air y vCloud Director, el almacenamiento mínimo se establece en función de lo que indique en la pestaña Almacenamiento. Cuando utilice un flujo de trabajo de aprovisionamiento de WIM en un blueprint, especifique un valor de almacenamiento que tenga en cuenta el tamaño de todos los discos que se usarán en la máquina. Use el valor total de todos los discos como valor de almacenamiento mínimo del componente de máquina. Especifique además un tamaño para cada disco con capacidad suficiente para dar cabida al sistema operativo.

Pestaña **Propiedades**

De forma opcional puede especificar la información de grupo de propiedades y de propiedad personalizada del componente de máquina de OpenStack.

Puede utilizar la pestaña **Propiedades** para añadir al componente de máquina propiedades personalizadas, ya sea de forma individual o en grupos. También puede añadir propiedades personalizadas y grupos de propiedades a todo el blueprint con la pestaña **Propiedades** durante la creación o la edición de un blueprint mediante la página **Propiedades de blueprint**.

Puede utilizar la pestaña **Propiedades personalizadas** para añadir y configurar opciones para las propiedades personalizadas existentes. Las propiedades personalizadas se suministran con vRealize Automation y también se pueden crear definiciones de propiedades.

Tabla 3-27. Configuración de la pestaña **Propiedades > Propiedades personalizadas**

Configuración	Descripción
Nombre	Escriba el nombre de una propiedad personalizada o seleccione una de las propiedades personalizadas disponibles en el menú desplegable. Por ejemplo, escriba el nombre de propiedad personalizada <code>Machine.SSH</code> para especificar si las máquinas aprovisionadas mediante este blueprint permiten las conexiones SSH. Las propiedades solo aparecen en el menú desplegable si el administrador de tenants o de tejido creó definiciones de propiedades.
Valor	Escriba o edite un valor para asociarlo al nombre de propiedad personalizada. Por ejemplo, establezca el valor en <code>true</code> para permitir que los usuarios autorizados se conecten mediante SSH a las máquinas aprovisionadas con su blueprint.
Cifrado	Puede optar por cifrar el valor de la propiedad si, por ejemplo, el valor es una contraseña.
Reemplazable	Puede especificar que la próxima persona u otra más adelante que utilice la propiedad pueda reemplazar el valor de la propiedad. Por lo general, suele ser otro arquitecto, pero, si selecciona Mostrar en solicitud , los usuarios empresariales podrán ver y editar valores de propiedades cuando soliciten elementos del catálogo.
Mostrar en solicitud	Si desea mostrar el nombre y el valor de la propiedad a los usuarios finales, puede seleccionar la opción para mostrar la propiedad en el formulario de solicitud cuando se solicite el aprovisionamiento de la máquina. También debe seleccionar Reemplazable si desea que los usuarios proporcionen un valor.

Puede utilizar la pestaña **Grupos de propiedades** para añadir y configurar opciones para los grupos de propiedades personalizadas existentes. Puede crear sus propios grupos de propiedades o usar los grupos de propiedades creados para que los use.

Tabla 3-28. Configuración de la pestaña **Propiedades > Grupos de propiedades**

Configuración	Descripción
Nombre	Seleccione uno de los grupos de propiedades disponibles en el menú desplegable.
Subir y Bajar	Controle el nivel de prioridad de los grupos de propiedades de la lista en orden descendente. El primer grupo de propiedades de la lista tiene prioridad sobre el siguiente grupo de propiedades de la lista y así sucesivamente.

Tabla 3-28. Configuración de la pestaña **Propiedades > Grupos de propiedades** (continuación)

Configuración	Descripción
Ver propiedades	Visualice las propiedades personalizadas en el grupo de propiedades seleccionado.
Ver propiedades combinadas	Visualice todas las propiedades personalizadas de los grupos de propiedades de la lista en el orden en que aparecen en la lista de grupos de propiedades. Si una misma propiedad aparece en más de un grupo de propiedades, el nombre de la propiedad aparece una sola vez en la lista, según su primera aparición en la misma.

Usar propiedades personalizadas de red

Puede especificar la información de red y seguridad para los componentes de máquina que no sean de vSphere y los blueprints que no contengan NSX mediante propiedades personalizadas de red en el nivel de componente del blueprint o la máquina.

Los componentes **Redes y seguridad** están disponibles para su utilización únicamente con componentes de máquina de vSphere. Los componentes de máquina que no son de vSphere no contienen las pestañas **Red** o **Seguridad**.

En los componentes de máquina que carecen de la pestaña **Red** o **Seguridad**, puede añadir propiedades personalizadas de redes y seguridad, como `VirtualMachine.Network0.Name` a sus correspondientes pestañas **Propiedades** en el lienzo. Las propiedades de red, seguridad y equilibrador de carga de NSX solo son aplicables a las máquinas de vSphere.

Para definir propiedades personalizadas, de forma individual o como parte de un grupo de propiedades existente, utilice la pestaña **Propiedades** cuando configure un componente de máquina en el lienzo de diseño. Las propiedades personalizadas que defina para un componente de máquina pertenecen a las máquinas de ese tipo que se hayan aprovisionado desde el blueprint.

Para obtener información sobre las propiedades personalizadas disponibles, consulte *Referencia de propiedades personalizadas*.

Solucionar problemas de blueprints de clon o clon vinculado

Faltan máquinas o plantillas durante la creación de un blueprint de clon o clon vinculado. Se produce un error de aprovisionamiento de máquinas cuando se usa el blueprint de clon compartido para solicitar máquinas.

Problema

Al trabajar con blueprints de clon o clon vinculado, puede encontrarse con alguno de estos problemas:

- Al crear un blueprint de clon vinculado, no aparece ninguna máquina en la lista para clonar o la máquina que desea clonar no aparece.
- Al crear un blueprint de clon, no aparece ninguna plantilla en la lista de plantillas para clonar o la plantilla que desea no aparece.

- Al solicitar máquinas mediante el blueprint de clon compartido, el aprovisionamiento no se realiza correctamente.
- Debido a la duración de la recopilación de datos, los usuarios pueden ver una plantilla que se ha eliminado cuando crean o editan blueprints de clon vinculado.

Causa

Existen varias causas posibles para los problemas habituales de blueprints de clon y clon vinculado.

Para obtener información relacionada con las opciones **Clonar de** y **Clonar desde snapshot** con **Usar snapshot actual** que están disponibles cuando se crean blueprints, consulte [Configuración de los componentes de máquina de vSphere](#).

Tabla 3-29. Causas de los problemas habituales de blueprints de clon y clon vinculado

Problema	Causa	Solución
Faltan máquinas	Solo puede crear blueprints de clon vinculado con las máquinas que administra como administrador de tenants o como administrador de grupo empresarial.	Un usuario de su tenant o grupo empresarial debe solicitar una máquina de vSphere. Puede hacerlo usted mismo si cuenta con las funciones adecuadas. En este cuadro de diálogo, también se ven las máquinas no administradas. Puede que las máquinas administradas se hayan importado. No es necesario aprovisionar las máquinas desde vRealize Automation para que se vean en el cuadro de diálogo.
Faltan plantillas	Se ha producido un error durante la recopilación de datos en un endpoint determinado, o no hay endpoints disponibles para la plataforma del componente.	<ul style="list-style-type: none"> ■ Si sus endpoints están agrupados en clúster y contienen varios recursos informáticos, compruebe que su administrador de IaaS haya añadido el clúster que contiene las plantillas a su grupo de tejido. ■ En las plantillas nuevas, compruebe que el personal de TI colocó las plantillas en el mismo clúster incluido en su grupo de tejido.
Error de aprovisionamiento con un blueprint compartido	En los blueprints, no existe ninguna validación que garantice que la plantilla seleccionada existe en la reserva que se usa para aprovisionar una máquina de un blueprint de clon compartido.	Considere la posibilidad de usar autorizaciones para restringir el blueprint a los usuarios que tengan una reserva en el recurso informático donde existe la plantilla.

Tabla 3-29. Causas de los problemas habituales de blueprints de clon y clon vinculado (continuación)

Problema	Causa	Solución
Error de aprovisionamiento con un agente invitado	La máquina virtual podría reiniciarse inmediatamente después de finalizar la personalización del sistema operativo invitado, pero antes de que se completen los elementos de trabajo del agente invitado, lo que provocaría un error de aprovisionamiento. Puede usar la propiedad personalizada <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> para aumentar el tiempo de retraso.	Compruebe que ha añadido la propiedad personalizada <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> . Este valor debe tener el formato HH:MM:SS. Si no se establece ningún valor, el valor predeterminado es un minuto (00:01:00).
Error de aprovisionamiento del clon vinculado cuando se utiliza SDRS	Cuando utilice el aprovisionamiento de clon vinculado y SDRS, la nueva máquina debe residir en el mismo clúster. Se produce un error de aprovisionamiento si los discos de la máquina de origen están en un clúster y usted solicita el aprovisionamiento de una máquina en un clúster diferente.	Cuando utilice SDRS y el aprovisionamiento del clon vinculado, aprovisiona las máquinas en el mismo clúster que el origen de clon vinculado. No aprovisiona en un clúster diferente.
Se produce un error durante el aprovisionamiento de blueprint de clon o de clon vinculado debido a que no se encuentra la plantilla en la que se basa el clon	No se pueden aprovisionar máquinas desde un blueprint que se ha clonado a partir de una plantilla que ya no existe. vRealize Automation ejecuta la recopilación de datos de forma periódica (24 horas de forma predeterminada). Si se elimina una plantilla, el cambio no se refleja hasta la siguiente recopilación de datos, por lo que es posible crear un blueprint basado en una plantilla que no existe.	Vuelva a definir el blueprint mediante una plantilla existente y, a continuación, solicite el aprovisionamiento. Como precaución, y si es posible, puede ejecutar la recopilación de datos antes de definir el blueprint de clon o de clon vinculado.

Diseñar blueprints con la configuración de NSX

Si tiene una instancia de NSX integrada con vRealize Automation, puede configurar los blueprints de vSphere para aprovechar la virtualización de red y seguridad de NSX.

Si ha configurado la integración de vRealize Automation con NSX, puede usar los componentes de red, seguridad y equilibrador de carga del lienzo de diseño para configurar el blueprint para el aprovisionamiento de máquinas. También puede añadir las siguientes opciones de configuración de red y seguridad de NSX a todo el blueprint cuando cree un nuevo blueprint o cuando edite uno existente.

- **Zona de transporte:** contiene las redes usadas para la implementación de máquinas aprovisionadas.
- **Política de reserva de puerta de enlace enrutada y de Edge:** administra la comunicación de red para la implementación de la máquina aprovisionada.
- **Aislamiento de aplicaciones:** solo permite el tráfico interno entre máquinas usadas en la implementación de la máquina aprovisionada.

Para obtener información adicional sobre la integración de vRealize Automation y NSX, y sobre el uso de los componentes de red y seguridad de NSX en el blueprint de vRealize Automation, consulte el artículo de blog que presenta una [introducción a la automatización de red y seguridad para vRA y NSX](#).

La configuración de NSX solo se aplica a los tipos de componente de máquina de vSphere.

Configuración de las páginas Nuevo blueprint y Propiedades de blueprint con NSX

Se puede especificar una configuración que se aplique a todo el blueprint, incluidas algunas opciones de NSX, en la página **Nuevo blueprint** cuando se crea el blueprint. Después de crear el blueprint, edite estas opciones en la página Propiedades de blueprint.

Pestaña **General**

Aplique las opciones de configuración en todo el blueprint, incluidos todos los componentes que desea añadir en este momento o posteriormente.

Tabla 3-30. Configuración de la pestaña **General**

Configuración	Descripción
Nombre	Escriba un nombre para el blueprint.
Identificador	El campo de identificador se rellena automáticamente en función del nombre que haya introducido. Si desea editar este campo, hágalo ahora, pues en cuanto guarde el blueprint ya no podrá cambiarlo. Dado que los identificadores son permanentes y únicos en el tenant, puede usarlos para interactuar con los blueprints mediante programación y para crear enlaces de propiedades.
Descripción	Incluya un resumen del blueprint para proporcionar información a otros arquitectos. Además, los usuarios verán esta descripción en el formulario de solicitud.
Límite de implementaciones	Especifique el número máximo de implementaciones que pueden crearse cuando se usa este blueprint para aprovisionar máquinas.
Días de concesión: Mínimo y Máximo	Establezca un valor mínimo y un valor máximo para permitir a los usuarios elegir entre un rango de duraciones de concesión. Cuando finaliza la concesión, la implementación se destruye o se archiva. Si no especifica un valor mínimo o un valor máximo, la concesión nunca caducará.

Tabla 3-30. Configuración de la pestaña **General** (continuación)

Configuración	Descripción
Días de archivado	Puede especificar un período de archivado para conservar las implementaciones de forma temporal en lugar de destruirlas cuando caduque su concesión. Especifique 0 (valor predeterminado) para destruir la implementación cuando caduque su concesión. El período de archivado comienza el día que caduca la concesión. Cuando finaliza el período de archivado, la implementación se destruye.
Propagar actualizaciones a implementaciones existentes	<p>Cuando se activa, especifica que cualquier ampliación de los límites de los valores máximos o mínimos de la CPU, la memoria y el almacenamiento del blueprint se insertarán en todas las implementaciones activas aprovisionadas desde el blueprint. Por ejemplo, si especifica un mínimo de 2 y un máximo de 4 (2,4) en un principio, un cambio a (1,4) o (2,5) surte efecto tras la reconfiguración, pero un cambio a (3,4) o (2,3) no se aplica.</p> <p>Los cambios surten efecto después de la siguiente acción de reconfiguración. Para obtener información relacionada con las acciones de reconfiguración, consulte Comandos del menú Acción en recursos aprovisionados.</p>

Pestaña Configuración de NSX

Si ha configurado NSX, puede especificar la configuración de la zona de transporte, la política de reserva de puerta de enlace enrutada y de Edge, y el aislamiento de aplicaciones de NSX cuando cree o edite un blueprint. Estas opciones de configuración están disponibles en la pestaña **Configuración de NSX** de las páginas **Blueprint** y **Propiedades de blueprint**.

Para obtener información sobre cómo configurar NSX, consulte la *guía de administración de NSX*.

Tabla 3-31. Configuración de la pestaña **Configuración de NSX**

Configuración	Descripción
Zona de transporte	<p>Seleccione una zona de transporte de NSX existente para incluir la red o las redes que puede usar la implementación de máquina aprovisionada.</p> <p>Una zona de transporte define los clústeres que pueden abarcar las redes. Cuando se aprovisionan máquinas, si se especifica una zona de transporte en una reserva y en un blueprint, los valores de la zona de transporte deben coincidir. Solo están disponibles las zonas de transporte que corresponden al tenant actual.</p> <p>Una zona de transporte solo se requiere en los blueprints que tienen una red a petición. En los grupos de seguridad, etiquetas de seguridad y equilibradores de carga, la zona de transporte es opcional. Si no especifica ninguna zona de transporte, el endpoint está determinado por la ubicación del grupo de seguridad, la etiqueta de seguridad o la red a la que se conecta el equilibrador de carga.</p>
Política de reserva de puerta de enlace enrutada y de Edge	<p>Seleccione una política de reserva de puerta de enlace enrutada o de NSX Edge. Esta política de reserva se aplica a las puertas de enlace enrutadas y a todos los Edges que se implementan como parte del aprovisionamiento. Solo hay un Edge aprovisionado por cada implementación.</p> <p>En el caso de las redes enrutadas, no se aprovisionan los Edges, pero puede usar una política de reserva para seleccionar una reserva con las puertas de enlace enrutadas que se usarán para el aprovisionamiento de la red enrutada.</p> <p>Cuando vRealize Automation aprovisiona una máquina con redes NAT o enrutadas, aprovisiona una puerta de enlace enrutada como enrutador de red. Esta puerta de enlace enrutada o de Edge es una máquina de administración que consume recursos informáticos como otras máquinas virtuales, pero que también se encarga de administrar las comunicaciones de red de todas las máquinas de la implementación. La reserva empleada para aprovisionar la puerta de enlace enrutada o de Edge determina la red externa que se usa para las direcciones IP virtuales del equilibrador de carga y NAT. El procedimiento recomendado es usar clústeres de administración independientes para las máquinas de administración, como los NSX Edges.</p>
Aislamiento de aplicaciones	<p>Active la casilla Aislamiento de aplicaciones para usar la política de seguridad de aislamiento de aplicaciones configurada en NSX. La política de aislamiento de aplicaciones se aplica a todos los componentes de máquinas de vSphere en el blueprint. Si lo prefiere, puede añadir etiquetas y grupos de seguridad de NSX para permitir que vRealize Orchestrator abra la configuración de redes aisladas y puedan incluirse o quitarse rutas adicionales en el aislamiento de aplicaciones.</p>

Pestaña **Propiedades**

Las propiedades personalizadas que añada al blueprint se aplican a todo el blueprint, incluidos todos sus componentes. Sin embargo, pueden reemplazarse con propiedades personalizadas asignadas posteriormente en la cadena de prioridad. Para obtener más información sobre el orden de prioridad de las propiedades personalizadas, consulte *Referencia de propiedades personalizadas*.

Tabla 3-32. Configuración de la pestaña **Propiedades**

Pestaña	Configuración	Descripción
Grupos de propiedades		Los grupos de propiedades son grupos reutilizables de propiedades que se han diseñado para simplificar el proceso de adición de propiedades personalizadas a los blueprints. Los administradores de tenant y de tejido pueden agrupar las propiedades que se suelen utilizar juntas para poder añadir el grupo de propiedades a un blueprint en lugar de insertar propiedades personalizadas una por una.
	Añadir	<p>Añada uno o varios grupos de propiedades existentes y aplíquelos a todo el blueprint.</p> <p>Se proporcionan los siguientes grupos de propiedades relacionados con contenedores:</p> <ul style="list-style-type: none"> ■ Propiedades del host de contenedor con autenticación con certificado ■ Propiedades del host de contenedor con autenticación con usuario/contraseña
	Subir /Bajar	Establezca una prioridad de los grupos para controlar el orden de prioridad de cada grupo de propiedades con respecto de los demás. El primer grupo de la lista es el que tiene mayor prioridad y sus propiedades personalizadas ocupan el primer puesto en el orden de prioridad. Si desea cambiar el orden, solo tiene que arrastrar y soltar.
	Ver propiedades	Visualice las propiedades personalizadas en el grupo de propiedades seleccionado.
	Ver propiedades combinadas	Si la propiedad personalizada está incluida en más de un grupo de propiedades, tendrá prioridad el valor incluido en el grupo de propiedades cuya prioridad sea mayor. Puede ver estas propiedades combinadas para establecer el orden de prioridad de los grupos de propiedades.
Propiedades personalizadas		Puede añadir propiedades personalizadas individuales en lugar de grupos de propiedades.
	Nuevo	Añada una propiedad personalizada individual y aplíquela a todo el blueprint.

Tabla 3-32. Configuración de la pestaña **Propiedades** (continuación)

Pestaña	Configuración	Descripción
	Nombre	Escriba el nombre de la propiedad. Para obtener una lista de las propiedades personalizadas y sus definiciones, consulte <i>Referencia de propiedades personalizadas</i> .
	Valor	Introduzca el valor de la propiedad personalizada.
	Cifrado	Puede optar por cifrar el valor de la propiedad si, por ejemplo, el valor es una contraseña.
	Reemplazable	Puede especificar que la próxima persona u otra más adelante que utilice la propiedad pueda reemplazar el valor de la propiedad. Por lo general, suele ser otro arquitecto, pero, si selecciona Mostrar en solicitud, los usuarios empresariales podrán ver y editar valores de propiedades cuando soliciten elementos del catálogo.
	Mostrar en solicitud	Si desea mostrar el nombre y el valor de la propiedad a los usuarios finales, puede seleccionar la opción para mostrar la propiedad en el formulario de solicitud cuando se solicite el aprovisionamiento de la máquina. También debe seleccionar Reemplazable si desea que los usuarios proporcionen un valor.

Aplicar una zona de transporte de NSX a un blueprint

Un administrador de NSX puede crear zonas de transporte para controlar el uso de clúster de las redes.

Si el blueprint contiene una red a petición, debe especificar la zona de transporte de NSX que contiene las redes que se usan en la implementación de la máquina aprovisionada. Esa misma zona de transporte debe especificarse en la reserva.

Cuando se crea un blueprint, solo se exponen las zonas de transporte que se aplican al tenant actual. En concreto, estas zonas se encuentran disponibles si las utiliza una reserva en el tenant actual.

Aplicar una política de reserva de puerta de enlace enrutada o de Edge de NSX a un blueprint

Se puede especificar una política de reserva con la que administrar las comunicaciones de red de las máquinas aprovisionadas por el blueprint. Cuando se solicite el aprovisionamiento de máquina, se usará la política de reserva para agrupar las reservas que puedan tenerse en cuenta en la implementación. La política de reserva de puerta de enlace enrutada también se conoce como política de reserva de Edge.

Cada reserva contiene información de red. Cuando las máquinas se aprovisionan, se asigna una puerta de enlace enrutada o de Edge como enrutador de red para poder administrar las comunicaciones de red de las máquinas aprovisionadas en la implementación. Puede añadir o editar propiedades de nivel de blueprint mediante la página de propiedades del blueprint.

La política de reserva de puerta de enlace enrutada es opcional. Controla las reservas que se pueden usar para aprovisionar la instancia de Edge de NSX asociada a los componentes de red a petición y de equilibrador de carga a petición especificados en el blueprint.

Las políticas de reserva se usan para controlar la selección de reservas. Selecciona una política de reserva en su definición de máquina virtual en el blueprint y luego asigna esa política a las reservas que desea que usen sus máquinas virtuales.

No puede compartir reservas entre varios grupos empresariales.

vRealize Automation aprovisiona una puerta de enlace enrutada, como por ejemplo una puerta de enlace de servicios de Edge (ESG), para redes NAT y para equilibradores de carga. Para redes enrutadas, vRealize Automation usa enrutadores distribuidos existentes.

Un perfil de red NAT y un equilibrador de carga permiten a vRealize Automation implementar una puerta de enlace de servicios de Edge de NSX. Un perfil de red enrutada usa un enrutador distribuido lógico de NSX (DLR). El DLR debe crearse en NSX para que vRealize Automation pueda consumirlo. vRealize Automation no puede crear DLR. Tras la recopilación de datos, vRealize Automation puede usar el DLR para el aprovisionamiento de máquinas virtuales.

La reserva empleada para aprovisionar la puerta de enlace enrutada o de Edge determina la red externa que se usa en los perfiles de red NAT y enrutada, así como las direcciones IP virtuales del equilibrador de carga.

Cuando se usa el blueprint para aprovisionar una implementación de una máquina, vRealize Automation intenta utilizar únicamente las reservas asociadas con la política de reserva especificada para aprovisionar la puerta de enlace enrutada o de Edge.

Aplicar una política de seguridad de aislamiento de aplicaciones de NSX a un blueprint

Una política de aislamiento de aplicaciones de NSX actúa como un cortafuegos que bloquea todo el tráfico entrante y saliente de las máquinas aprovisionadas en la implementación. Si se especifica una política de aislamiento de aplicaciones de NSX establecida, las máquinas aprovisionadas por el blueprint se podrán comunicar entre sí, pero no conectarse fuera del cortafuegos.

Puede aplicar el aislamiento de aplicaciones a nivel de blueprint mediante la página **Nuevo blueprint** o **Propiedades de blueprint**.

Cuando se usa una política de aislamiento de aplicaciones de NSX, solo se permite el tráfico interno entre las máquinas aprovisionadas por el blueprint. Cuando se solicita el aprovisionamiento, se crea un grupo de seguridad para las máquinas que se van a aprovisionar. Se crea una política de seguridad de aislamiento de aplicaciones en NSX y se aplica al grupo de seguridad. Se definen reglas de cortafuegos en la política de seguridad para permitir únicamente el tráfico interno entre los componentes de la implementación. Para obtener información relacionada, consulte [Crear un endpoint de NSX y asociarlo a un endpoint de vSphere](#).

Nota Cuando el aprovisionamiento se realiza con un blueprint que usa tanto un equilibrador de carga de NSX Edge como una política de seguridad de aislamiento de aplicaciones de NSX, el equilibrador de carga aprovisionado dinámicamente no se añade al grupo de seguridad. Esto evita que el equilibrador de carga se comuniquen con las máquinas en las que debe controlar las conexiones. Las instancias de Edge no se pueden añadir a grupos de seguridad, ya que están excluidas del firewall distribuido de NSX. A fin de que el equilibrio de carga funcione de forma correcta, utilice otro grupo de seguridad o política de seguridad que permita el tráfico necesario a las máquinas virtuales de componentes.

La política de aislamiento de aplicaciones tiene una prioridad menor frente a otras políticas de seguridad en NSX. Así, por ejemplo, si la implementación aprovisionada contiene una máquina de componente web y otra de componente de aplicación y la máquina de componente web aloja un servicio web, el servicio deberá permitir el tráfico entrante en los puertos 80 y 443. En este caso, los usuarios deben crear una política de seguridad web en NSX con reglas de cortafuegos establecidas para permitir el tráfico entrante en esos puertos. En vRealize Automation, los usuarios deben aplicar la política de seguridad web en el componente web de la implementación de máquina aprovisionada.

Nota Si un blueprint contiene uno o varios equilibradores de carga y el aislamiento de aplicaciones está habilitado para el blueprint, la direcciones VIP de los equilibradores de carga se añaden al grupo de seguridad de aislamiento de aplicaciones como un IPSet. Si un blueprint contiene un grupo de seguridad a petición que está asociado con un nivel de máquina que también está asociado con un equilibrador de carga, el grupo de seguridad a petición incluye el nivel de máquina y el IPSet con la dirección VIP del equilibrador de carga.

Si la máquina de componente web requiere acceso a la máquina de componente de aplicación mediante equilibradores de carga en los puertos 8080 y 8443, la política de seguridad web también deberá incluir reglas de cortafuegos que permitan el tráfico saliente a esos puertos, aparte de las reglas de cortafuegos existentes que permiten el tráfico entrante en los puertos 80 y 443.

Para obtener información sobre las funciones de seguridad que se pueden usar en un componente de máquina de un blueprint, consulte [Usar componentes de seguridad en el lienzo de diseño](#).

Configurar opciones del componente de red y seguridad

vRealize Automation admite redes virtualizadas basadas en la plataforma NSX. También se admiten redes de Contenedores para vRealize Automation integradas.

Para integrar redes y seguridad con vRealize Automation, un administrador de IaaS debe configurar endpoints de vSphere y de NSX.

Para obtener más información sobre la preparación externa, consulte *Configuración de vRealize Automation*.

Se pueden crear perfiles de red que especifiquen valores de red en reservas y en el lienzo de diseño. Los perfiles de red externos definen las redes físicas existentes. NAT y los perfiles enrutados son plantillas que compilarán conmutadores lógicos NSX y configuraciones de enrutamiento para disponer de un nuevo nombre de red y para configurar interfaces de red para conectarse al nombre de red cuando aprovisiona máquinas virtuales y configure dispositivos Edge de NSX.

La configuración del componente de red y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario ejecutar la recopilación de datos en el inventario de NSX de clústeres de vSphere. Los componentes de redes y seguridad son específicos de NSX y solo se pueden usar con componentes de máquina de vSphere. Para obtener información sobre cómo configurar NSX, consulte la *guía de administración de NSX*.

En los componentes de máquina que carecen de la pestaña **Red o Seguridad**, puede añadir propiedades personalizadas de redes y seguridad, como `VirtualMachine.Network0.Name` a sus correspondientes pestañas **Propiedades** en el lienzo. Las propiedades de red, seguridad y equilibrador de carga de NSX solo son aplicables a las máquinas de vSphere.

Si especifica un perfil de red en una reserva y un blueprint, el valor del blueprint tiene prioridad. Por ejemplo, si especifica un perfil de red en el blueprint (mediante la propiedad personalizada `VirtualMachine.NetworkN.ProfileName`) y en una reserva utilizada por el blueprint, el perfil de red especificado en el blueprint tendrá prioridad. Sin embargo, si la propiedad personalizada no se utiliza en el blueprint, y selecciona un perfil de red para un NIC de máquina, vRealize Automation usa la ruta de red de reserva para el NIC de máquina cuyo perfil de red se haya especificado.

En función del recurso informático, se puede seleccionar una zona de transporte que identifique un endpoint de vSphere. Una zona de transporte especifica los hosts y los clústeres que se pueden asociar con los conmutadores lógicos creados dentro de la zona. A su vez, una zona de transporte puede abarcar varios clústeres de vSphere. El blueprint y las reservas empleados en el aprovisionamiento deben tener la misma configuración de zona de transporte. Las zonas de transporte se definen en los entornos de NSX. Consulte la *guía de administración de NSX*.

Puede configurar opciones de seguridad para las máquinas virtuales que se van a aprovisionar mediante la especificación de información en el script de una reserva, un blueprint o un agente invitado. Si las máquinas que se aprovisionarán requieren un agente invitado, debe añadir una regla de seguridad que contenga ese requisito a la reserva o el blueprint. Por ejemplo, si usa una política de seguridad predeterminada que deniegue la comunicación entre todas las máquinas y dependa de una política de seguridad independiente para permitir la comunicación entre

máquinas específicas, es posible que el agente invitado no pueda comunicarse con vRealize Automation durante la fase de personalización. Para evitar este problema durante el aprovisionamiento de máquinas, use una política de seguridad predeterminada que permita la comunicación durante la fase de personalización.

También puede añadir un componente de red de Contenedores a un blueprint.

Usar componentes de red en el lienzo de diseño

Puede añadir uno o varios componentes de red de NSX al lienzo de diseño y configurar las opciones de los componentes de máquina de vSphere en el blueprint.

Puede añadir componentes de red al lienzo de diseño para que sus opciones configuradas estén disponibles para uno o varios componentes de máquina del blueprint.

La configuración del componente de red y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario ejecutar la recopilación de datos en el inventario de NSX de clústeres de vSphere. Los componentes de redes y seguridad son específicos de NSX y solo se pueden usar con componentes de máquina de vSphere. Para obtener información sobre cómo configurar NSX, consulte la *guía de administración de NSX*.

Añadir un componente de red existente

Puede añadir un componente de red de NSX existente al lienzo de diseño del blueprint como preparación para asociar su configuración a uno o varios componentes de máquina de vSphere en el blueprint.

Puede usar un componente de red existente para añadir una red de NSX al lienzo de diseño y configurar sus ajustes para usarlo con componentes de máquina de vSphere y componentes de Software o XaaS pertenecientes a vSphere.

Cuando un componente de red o un componente de red a petición existente se asocia a un componente de máquina, la información de NIC se almacena junto con el componente de máquina. La información de perfil de red que especifique se almacena junto con el componente de red.

Se pueden añadir varios componentes de redes y seguridad al lienzo de diseño.

En los componentes de máquina que carecen de la pestaña **Red** o **Seguridad**, puede añadir propiedades personalizadas de redes y seguridad, como `VirtualMachine.Network0.Name` a sus correspondientes pestañas **Propiedades** en el lienzo. Las propiedades de red, seguridad y equilibrador de carga de NSX solo son aplicables a las máquinas de vSphere.

Cuando se crea un blueprint, solo se exponen los perfiles de red que corresponden al tenant actual. En concreto, dichos perfiles se encuentran disponibles si hay al menos una reserva en el tenant actual que tiene, como mínimo, una red asignada al perfil.

Requisitos previos

- Cree y configure los ajustes de red para NSX. Consulte *Configuración de vRealize Automation* y la *guía de administración de NSX*.
- Compruebe que el inventario de NSX se ha ejecutado correctamente en el clúster.

Para usar las configuraciones de NSX en vRealize Automation, debe ejecutar una recopilación de datos.

- Cree un perfil de red.
- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Abra un blueprint nuevo o uno ya existente en el lienzo de diseño mediante la pestaña **Diseño**.

Procedimiento

- 1 Haga clic en **Redes y seguridad** en la sección Categorías para mostrar la lista de componentes de red y seguridad disponibles.
- 2 Arrastre un componente **Red existente** al lienzo de diseño.
- 3 Haga clic en el cuadro de texto **Red existente** y seleccione un perfil de red existente.
Los valores de descripción, máscara de subred y puerta de enlace se rellenan en función del perfil de red seleccionado.
- 4 (opcional) Haga clic en la pestaña **DNS/WINS**.
- 5 (opcional) Especifique o acepte la configuración de DNS y WINS proporcionada para el perfil de red.

- DNS primario
- DNS secundario
- Sufijo DNS
- WINS preferido
- WINS alternativo

No puede cambiar la configuración de DNS o WINS de una red existente.

- 6 (opcional) Haga clic en la pestaña **Rangos de IP**.

Se muestran los rangos de direcciones IP especificados en el perfil de red. Puede cambiar el criterio de ordenación o la visualización de columnas. Para las redes NAT, también puede cambiar los valores de rango de direcciones IP.

- 7 Haga clic en **Finalizar** para guardar el blueprint como un borrador o seguir con la configuración del blueprint.

Pasos siguientes

Si desea configurar más opciones de red, añada componentes de red adicionales y seleccione las opciones de configuración de la pestaña **Red** de un componente de máquina de vSphere en el lienzo de diseño.

Crear y usar las reglas NAT

Puede añadir reglas NAT a un componente de red NAT de uno a muchos en un blueprint cuando el componente de red NAT está asociado a un componente de máquina de vSphere no agrupado en clúster o a un componente de equilibrador de carga de NSX a petición.

Puede definir las reglas NAT para cualquier protocolo compatible con NSX. Puede asignar un puerto o un rango de puertos de la dirección IP externa de una instancia de Edge a una dirección IP privada en el componente de red NAT.

- **Componente de máquina de vSphere**

Puede crear reglas NAT para un componente de red NAT de uno a muchos que está asociado a un componente de máquina de vSphere no agrupado en clúster.

Por ejemplo, si dos máquinas están asociadas a un componente de red NAT de uno a muchos en el blueprint, puede definir una regla NAT que permita que el puerto 443 en la dirección IP externa se conecte a las máquinas a través del puerto 80 en la red NAT con el protocolo TCP.

- **Componente de equilibrador de carga de NSX**

Puede crear reglas NAT para un componente de red NAT de uno a muchos que esté asociado a la red de VIP de un componente de equilibrador de carga de NSX.

Por ejemplo, si el componente de red NAT está asociado a un componente de equilibrador de carga que equilibra la carga de tres máquinas, puede definir una regla NAT que permita que el puerto 90 en la dirección IP externa se conecte a la VIP del equilibrador de carga a través del puerto 80 en la red NAT con el protocolo UDP.

Puede crear cualquier número de reglas NAT y puede controlar el orden en que se procesan.

No se admiten los siguientes elementos para las reglas NAT:

- NIC que no están en la red actual
- NIC que están configuradas para obtener las direcciones IP a través de DHCP
- Clústeres de máquinas

Para agregar reglas NAT a un componente de red NAT en un blueprint, consulte [Añadir un componente de red enrutada a petición o red NAT a petición](#).

Para obtener información relacionada con el uso de reglas NAT, consulte artículos públicos, como esta [publicación del blog vmwarelab](#).

Añadir un componente de red enrutada a petición o red NAT a petición

Puede añadir un componente de red NAT a petición NSX o un componente de red con enrutamiento a petición NSX al lienzo de diseño como preparación para asociar su configuración a uno o varios componentes de máquina de vSphere en el blueprint.

Cuando un componente de red o un componente de red a petición existente se asocia a un componente de máquina, la información de NIC se almacena junto con el componente de máquina. La información de perfil de red que especifique se almacena junto con el componente de red.

Se pueden añadir varios componentes de redes y seguridad al lienzo de diseño.

Puede haber más de un componente de red a petición en un único blueprint. Sin embargo, todos los perfiles de red a petición que se utilizan en el blueprint deben hacer referencia al mismo perfil de red externa.

En los componentes de máquina que carecen de la pestaña **Red** o **Seguridad**, puede añadir propiedades personalizadas de redes y seguridad, como `VirtualMachine.Network0.Name` a sus correspondientes pestañas **Propiedades** en el lienzo. Las propiedades de red, seguridad y equilibrador de carga de NSX solo son aplicables a las máquinas de vSphere.

Cuando se crea un blueprint, solo se exponen los perfiles de red que corresponden al tenant actual. En concreto, dichos perfiles se encuentran disponibles si hay al menos una reserva en el tenant actual que tiene, como mínimo, una red asignada al perfil.

Requisitos previos

- Cree y configure los ajustes de red para NSX. Consulte *Configuración de vRealize Automation* y la *guía de administración de NSX*.
- Compruebe que el inventario de NSX se ha ejecutado correctamente en el clúster.
Para usar las configuraciones de NSX en vRealize Automation, debe ejecutar una recopilación de datos.
- Cree un perfil de red a petición. Consulte [Crear un perfil de red](#).
Por ejemplo, si va a añadir un componente de red NAT a petición, consulte [Crear un perfil de red NAT para una red a petición](#).
- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Abra un blueprint nuevo o uno ya existente en el lienzo de diseño mediante la pestaña **Diseño**.
- Si desea especificar reglas NAT para un componente de red NAT, debe utilizar un perfil de red NAT de uno a muchos. Consulte [Crear un perfil de red NAT mediante el endpoint de IPAM suministrado](#) o [Crear un perfil de red NAT mediante un endpoint de IPAM de terceros](#).
Para obtener información acerca de las reglas NAT, consulte [Crear y usar las reglas NAT](#).

Procedimiento

- 1 Haga clic en **Redes y seguridad** en la sección Categorías para mostrar la lista de componentes de red y seguridad disponibles.
- 2 Arrastre un NAT a petición o un componente de red enrutada a petición al lienzo de diseño.
- 3 Introduzca un nombre de componente en el cuadro de texto **ID** para etiquetar el componente de forma exclusiva en el lienzo de diseño.
- 4 Seleccione un perfil de red adecuado del menú desplegable **Perfil de red principal**. Por ejemplo, si desea agregar un componente de red NAT, seleccione un perfil de red NAT que esté configurado para admitir las opciones de red que pretende.

Si desea especificar reglas NAT en un componente de red NAT, debe utilizar un perfil de red principal que esté configurado para NAT uno a muchos.

La siguiente configuración de red se rellena en función del tipo de perfil de red que haya seleccionado. Estos valores deben cambiarse en el perfil de red:

- Nombre de perfil de red externa
- Tipo NAT (Red NAT a petición)
- Máscara de subred
- Máscara de subred del rango (Red con enrutamiento a petición)
- Máscara de subred del rango (Red con enrutamiento a petición)
- Dirección IP base (Red con enrutamiento a petición)

5 (opcional) Escriba una descripción del componente en el cuadro de texto **Descripción**.

6 (opcional) Haga clic en la pestaña **DNS/WINS**.

7 (opcional) Especifique o acepte la configuración de DNS y WINS proporcionada para el perfil de red.

- DNS primario
- DNS secundario
- Sufijo DNS
- WINS preferido
- WINS alternativo

No puede cambiar la configuración de DNS o WINS de una red existente.

8 Haga clic en la pestaña **Rangos de IP**.

Se muestran los rangos de direcciones IP especificados en el perfil de red. Puede cambiar el criterio de ordenación o la visualización de columnas. Para las redes NAT, también puede cambiar los valores de rango de direcciones IP.

- a Introduzca un valor de dirección IP inicial en el cuadro de texto **Inicio de rango de IP**.
- b Introduzca un valor de dirección IP inicial en el cuadro de texto **Inicio de rango de IP**.

9 Si utiliza una red NAT basada en un perfil de red NAT uno a muchos que use intervalos de direcciones IP estáticas, puede utilizar la pestaña **Reglas NAT** para agregar reglas que permitan que una dirección IP externa acceda a los componentes de la red NAT interna.

En una red NAT uno a muchos, puede definir las reglas NAT que se pueden configurar cuando se añade un componente de red NAT al blueprint y se pueden cambiar cuando se edita la red NAT en una implementación.

Las opciones disponibles para su selección se basan en los componentes de máquina de vSphere o equilibrador de carga de NSX que se hayan asociado al componente de red NAT.

- **Nombre:** introduzca un nombre de regla único.
- **Componente:** seleccione en la lista de componentes de máquina o equilibrador de carga asociados de vSphere a los que esté asociada la red NAT.

Solo se admiten las reglas NAT en las máquinas no agrupadas en clústeres. Si se especificó un tamaño de clúster superior a 1, no se muestran componentes, ya que no se admite la configuración.

- **Puerto de origen:** seleccione la opción ANY, introduzca un puerto o un rango de puertos válidos, o especifique un enlace de propiedad válido.
- **Puerto de destino:** seleccione la opción ANY, introduzca un puerto o un rango de puertos válidos, o especifique un enlace de propiedad válido.
- **Protocolo:** introduzca un protocolo válido que sea compatible con NSX, o seleccione la opción TCP, UDP o ANY.
- **Descripción:** escriba una breve descripción de para qué está diseñada la regla NAT.

10 Haga clic en **Finalizar** para guardar el blueprint como un borrador o seguir con la configuración del blueprint.

Pasos siguientes

Si desea configurar más opciones de red, añada componentes de red adicionales y seleccione las opciones de configuración de la pestaña **Red** de un componente de máquina de vSphere en el lienzo de diseño.

Usar componentes de equilibrador de carga en el lienzo de diseño

Puede añadir uno o varios componentes de equilibrador de carga de NSX a petición al lienzo de diseño para configurar los ajustes de los componentes de máquina de vSphere en el blueprint.

La configuración del componente de red y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario ejecutar la recopilación de datos en el inventario de NSX de clústeres de vSphere. Los componentes de redes y seguridad son específicos de NSX y solo se pueden usar con componentes de máquina de vSphere. Para obtener información sobre cómo configurar NSX, consulte la *guía de administración de NSX*.

Las siguientes reglas se aplican a los grupos y la configuración de red de VIP de equilibrador de carga en el blueprint.

- Si el perfil de red de grupos es NAT, el perfil de red de VIP puede formar parte del perfil de red NAT.
- Si el perfil de red de grupos es enrutado, el perfil de red VIP solo podrá estar en la misma red enrutada.
- Si el perfil de red de grupos es externo, el perfil de red VIP solo podrá ser el mismo perfil de red externo.

Cada componente de equilibrador de carga puede tener varios servidores virtuales, también conocidos como servicios de equilibrador de carga. Cada servidor virtual del componente de equilibrador de carga puede tener un puerto y un protocolo. Por ejemplo, puede equilibrar la carga de un servicio HTTP o HTTPS. Un equilibrador de carga puede equilibrar la carga de varios servicios.

NSX Edge es el dispositivo de red que contiene los servidores virtuales del equilibrador de carga. Aunque es posible tener más de un componente de equilibrador de carga en un blueprint, al aprovisionar la implementación, se incluyen los servidores virtuales definidos en cada componente de equilibrador de carga en una sola instancia de NSX Edge .

Si un blueprint contiene uno o varios equilibradores de carga y el aislamiento de aplicaciones está habilitado para el blueprint, la direcciones VIP de los equilibradores de carga se añaden al grupo de seguridad de aislamiento de aplicaciones como un IPSet. Si un blueprint contiene un grupo de seguridad a petición que está asociado con un nivel de máquina que también está asociado con un equilibrador de carga, el grupo de seguridad a petición incluye el nivel de máquina y el IPSet con la dirección VIP del equilibrador de carga.

Puede reconfigurar las opciones del equilibrador de carga en una implementación existente para añadir, editar o quitar servidores virtuales. Para obtener información, consulte [Reconfigurar un equilibrador de carga en una implementación](#).

Para obtener información sobre cómo trabajar con componentes de equilibrador de carga después de la actualización o migración, consulte [Consideraciones al trabajar con componentes de equilibrador de carga actualizados o migrados](#).

Consideraciones al trabajar con componentes de equilibrador de carga actualizados o migrados
Es importante tener en cuenta las siguiente consideraciones para comprender y actuar en cuestiones relacionadas con los componentes de equilibrador de carga de NSX en la versión de destino de vRealize Automation.

Esta información se aplica a los componentes de equilibrador de carga de NSX que se hayan actualizado o migrado a esta versión de vRealize Automation.

- Debe ejecutar la recopilación de datos del inventario de seguridad y redes NSX antes y después de actualizar o migrar a esta versión para evitar que surjan problemas cuando ejecute la acción de reconfiguración del equilibrador de carga. La acción de reconfiguración del equilibrador de carga para nuevas implementaciones no se verá afectada.

Para obtener más información, consulte *Actualización de vRealize Automation 7.1, 7.2 o 7.3 y Migración de vRealize Automation*.

- A partir de vRealize Automation 7.3, puede volver a configurar un equilibrador de carga. La autorización de catálogo que se necesita es Reconfigurar (equilibrador de carga). Para obtener información relacionada, consulte [Reconfigurar un equilibrador de carga en una implementación](#).
- En el caso de las implementaciones que se han actualizado o migrado desde vRealize Automation 7.x a esta versión de vRealize Automation, la reconfiguración del equilibrador de carga se limita a las implementaciones que contienen un único equilibrador de carga.
- No se admite la operación de reconfiguración del equilibrador de carga para implementaciones que se hayan actualizado o migrado desde vRealize Automation 6.2.x a esta versión de vRealize Automation.

Añadir un componente de equilibrador de carga a petición

Puede arrastrar un componente de equilibrador de carga a petición de NSX en el lienzo de diseño y configurarlo para utilizarlo con componentes de contenedor y componentes de máquina de vSphere en el blueprint.

Para obtener información relacionada con la creación de perfiles de aplicación de NSX y definir el comportamiento de un tipo particular de tráfico de red, consulte la *guía de administración de NSX* para su versión en https://www.vmware.com/support/pubs/nsx_pubs.html.

Procedimiento

1 Definir la configuración del miembro del equilibrador de carga

Es posible definir un componente de equilibrador de carga de NSX a petición para distribuir el procesamiento de tareas entre las máquinas aprovisionadas de contenedor o de miembro de vSphere en una red.

2 Definir la configuración general del servidor virtual

Puede definir un puerto y un protocolo de un único servidor virtual para el equilibrador de carga, o bien puede añadir más servidores virtuales para personalizar opciones adicionales del equilibrador de carga de NSX.

3 Definir la configuración de distribución de servidores virtuales

Si selecciona la opción **Personalizar** en la pestaña **General**, puede especificar información sobre los miembros del grupo, como el puerto en el que los miembros reciben el tráfico, el tipo de protocolo que el equilibrador de carga de NSX puede utilizar para acceder a ese puerto, el algoritmo empleado en el equilibrio de carga y las opciones de configuración de persistencia.

4 Definir la configuración de comprobación de estado del servidor virtual

Si selecciona la opción **Personalizar** en la pestaña **General**, puede especificar si (o cómo) el equilibrador de carga de NSX va a realizar comprobaciones de estado en los miembros del grupo en el servidor virtual.

5 Definir la configuración avanzada del servidor virtual

Si selecciona la opción **Personalizar** en la pestaña **General**, puede personalizar el componente de equilibrador de carga de NSX para especificar parámetros como el número de conexiones simultáneas que puede reconocer un único miembro de grupo y el número máximo de conexiones simultáneas que puede procesar el servidor virtual.

6 Definir opciones de registro de equilibrador de carga

Puede definir los tipos de acciones de registro del equilibrador de carga que se capturan y se registran en los logs del equilibrador de carga.

Definir la configuración del miembro del equilibrador de carga

Es posible definir un componente de equilibrador de carga de NSX a petición para distribuir el procesamiento de tareas entre las máquinas aprovisionadas de contenedor o de miembro de vSphere en una red.

Al añadir un componente de equilibrador de carga a un blueprint en el lienzo de diseño, puede elegir una opción predeterminada o una opción personalizada al crear o editar las definiciones del servidor virtual en el componente de equilibrador de carga. La opción predeterminada permite especificar el protocolo, el puerto y la descripción del servidor virtual, así como utilizar los valores predeterminados para todas las demás configuraciones. La opción personalizada permite definir niveles de detalle adicionales.

Si el equilibrador de carga se aprovisiona con una red externa, la VIP (especificada con la **Red de VIP**) y el grupo de miembros (especificado con la **Red del miembro**) debe estar en la misma red existente. Si la VIP y el grupo no están en la misma red externa, se produce un error durante el aprovisionamiento.

Requisitos previos

- Cree y configure los ajustes de equilibrador de carga para NSX. Consulte *Configuración de vRealize Automation* y la *guía de administración de NSX*.

- Compruebe que el inventario de NSX se ha ejecutado correctamente en el clúster.

Para usar las configuraciones de NSX en vRealize Automation, debe ejecutar una recopilación de datos.

- Cree un perfil de red.
- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Abra un blueprint nuevo o uno ya existente en el lienzo de diseño mediante la pestaña **Diseño**.
- Compruebe que exista al menos un componente de contenedor o un componente de máquina de vSphere en el blueprint.

Procedimiento

- 1 Haga clic en **Redes y seguridad** en la sección Categorías para mostrar la lista de componentes de red y seguridad disponibles.
- 2 Arrastre un componente **Equilibrador de carga a petición** al lienzo de diseño.
- 3 Introduzca un nombre de componente en el cuadro de texto **ID** para etiquetar el componente de forma exclusiva en el lienzo de diseño.
- 4 Seleccione un nombre de componente de contenedor o de componente de máquina de vSphere del menú desplegable **Miembro**.

La lista contiene solo los componentes de contenedor y los componentes de máquina de vSphere en el blueprint activo.

- 5 Seleccione el NIC para equilibrar la carga en el menú desplegable **Member network** (Red de miembro).

La lista contiene los NIC que se han definido en relación con el miembro de la máquina de vSphere seleccionado.

- 6 Seleccione una red de dirección IP virtual disponible en el menú desplegable **Red de VIP**. Por ejemplo, seleccione una red NAT o una red externa disponible.

Aunque es posible tener varios componentes de equilibrador de carga de NSX y de red a petición de NSX en un blueprint, todos deben estar asociados a la misma red de VIP.

- 7 (opcional) Introduzca una dirección IP válida para el NIC en el cuadro de texto **Dirección IP**.

La configuración predeterminada es la dirección IP estática asociada a la red VIP. Puede especificar otra dirección IP o un rango de direcciones IP. De forma predeterminada, la siguiente dirección IP disponible se asigna desde la red de VIP asociada.

Deje el campo correspondiente a la dirección IP en blanco para que la dirección IP se asigne a partir de la red VIP asociada durante el aprovisionamiento.

Solo puede especificar una dirección IP cuando se crea VIP en una red NAT.

- 8 Para crear una definición de servidor virtual, haga clic en **Nuevo** y consulte [Definir la configuración general del servidor virtual](#).

Cada componente de equilibrador de carga requiere al menos un servidor virtual.

Para especificar opciones de registro, consulte [Definir opciones de registro de equilibrador de carga](#).

Definir la configuración general del servidor virtual

Puede definir un puerto y un protocolo de un único servidor virtual para el equilibrador de carga, o bien puede añadir más servidores virtuales para personalizar opciones adicionales del equilibrador de carga de NSX.

Por ejemplo, puede personalizar el componente de equilibrador de carga para definir parámetros como el puerto y el protocolo de comprobación de estado, el algoritmo, la persistencia y la transparencia.

Requisitos previos

[Definir la configuración del miembro del equilibrador de carga](#).

Procedimiento

- 1 Haga clic en la pestaña **General** en la página **Nuevo servidor virtual**.
- 2 En el menú desplegable **Protocolo**, seleccione el protocolo de tráfico de red que se utilizará para el equilibrio de carga del servidor virtual.

Las opciones de protocolo son HTTP, HTTPS, TCP y UDP.

- 3 Introduzca un valor de puerto en el cuadro de texto **Puerto**.

El protocolo seleccionado determina la configuración de puerto predeterminada.

Protocolo	Puerto predeterminado
HTTP	80
HTTPS	443

Protocolo	Puerto predeterminado
TCP	8080
UDP	Sin valor predeterminado

Los protocolos HTTP, HTTPS y TCP pueden compartir un puerto con UDP. Por ejemplo, si el servicio 1 utiliza TCP, HTTP o HTTPS en el puerto 80, el servicio 2 puede utilizar UDP en el puerto 80. Si el servicio 1 utiliza UDP en el puerto 80, el servicio 2 no puede utilizar UDP en el puerto 80.

4 (opcional) Escriba una descripción para el componente de servidor virtual.

5 Seleccione una de las opciones de **Configuración**.

■ **Usar valor predeterminado para todas las demás configuraciones**

Acepte todas las demás configuraciones predeterminadas. Haga clic en **Aceptar** para finalizar la definición del componente de equilibrador de carga y seguir trabajando en el blueprint.

Para ver los valores predeterminados, haga clic en **Personalizar** y examine las opciones de las demás pestañas. Si la configuración predeterminada es aceptable, haga clic en **Usar valor predeterminado para todas las demás configuraciones** en la pestaña **General**.

■ **Personalizar**

Configure el componente de equilibrador de carga con parámetros adicionales para, por ejemplo, definir un protocolo diferente para la supervisión del estado o un puerto diferente para la supervisión del tráfico de miembro.

Aparecerán pestañas adicionales que le permitirán añadir configuraciones personalizadas.

Si selecciona **Usar valor predeterminado para todas las demás configuraciones** y hace clic en **Aceptar**, finaliza el proceso y puede seguir definiendo o editando el blueprint en el lienzo de diseño. Si selecciona **Personalizar**, vaya al siguiente paso.

6 Haga clic en la pestaña **Distribución** y consulte el tema [Definir la configuración de distribución de servidores virtuales](#) para seguir definiendo el componente de equilibrador de carga de NSX.

Definir la configuración de distribución de servidores virtuales

Si selecciona la opción **Personalizar** en la pestaña **General**, puede especificar información sobre los miembros del grupo, como el puerto en el que los miembros reciben el tráfico, el tipo de protocolo que el equilibrador de carga de NSX puede utilizar para acceder a ese puerto, el algoritmo empleado en el equilibrio de carga y las opciones de configuración de persistencia.

Un grupo representa un clúster de máquinas cuyas cargas se están equilibrando. Un miembro del grupo representa una máquina de ese clúster.

La configuración predeterminada de protocolo del miembro y de puerto del miembro coincide con la configuración de protocolo y de puerto en la pestaña **General**.

El grupo de máquinas miembro se muestra en el valor de la opción **Miembro** de la interfaz de usuario de componente de equilibrador de carga de blueprint. La entrada **Miembro** se establece en el grupo o el clúster de máquinas.

Requisitos previos

[Definir la configuración general del servidor virtual.](#)

Procedimiento

- 1 (opcional) La opción **Protocolo del miembro** coincide con el protocolo que se ha especificado en la pestaña **General**. Esta configuración define la manera en la que el miembro del grupo recibirá el tráfico de red.
- 2 (opcional) Introduzca un número de puerto en el cuadro de texto **Puerto del miembro** para especificar el puerto en el que el miembro del grupo recibirá el tráfico de red.

Por ejemplo, si la solicitud entrante en la dirección IP virtual (virtual IP, VIP) del equilibrador de carga está en el puerto 80, puede que desee enrutar la solicitud a otro puerto (por ejemplo, el puerto 8080) en los miembros del grupo.

- 3 (opcional) Seleccione el método de equilibrio de algoritmo de este grupo.

En la siguiente tabla se describen las opciones y los parámetros de algoritmo de las opciones que las necesitan.

Opción	Descripción y parámetros de algoritmo
ROUND_ROBIN	<p>Se utiliza un servidor por vez según el peso que se le haya asignado.</p> <p>Si el equilibrador de carga se creó en vRealize Automation, el peso es el mismo para todos los miembros.</p> <p>Este es el algoritmo más uniforme y justo cuando el tiempo de procesamiento del servidor se distribuye de forma equitativa.</p> <p>Los parámetros del algoritmo se desactivan para esta opción.</p>
IP-HASH	<p>Se selecciona un servidor según un hash de la dirección IP de origen y el peso total de los servidores en ejecución.</p> <p>Los parámetros del algoritmo se desactivan para esta opción.</p>
LEASTCONN	<p>Se distribuyen las solicitudes de los clientes entre varios servidores según la cantidad de conexiones existentes en el servidor.</p> <p>Las conexiones nuevas se envían al servidor con menos conexiones.</p> <p>Los parámetros del algoritmo se desactivan para esta opción.</p>

Opción	Descripción y parámetros de algoritmo
URI	<p>Se aplica un hash a la porción izquierda del URI (antes del signo de interrogación) y se divide entre el peso total de los servidores en ejecución. El resultado permite determinar el servidor que recibirá la solicitud. Esto garantiza que un URI se dirija siempre al mismo servidor, siempre que ningún servidor se active o desactive.</p> <p>El parámetro del algoritmo URI tiene dos opciones: <code>uriLength=<len></code> y <code>uriDepth=<dep></code>. Introduzca los parámetros de longitud y de profundidad en líneas separadas en el cuadro de texto Parámetros de algoritmo.</p> <p>Los parámetros de longitud y de profundidad están seguidos de un número entero positivo. Estas opciones pueden equilibrar los servidores exclusivamente según la parte inicial del URI.</p> <p>El parámetro de longitud indica que el algoritmo solo debe considerar los caracteres definidos en la parte inicial del URI para calcular el hash. El rango del parámetro de longitud debe ser $1 \leq \text{len} < 256$.</p> <p>El parámetro de profundidad indica la profundidad máxima del directorio que se va a utilizar para calcular el hash. Se cuenta un nivel por cada barra diagonal en la solicitud. El rango del parámetro de profundidad debe ser $1 \leq \text{dep} < 10$.</p> <p>Si se especifican ambos parámetros, la evaluación se detiene cuando se llega a cualquiera de los parámetros.</p>
HTTPHEADER	<p>El nombre del encabezado HTTP se busca en cada solicitud HTTP.</p> <p>El nombre del encabezado entre paréntesis no distingue entre mayúsculas y minúsculas de forma similar a la función ACL <code>"hdr()"</code>.</p> <p>El parámetro del algoritmo HTTPHEADER tiene una opción <code>headerName=<name></code>. Por ejemplo, puede utilizar host como el parámetro del algoritmo HTTPHEADER.</p> <p>Si falta el encabezado o este no contiene ningún valor, se aplica el algoritmo Round Robin.</p>
URL	<p>El parámetro URL especificado en el argumento se busca en la cadena de consulta de cada solicitud HTTP GET.</p> <p>El parámetro del algoritmo URL tiene una opción <code>urlParam=<url></code>.</p> <p>Si el parámetro está seguido de un signo igual (=) y un valor, se le aplicará un hash al valor y se dividirá entre el peso total de los servidores en ejecución. El resultado permite determinar el servidor que recibirá la solicitud. Este proceso se utiliza para realizar el seguimiento de los identificadores de usuario de las solicitudes y para garantizar que siempre se envíe el mismo identificador de usuario al mismo servidor, siempre que ningún servidor se active o se desactive.</p> <p>Si no se encuentra ningún parámetro ni ningún valor, se aplica un algoritmo Round Robin.</p>

4 (opcional) Seleccione el método de persistencia de este grupo.

La persistencia realiza un seguimiento de los datos de la sesión, como el miembro del grupo específico que ha procesado una solicitud de cliente, y los almacena. Con la persistencia, las solicitudes de cliente se dirigen al mismo miembro del grupo durante toda una sesión o durante las sesiones posteriores.

Protocolo	Método de persistencia admitido
HTTP	Ninguno, Cookie e IP de origen
HTTPS	Ninguno, IP de origen e ID de sesión SSL
TCP	Ninguno, IP de origen y RDP de Microsoft
UDP	Ninguno e IP de origen

- Seleccione **Cookie** para insertar una cookie única que identifique la sesión la primera vez que un cliente acceda al sitio. En las solicitudes posteriores se hace referencia a la cookie para persistir en la conexión al servidor apropiado.
- Seleccione **IP de origen** para hacer un seguimiento de las sesiones con base en la dirección IP de origen. Cuando un cliente solicita una conexión a un servidor virtual que admite la persistencia de afinidad de dirección de origen, el equilibrador de carga comprueba si ese cliente se ha conectado anteriormente y, de ser así, devuelve el cliente al mismo miembro del grupo.
- Seleccione el **ID de sesión SSL** y el patrón de tráfico HTTPS de acceso directo a SSL.
 - Acceso directo SSL: Cliente -> HTTPS -> LB (acceso directo SSL) -> HTTPS -> Servidor
 - Cliente: HTTP-> LB -> HTTP -> Servidores

Nota vRealize Automation actualmente solo es compatible con el acceso directo a SSL. Se utiliza el método de acceso directo a SSL independientemente de la opción que se seleccione.

- Seleccione **RDP de Microsoft** para mantener las sesiones persistentes entre los servidores y los clientes de Windows que ejecutan el servicio Protocolo de escritorio remoto (Remote Desktop Protocol, RDP) de Microsoft. El escenario recomendado para habilitar la persistencia de RDP de Microsoft consiste en crear un grupo de equilibrio de carga compuesto por miembros que ejecuten la instancia compatible de Windows Server, en el que todos los miembros pertenezcan a un clúster de Windows y participen en un directorio de sesiones de Windows.
- Seleccione **Ninguno** para impedir que se almacenen las acciones de la sesión para una recuperación posterior.

5 Si utiliza una configuración de persistencia de cookies, escriba el nombre de la cookie.

- 6 (opcional) En el menú desplegable de **Modo**, seleccione el modo en que se inserta la cookie.

Opción	Descripción
Insertar	NSX Edge envía una cookie. Si el servidor envía una o varias cookies, el cliente recibe una cookie extra (la o las cookies del servidor+la cookie de NSX Edge). Si el servidor no envía ninguna cookie, el cliente recibe la cookie de NSX Edge.
Prefijo	El servidor envía una cookie. Utilice esta opción si el cliente no admite más de una cookie. Si dispone de una aplicación propia que utiliza un cliente propio que solo admite una cookie, el servidor web envía una cookie, pero NSX Edge añade la información de cookie al valor de cookie del servidor como un prefijo.
Sesión de aplicación	El servidor no envía una cookie. En su lugar, envía información de sesión del usuario como una URL. Por ejemplo, <code>http://mysite.com/admin/UpdateUserServlet;jsessionid=X000X0XXX0XXXX</code> , donde <code>jsessionid</code> es la información de sesión del usuario y se utiliza para la persistencia.

- 7 (opcional) Introduzca el tiempo de caducidad de la persistencia de la cookie en segundos.

Por ejemplo, para el equilibrio de carga de L7 con una IP de origen de TCP, se agota el tiempo de espera de la entrada de persistencia si no se establecen nuevas conexiones de TCP durante el tiempo de caducidad especificado, incluso si las conexiones existentes siguen activas.

- 8 (opcional) Haga clic en la pestaña **Comprobación de estado** y consulte el tema [Definir la configuración de comprobación de estado del servidor virtual](#) para seguir definiendo el componente de equilibrador de carga de NSX.

Definir la configuración de comprobación de estado del servidor virtual

Si selecciona la opción **Personalizar** en la pestaña **General**, puede especificar si (o cómo) el equilibrador de carga de NSX va realizar comprobaciones de estado en los miembros del grupo en el servidor virtual.

La configuración predeterminada del protocolo y el puerto de comprobación de estado coincide con la configuración del protocolo y el puerto en la pestaña **General**.

Para obtener información relacionada, consulte el tema sobre cómo *crear un supervisor de servicios* en la documentación del producto de NSX, en https://www.vmware.com/support/pubs/nsx_pubs.html. Cabe decir que la documentación de NSX hace referencia al miembro del servidor virtual como un miembro del grupo.

Requisitos previos

[Definir la configuración general del servidor virtual.](#)

Procedimiento

- 1 (opcional) Seleccione un protocolo de comprobación de estado del menú desplegable **Protocolo de comprobación de estado** para especificar la manera en la que se accede al miembro del grupo cuando el equilibrador de carga escucha para averiguar el estado del miembro del grupo.

Las opciones de protocolo son **HTTP, HTTPS, TCP, ICMP, UDP y Ninguno**.

También puede aceptar el protocolo predeterminado como se indica en la pestaña General.

- 2 (opcional) Introduzca un valor en el cuadro de **Puerto de comprobación de estado** para especificar el puerto del equilibrador de carga en el que se escucha para supervisar el estado del miembro de servidor virtual o del miembro del grupo.

Cabe decir que la documentación de NSX hace referencia al miembro del servidor virtual como un miembro del grupo.

Los protocolos HTTP, HTTPS y TCP pueden compartir un puerto con UDP. Por ejemplo, si el servicio 1 utiliza TCP, HTTP o HTTPS en el puerto 80, el servicio 2 puede utilizar UDP en el puerto 80. Si el servicio 1 utiliza UDP en el puerto 80, el servicio 2 no puede utilizar UDP en el puerto 80.

- 3 Introduzca el valor de **Intervalo** en segundos en el que se debe hacer ping en el servidor.
- 4 Introduzca el valor máximo de **Tiempo de espera** en segundos en el que se debe recibir una respuesta del servidor.
- 5 Introduzca un valor de **Número máximo de reintentos** para hacer ping en el servidor antes de declararlo inactivo.
- 6 Especifique otras configuraciones de comprobación de estado según el **Protocolo de comprobación de estado** seleccionado.
 - a Especifique el **Método** que se va a usar para detectar el estado del servidor. Las opciones son GET, OPTIONS y POST.
 - b Introduzca la **URL** que se va a usar en la solicitud para detectar el estado del servidor. Se trata de la dirección URL que se utiliza en las opciones de los métodos GET y POST ("/" de forma predeterminada).
 - c En el cuadro de texto **Enviar**, introduzca la cadena que se va a enviar al servidor después de que se establezca una conexión.

En el cuadro de texto **Enviar**, introduzca la cadena que se va a enviar al servidor después de que se establezca una conexión.
 - d En el cuadro de texto **Recibir**, introduzca la cadena que se espera recibir del servidor.

El servidor se considerará activo únicamente si la cadena recibida coincide con esta definición.

La cadena puede ser un encabezado o formar parte del cuerpo de la respuesta.

- 7 Haga clic en la pestaña **Avanzado** y consulte el tema [Definir la configuración avanzada del servidor virtual](#) para seguir definiendo el componente de equilibrador de carga de NSX.

Para especificar opciones de registro, consulte [Definir opciones de registro de equilibrador de carga](#).

Definir la configuración avanzada del servidor virtual

Si selecciona la opción **Personalizar** en la pestaña **General**, puede personalizar el componente de equilibrador de carga de NSX para especificar parámetros como el número de conexiones simultáneas que puede reconocer un único miembro de grupo y el número máximo de conexiones simultáneas que puede procesar el servidor virtual.

Requisitos previos

[Definir la configuración general del servidor virtual](#).

Procedimiento

- 1 Escriba un valor en el cuadro de texto **Límite de conexiones** para especificar el número máximo de conexiones simultáneas en NSX que puede procesar el servidor virtual.

Esta configuración toma en cuenta el número de conexiones de todos los miembros.

Escriba 0 para no establecer ningún límite.

- 2 Escriba un valor en el cuadro de texto **Límite de velocidad de conexión** para especificar el número máximo de solicitudes de conexión entrantes en NSX que se pueden aceptar por segundo.

Esta configuración toma en cuenta el número de conexiones de todos los miembros.

Escriba 0 para no establecer ningún límite.

- 3 (opcional) Active la casilla de verificación **Habilitar aceleración** para especificar que cada IP virtual (virtual IP, VIP) debe utilizar el equilibrador de carga L4, que es más rápido, en lugar del equilibrador de carga L7.

- 4 (opcional) Active la casilla de verificación **Transparente** para permitir que los miembros del grupo de equilibradores de carga vean la dirección IP de las máquinas que llaman al equilibrador de carga.

Si no se activa, los miembros del grupo de equilibradores de carga verán la dirección IP de origen del tráfico como una dirección IP interna del equilibrador de carga.

- 5 Escriba un valor en el cuadro de texto **Número máximo de conexiones** para especificar el número máximo de conexiones simultáneas que un único miembro de grupo puede reconocer.

Si el número de solicitudes entrantes supera este valor, las solicitudes se colocan en una cola y se procesan en el orden en el que se reciben a medida que se liberan las conexiones.

Escriba 0 para no establecer ningún valor máximo.

- 6 Escriba un valor en el cuadro de texto **Número mínimo de conexiones** para especificar el número mínimo de conexiones simultáneas que un único miembro debe aceptar siempre.
Escriba 0 para no establecer ningún valor mínimo.
- 7 Haga clic en **Aceptar** para completar la definición del servidor virtual.
- 8 Para especificar opciones de registro, consulte [Definir opciones de registro de equilibrador de carga](#); en caso contrario, haga clic en **Guardar** o en **Finalizar**.

Definir opciones de registro de equilibrador de carga

Puede definir los tipos de acciones de registro del equilibrador de carga que se capturan y se registran en los logs del equilibrador de carga.

Tras la definición de un componente de equilibrador de carga o durante esta, puede especificar un nivel de registro para la recopilación de logs de tráfico de equilibrador de carga. Los niveles de registro que define para cualquier componente de equilibrador de carga en el blueprint se aplican en todos los equilibradores de carga que se definen en el blueprint.

Los niveles de registro incluyen Depuración, Información, Advertencia, Error y Crítico. Las opciones Depuración e Información registran las solicitudes de usuario, mientras que las opciones Advertencia, Error y Crítico opciones no las registran.

Para obtener más información sobre el registro del equilibrador de carga de NSX, consulte la *guía de administración de NSX*.

Requisitos previos

[Definir la configuración del miembro del equilibrador de carga.](#)

Procedimiento

- 1 Seleccione la pestaña **Global** en el componente de equilibrador de carga del lienzo de diseño.
- 2 Seleccione una o varias opciones de registro del menú desplegable **Nivel de registro**.

Seleccione un nivel de registro para la recopilación de logs de tráfico de equilibrador de carga. La configuración es válida para todos los componentes de equilibrador de carga de NSX del blueprint.

La configuración del registro se define en el cliente web de vSphere.

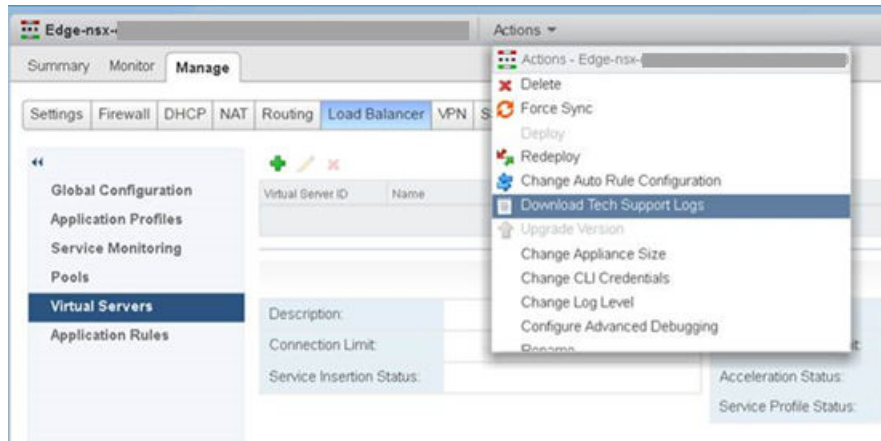
- Ninguno
- Información
- Emergencia
- Alerta
- Crítico
- Error
- Advertencia
- Aviso

- Depuración

3 Haga clic en **Guardar**.

Resultados

Puede ver y descargar los logs en el cliente web de vSphere, a través del menú **Acciones** para NSX Edge, tal y como se describe en el tema sobre *cómo descargar logs de soporte técnico de NSX Edge* en la documentación del producto NSX, en https://www.vmware.com/support/pubs/nsx_pubs.html.



Usar componentes de seguridad en el lienzo de diseño

Puede añadir componentes de seguridad de NSX al lienzo de diseño para que los ajustes configurados estén disponibles en uno o varios componentes de la máquina de vSphere en el blueprint.

Los grupos de seguridad, las etiquetas y las políticas se configuran fuera de vRealize Automation en la aplicación NSX.

La configuración del componente de red y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario ejecutar la recopilación de datos en el inventario de NSX de clústeres de vSphere. Los componentes de redes y seguridad son específicos de NSX y solo se pueden usar con componentes de máquina de vSphere. Para obtener información sobre cómo configurar NSX, consulte la *guía de administración de NSX*.

Si desea añadir controles de seguridad a los blueprints, puede configurar grupos de seguridad, etiquetas y políticas para el recurso informático de vSphere en NSX. Después de ejecutar la recopilación de datos, las configuraciones de seguridad están disponibles y pueden seleccionarse en vRealize Automation.

Grupo de seguridad

Un grupo de seguridad es una colección de activos u objetos de grupo del inventario de vSphere que se asigna a un conjunto de políticas de seguridad, por ejemplo, reglas de firewall distribuidas e integraciones de servicios de terceros tales como antivirus y detección de intrusiones. La función de grupo permite crear contenedores personalizados a los que se pueden asignar recursos, como máquinas virtuales y adaptadores de red, para la protección de firewall distribuido. En cuanto se ha definido un grupo, este se puede añadir como recurso o destino a una regla de firewall para protegerlo.

Puede añadir grupos de seguridad de NSX existentes o a petición a un blueprint, además de los grupos de seguridad especificados en la reserva.

Puede crear uno o más grupos de seguridad a petición. Puede seleccionar una o más directivas de seguridad para configurarlas en un grupo de seguridad.

Los grupos de seguridad se administran en el recurso de origen. Para obtener información sobre la administración de grupos de seguridad para los diversos tipos de recursos, consulte la documentación de NSX.

Si un blueprint contiene uno o varios equilibradores de carga y el aislamiento de aplicaciones está habilitado para el blueprint, la direcciones VIP de los equilibradores de carga se añaden al grupo de seguridad de aislamiento de aplicaciones como un IPSet. Si un blueprint contiene un grupo de seguridad a petición que está asociado con un nivel de máquina que también está asociado con un equilibrador de carga, el grupo de seguridad a petición incluye el nivel de máquina y el IPSet con la dirección VIP del equilibrador de carga.

Etiqueta de seguridad

Una etiqueta de seguridad es un objeto calificador o una entrada de categoría que puede usar como mecanismo de agrupamiento. Debe definir los criterios que debe cumplir un objeto para añadirse al grupo de seguridad que esté creando. De este modo, podrá incluir máquinas definiendo un criterio de filtro con varios parámetros que coincidan con los criterios de búsqueda. Por ejemplo, puede añadir a un grupo de seguridad todas las máquinas que tengan una determinada etiqueta de seguridad.

Puede añadir una etiqueta de seguridad al lienzo de diseño.

Política de seguridad

Una política de seguridad es un conjunto de servicios de introspección de red, firewall y endpoint que pueden aplicarse a un grupo de seguridad. Puede añadir políticas de seguridad a una máquina virtual de vSphere usando un grupo de seguridad bajo demanda en un blueprint. No puede añadir una política de seguridad directamente a una reserva. Tras la recopilación de datos, las políticas de seguridad que se hayan definido en NSX para un recurso informático podrán seleccionarse en un blueprint.

Aislamiento de aplicaciones

Cuando se habilita el aislamiento de aplicaciones, se crea una política de seguridad independiente. El aislamiento de aplicaciones usa un firewall lógico para bloquear todo el tráfico entrante y saliente de las aplicaciones en el blueprint. Las máquinas de componentes que se aprovisionan mediante un blueprint que contiene una política de aislamiento de aplicaciones se pueden comunicar entre ellas, pero no pueden conectarse fuera del firewall a menos que se añadan otros grupos de seguridad al blueprint con políticas de seguridad que permitan el acceso.

Controlar el acceso a tenants de los objetos de seguridad

Puede controlar la disponibilidad en una estructura de varios tenants de los objetos de seguridad de NSX en vRealize Automation.

Cuando se crea un objeto de seguridad de NSX en vRealize Automation, su disponibilidad predeterminada puede ser global, lo que significa que está disponible en todos los tenants para los que el endpoint asociado tenga una reserva, o bien puede estar oculto para todos los usuarios, salvo el administrador.

La disponibilidad de objetos de seguridad en todos los tenants también está relacionada con el hecho de que el endpoint asociado tenga o no una reserva o una política de reserva en el tenant.

NSX no usa tenants en los grupos de seguridad. Sin embargo, puede controlar la disponibilidad de los grupos de seguridad en vRealize Automation con la propiedad personalizada `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects`.

Los nuevos objetos de seguridad se encuentran disponibles de forma predeterminada para todos los tenants de los endpoints de NSX asociados en los que tiene una reserva. Si el endpoint no tiene ninguna reserva en el tenant activo, los objetos de seguridad no están disponibles en él.

Si no ha configurado la propiedad personalizada

`VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` en los endpoints de NSX, los nuevos objetos de seguridad se definen como globales de forma predeterminada. Asimismo, los objetos de seguridad que existían antes de actualizar a esta versión de vRealize Automation se definen como globales independientemente de la propiedad personalizada.

Nota Cuando se actualiza a esta versión de vRealize Automation, los grupos de seguridad de la versión anterior se definen como globales de forma predeterminada. Los grupos y las etiquetas de seguridad existentes están disponibles en todos los tenants en los que el endpoint asociado tiene una reserva.

Puede ocultar los nuevos grupos de seguridad de forma predeterminada añadiendo la propiedad personalizada `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` al endpoint asociado de NSX. Esta configuración se hará efectiva la próxima vez que se recopilen los datos del endpoint de NSX y que este se aplique únicamente a los nuevos objetos de seguridad.

También puede cambiar la configuración de tenants de un objeto de seguridad existente mediante programación. Por ejemplo, si un grupo de seguridad se define como global, puede cambiar la disponibilidad de los tenants de un objeto de seguridad usando la configuración de ID de tenant del endpoint asociado de NSX, que se puede encontrar en la API de REST de vRealize Automation o en vRealize CloudClient. Los valores de configuración de ID de tenant disponibles para el endpoint de NSX son los siguientes:

- "<global>": el objeto de seguridad está disponible para todos los tenants. Esta es la configuración predeterminada para los objetos de seguridad existentes después de actualizar a esta versión y para todos los objetos de seguridad nuevos que cree.
- "<unscoped>": el objeto de seguridad no está disponible para ningún tenant. Solo el administrador del sistema puede acceder al objeto de seguridad. Esta configuración es idónea para definir los objetos de seguridad que finalmente se asignarán a un tenant específico.
- "*tenant_id_name*": el objeto de seguridad únicamente está disponible para un solo tenant con nombre.

Puede emplear la API de REST de vRealize Automation o las herramientas de vRealize CloudClient para asignar a un tenant con nombre el parámetro de ID de tenant (*tenantId*) de los objetos de seguridad que están asociados a un endpoint específico. Para obtener información relacionada, consulte <https://code.vmware.com/apis/vrealize-automation> y <https://code.vmware.com/web/dp/explorer-apis>. Para obtener información sobre vRealize CloudClient, consulte <https://code.vmware.com/web/dp/tool/cloudclient>. Para obtener información adicional, consulte la *Guía de programación* de vRealize Automation en <https://docs.vmware.com/es/vRealize-Automation>.

Añadir un componente de grupo de seguridad existente

Puede añadir un componente de grupo de seguridad existente de NSX al lienzo de diseño como preparación para asociar su configuración a uno o varios componentes de máquina o a otros tipos de componentes disponibles en el blueprint.

Puede usar un componente de grupo de seguridad existente para añadir un grupo de seguridad de NSX al lienzo de diseño y configurar sus ajustes para usarlo con componentes de máquina de vSphere y componentes de Software o XaaS pertenecientes a vSphere.

Cuando se crea un blueprint, se exponen de forma predeterminada los grupos de seguridad que corresponden al tenant actual. En concreto, dichos grupos se encuentran disponibles si el endpoint asociado tiene una reserva en el tenant actual. Para obtener más información sobre cómo controlar el acceso a los tenants, consulte [Controlar el acceso a tenants de los objetos de seguridad](#).

Requisitos previos

- Cree y configure un grupo de seguridad en NSX. Consulte *Configuración de vRealize Automation* y la *guía de administración de NSX*.
- Compruebe que el inventario de NSX se ha ejecutado correctamente en el clúster.

Para usar las configuraciones de NSX en vRealize Automation, debe ejecutar una recopilación de datos.

- Revise los conceptos de los componentes de seguridad. Consulte [Usar componentes de seguridad en el lienzo de diseño](#).
- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Abra un blueprint nuevo o uno ya existente en el lienzo de diseño mediante la pestaña **Diseño**.

Procedimiento

- 1 Haga clic en **Redes y seguridad** en la sección Categorías para mostrar la lista de componentes de red y seguridad disponibles.
- 2 Arrastre un componente **Grupo de seguridad existente** al lienzo de diseño.
- 3 Seleccione uno de los grupos de seguridad del menú desplegable **Grupo de seguridad**.
- 4 Haga clic en **Aceptar**.
- 5 Haga clic en **Finalizar** para guardar el blueprint como un borrador o seguir con la configuración del blueprint.

Resultados

Si desea configurar más opciones de seguridad, añada componentes de seguridad adicionales y seleccione las opciones de configuración en la pestaña **Seguridad** de un componente de máquina de vSphere en el lienzo de diseño.

Añadir un componente de grupo de seguridad a petición

Puede añadir un componente de grupo de seguridad de NSX a petición al lienzo de diseño como preparación para asociar su configuración a uno o varios componentes de máquina de vSphere o a otros tipos de componentes disponibles en el blueprint.

Cuando se crea un grupo de seguridad a petición, se añaden políticas de seguridad. Dichas políticas se pueden ocultar o exponer globalmente de forma predeterminada. Las políticas solo se exponen en los tenants en los que el endpoint de NSX asociado tiene una reserva.

Cuando se crea un blueprint, se exponen de forma predeterminada los grupos de seguridad que corresponden al tenant actual. En concreto, dichos grupos se encuentran disponibles si el endpoint asociado tiene una reserva en el tenant actual. Para obtener más información sobre cómo controlar el acceso a los tenants, consulte [Controlar el acceso a tenants de los objetos de seguridad](#).

Requisitos previos

- Cree y configure una política de seguridad en NSX. Consulte la *guía de administración de NSX*.
- Compruebe que el inventario de NSX se ha ejecutado correctamente en el clúster.

Para usar las configuraciones de NSX en vRealize Automation, debe ejecutar una recopilación de datos.

- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Revise los conceptos de los componentes de seguridad. Consulte [Usar componentes de seguridad en el lienzo de diseño](#).
- Abra un blueprint nuevo o uno ya existente en el lienzo de diseño mediante la pestaña **Diseño**.

Procedimiento

- 1 Haga clic en **Redes y seguridad** en la sección Categorías para mostrar la lista de componentes de red y seguridad disponibles.
- 2 Arrastre un componente **Grupo de seguridad a petición** al lienzo de diseño.
- 3 Especifique un nombre y, opcionalmente, una descripción.
- 4 Para añadir una o varias políticas de seguridad, haga clic en el icono Añadir en el área **Políticas de seguridad** y seleccione políticas de seguridad disponibles.
- 5 Haga clic en **Aceptar**.
- 6 Haga clic en **Finalizar** para guardar el blueprint como un borrador o seguir con la configuración del blueprint.

Resultados

Si desea configurar más opciones de seguridad, añada componentes de seguridad adicionales y seleccione las opciones de configuración en la pestaña **Seguridad** de un componente de máquina de vSphere en el lienzo de diseño.

Añadir un componente de etiqueta de seguridad existente

Puede añadir un componente de etiqueta de seguridad de NSX al lienzo de diseño del blueprint como preparación para asociar su configuración a uno o varios componentes de máquina en el blueprint.

Puede usar un componente de etiqueta de seguridad para añadir una etiqueta de seguridad de NSX al lienzo de diseño y configurar sus ajustes para usarlo con componentes de máquina de vSphere y componentes de Software pertenecientes a vSphere.

Cuando se crea un blueprint, se exponen de forma predeterminada las etiquetas de seguridad que corresponden al tenant actual. En concreto, dichas etiquetas se encuentran disponibles si el endpoint asociado tiene una reserva en el tenant actual. Para obtener más información sobre cómo controlar el acceso a los tenants, consulte [Controlar el acceso a tenants de los objetos de seguridad](#).

Se pueden añadir varios componentes de redes y seguridad al lienzo de diseño.

Requisitos previos

- Cree y configure etiquetas de seguridad en NSX. Consulte *Configuración de vRealize Automation* y la *guía de administración de NSX*.

- Compruebe que el inventario de NSX se ha ejecutado correctamente en el clúster.

Para usar las configuraciones de NSX en vRealize Automation, debe ejecutar una recopilación de datos.

- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Abra un blueprint nuevo o uno ya existente en el lienzo de diseño mediante la pestaña **Diseño**.

Procedimiento

- 1 Haga clic en **Redes y seguridad** en la sección Categorías para mostrar la lista de componentes de red y seguridad disponibles.
- 2 Arrastre un componente **Etiqueta de seguridad existente** al lienzo de diseño.
- 3 Haga clic en el cuadro de texto **Etiqueta de seguridad** y seleccione una etiqueta de seguridad existente.
- 4 Haga clic en **Aceptar**.
- 5 Haga clic en **Finalizar** para guardar el blueprint como un borrador o seguir con la configuración del blueprint.

Resultados

Si desea configurar más opciones de seguridad, añada componentes de seguridad adicionales y seleccione las opciones de configuración en la pestaña **Seguridad** de un componente de máquina de vSphere en el lienzo de diseño.

Asociar componentes de red y de seguridad

Puede arrastrar componentes de red y de seguridad al lienzo de diseño para incluir sus opciones de configuración en la configuración de componentes de máquina en el blueprint. Tras definir la configuración de red y de seguridad de la máquina, también puede asociar la configuración desde el componente de equilibrador de carga.

Tras añadir un componente de red o de seguridad de NSX al lienzo de diseño y definir la configuración disponible, podrá abrir las pestañas de red y de seguridad de un componente de máquina de vSphere en el lienzo y ajustar su configuración.

Puede arrastrar un componente de red NAT a petición al lienzo de diseño y asociarlo a un componente de máquina de vSphere o a un componente de equilibrador de carga de NSX del blueprint.

La configuración del componente de red y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario ejecutar la recopilación de datos en el inventario de NSX de clústeres de vSphere. Los componentes de redes y seguridad son específicos de NSX y solo se pueden usar con componentes de máquina de vSphere. Para obtener información sobre cómo configurar NSX, consulte la *guía de administración de NSX*.

Nota Si un blueprint contiene uno o varios equilibradores de carga y el aislamiento de aplicaciones está habilitado para el blueprint, la direcciones VIP de los equilibradores de carga se añaden al grupo de seguridad de aislamiento de aplicaciones como un IPSet. Si un blueprint contiene un grupo de seguridad a petición que está asociado con un nivel de máquina que también está asociado con un equilibrador de carga, el grupo de seguridad a petición incluye el nivel de máquina y el IPSet con la dirección VIP del equilibrador de carga.

Para obtener información sobre el uso de reglas NAT que permitan a un puerto TCP o UDP asignar desde la dirección IP externa de una instancia de Edge (puerto de origen) a una dirección IP privada en el componente de red NAT (puerto de destino), consulte [Crear y usar las reglas NAT](#).

Configurar un blueprint para aprovisionar desde un OVF

Puede utilizar un OVF para definir las propiedades de máquina y la configuración de hardware de vSphere, las cuales normalmente se definen en las páginas de configuración de blueprint de vRealize Automation o mediante programación usando las API de REST de vRealize Automation o vRealize CloudClient.

También puede importar la configuración de un OVF para definir un conjunto de valores de un perfil de componente de imagen. Los blueprints parametrizados utilizan los tipos de perfil de componente de imagen y tamaño.

OVF es un estándar de código abierto de empaquetado y distribución de aplicaciones de software para máquinas virtuales.

El aprovisionamiento de OVF es similar a la clonación, salvo que la máquina de origen es una plantilla de OVF alojada en un servidor o un sitio web, en lugar de una plantilla de máquina virtual alojada en vCenter.

Un archivo OVF se suele utilizar para describir una única máquina virtual o un único dispositivo virtual. Puede contener información sobre el formato de un archivo de imagen de disco virtual y una descripción del hardware virtual que debe emularse para ejecutar el sistema operativo o la aplicación contenidos en la imagen de disco. Un archivo OVA es un paquete de dispositivo virtual que contiene archivos que se utilizan para describir una máquina virtual, como un archivo de descriptor de OVF, los archivos de manifiesto y certificado opcionales, y otros archivos relacionados.

La opción de aprovisionamiento `ImportOvfWorkflow` está disponible en un componente de máquina de vSphere al definir un blueprint. También está disponible al definir un conjunto de valores de un perfil de componente de imagen en el diccionario de propiedades.

Puede añadir opciones de configuración de blueprint a un OVF para describir los siguientes tipos de información:

- Asignaciones mínimas de CPU, memoria y almacenamiento.
- Propiedades personalizadas configurables por el usuario.
- Configuración de los perfiles de componente para la parametrización de blueprints.

No se admiten OVF ni OVA con varias máquinas.

Las consideraciones fundamentales incluyen las siguientes afirmaciones:

- Se admiten los archivos OVF y los paquetes OVA.
- Se admite la autenticación básica de nombre de usuario y contraseña para el servidor HTTP en el que residen los OVF u OVA alojados. La URL especificada se valida en el blueprint.
- No se recopilan los datos de los OVF ni de los OVA desde vCenter Server.
- Se admiten las suscripciones de EBS.
- Puede definir propiedades personalizadas al importar ajustes de OVF configurables por el usuario al blueprint.
- Puede añadir, cambiar o eliminar la configuración obtenida a partir de una importación de OVF al solicitar el aprovisionamiento de máquinas de vSphere.
- Puede agregar, cambiar o quitar la configuración durante la reconfiguración de la máquina.

Definir la configuración del blueprint para un componente de vSphere a través de un OVF

Puede importar la configuración de un OVF para simplificar el proceso de configuración de los componentes de máquina de vSphere en un blueprint de vRealize Automation.

En este procedimiento se asume que cuenta con un conocimiento básico del proceso de creación de blueprints de vRealize Automation.

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Debe cumplir con los requisitos previos restantes que se especifican en [Configurar un blueprint de máquina](#).

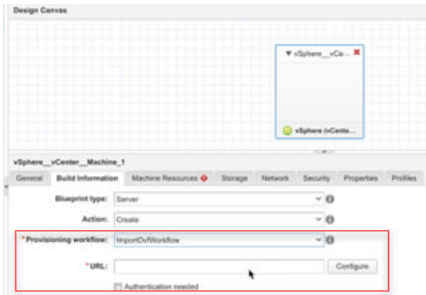
Procedimiento

- 1 Seleccione **Diseño > Blueprints**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Introduzca un nombre y una descripción para el blueprint, y haga clic en **Aceptar**.
- 4 Haga clic en **Tipos de máquina** en el área Categorías y arrastre un componente de **Máquina de vSphere (vCenter)** al lienzo de diseño.

5 Haga clic en la pestaña **Información de creación** y especifique las siguientes opciones:

- **Tipo de blueprint:** servidor
- **Acción:** crear
- **Flujo de trabajo de aprovisionamiento:** ImportOvfWorkflow

El parámetro ImportOvfWorkflow permite que la opción **URL** esté disponible.



6 Especifique la ubicación del OVF.

- Introduzca la ruta de acceso a la URL de OVF con el formato `https://servidor/carpeta/nombre.ovf` o `nombre.ova`.

Si habilita la autenticación con el servidor que aloja el OVF, introduzca las credenciales del usuario que se autentica.

- Si el OVF está alojado en un sitio web y ha creado un endpoint de proxy que se utilizará para acceder al sitio web, seleccione **Utilizar proxy** y seleccione el endpoint de proxy disponible.

7 Haga clic en **Configurar**.

Nota Si recibe un mensaje de error de autenticación, el servidor en el que se aloja el OVF requiere credenciales de autenticación. Si esto ocurre, active la casilla **Autenticación necesaria**, introduzca las credenciales de **Nombre de usuario** y **Contraseña** necesarias para autenticar con el servidor HTTP en el que reside el OVF, y vuelva a hacer clic en **Configurar**.

La opción Configurar abre un asistente, el cual muestra todas las propiedades configurables por el usuario y los valores que se importarán del OVF como propiedades personalizadas. Si no hay propiedades configurables para importar, el panel está vacío.

- a Use el asistente para aceptar los valores predeterminados que se van a importar o cambie esos valores del blueprint antes de importarlos.
- b Haga clic en **Aceptar** para importar las propiedades y los valores.

Todas las propiedades configurables por el usuario de la plantilla de OVF se importan al blueprint como propiedades personalizadas editables de vRealize Automation, precedidas de `VMware.Ovf`, mientras que otras se importan como propiedades ocultas que no están diseñadas para editarse después de importarlas.

- 8 Haga clic en la pestaña **Recursos de máquinas** para mostrar los resultados de la importación de OVF que se reflejan en las entradas de valor mínimo para las opciones **CPU**, **Memoria (MB)** y **Almacenamiento (GB)**.

Puede cambiar cualquiera de estos valores tras la importación.

- 9 Haga clic en la pestaña **Almacenamiento** para mostrar los resultados de la importación de OVF.
- 10 Haga clic en la secuencia de pestañas **Propiedades > Propiedades personalizadas** para mostrar los resultados de la importación de OVF.
- 11 Haga clic en **Guardar**.

Pasos siguientes

Siga definiendo la configuración del blueprint o haga clic en **Finalizar**.

Definir un conjunto de valores de imagen para un perfil de componente mediante un OVF

Puede importar la configuración de un OVF para crear uno o varios conjuntos de valores de modo que se utilice un perfil de componente de imagen en un blueprint de vRealize Automation parametrizado.

Después de importar las definiciones de los conjuntos de valores del perfil de componentes de Image, puede añadir uno o varios conjuntos de valores al perfil de componentes de un componente de máquina de vSphere en un blueprint. Cuando un usuario solicita un elemento del catálogo, puede seleccionar una instancia de Image disponible e implementarla utilizando los parámetros que se definen en el conjunto de valores de la imagen.

Al importar el OVF, las propiedades configurables por el usuario y los valores del OVF no se importan como propiedades personalizadas en el conjunto de valores. Si desea usar nuevas propiedades personalizadas del OVF importado en relación con el conjunto de valores de imagen, debe definir manualmente las nuevas propiedades personalizadas en el blueprint general o el componente de máquina de vSphere. Las propiedades personalizadas creadas en el blueprint parametrizado deberían poder aplicarse al conjunto de valores de cada imagen de perfil de componente.

Nota Las propiedades personalizadas de OVF para vRealize Automation no se pueden aplicar a las propiedades personalizadas de OVF para vSphere. Considere la posibilidad de crear un conjunto de valores de imagen para vRealize Automation y otro para vSphere.

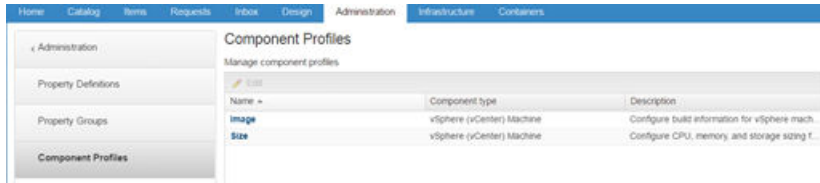
Para obtener más información sobre el uso de perfiles de componente para la parametrización de blueprints, consulte [Descripción y el uso de la parametrización de blueprints](#).

Requisitos previos

- Inicie sesión en vRealize Automation como administrador con derechos de acceso de **administrador de tenants** y **administrador de IaaS**.

Procedimiento

- 1 Seleccione **Administración > Diccionario de propiedades > Perfiles de componentes**.



- 2 Haga clic en **Imagen** en la columna Nombre.

Se muestra información acerca de la propiedad del componente de imagen proporcionada.

- 3 Haga clic en la pestaña **Conjuntos de valores**.

- 4 Para definir un conjunto de valores nuevo, haga clic en **Nuevo** y configure la opción Image.

- a Introduzca un valor en el campo **Nombre para mostrar** para anexarlo al delimitador ValueSet (por ejemplo, **Prod0VF**).
- b Acepte el valor predeterminado que se muestra en el cuadro de texto **Nombre** o introduzca un nombre personalizado.
- c Escriba una descripción, como **Opción de compilación para clonar el escenario A** en el cuadro de texto **Descripción**.
- d Seleccione **Activo** o **Inactivo** en el menú desplegable **Estado**.
 Seleccione **Activo** para permitir que el conjunto de valores se vea en el catálogo que aprovisiona el formulario de solicitud.
- e Seleccione la acción de compilación **Crear**.
- f Seleccione **Servidor** o **Escritorio** como el tipo de blueprint.
- g Seleccione el flujo de trabajo de aprovisionamiento **ImportOvfWorkflow**.
- h Introduzca la ruta de acceso a la URL de OVF con el formato `https://servidor/carpeta/nombre.ovf` o `nombre.ova`.
- i Si habilita la autenticación con el servidor que aloja el OVF, introduzca las credenciales del usuario que se autentica.
- j Si el OVF está alojado en un sitio web y ha creado un endpoint de proxy que se utilizará para acceder al sitio web, seleccione **Utilizar proxy** y seleccione el endpoint de proxy disponible.

- 5 Haga clic en **Guardar**.

- 6 Cuando considere que las opciones están bien configuradas, haga clic en **Finalizar**.

Pasos siguientes

Después de crear la imagen e importar el OVF para definir el conjunto de valores de imagen, puede añadir la imagen a un componente de máquina de vSphere en un blueprint.

Usar componentes de contenedor en blueprints

Puede configurar y usar componentes de contenedor en el blueprint.

Después de que un administrador de contenedores cree definiciones de contenedor en Contenedores para vRealize Automation, un arquitecto de contenedores puede añadir y configurar componentes de contenedor para blueprints de vRealize Automation en el lienzo de diseño.

Configurar los componentes de contenedor

Puede configurar ajustes y opciones de blueprint para un componente de contenedor de Contenedores para vRealize Automation en el lienzo de diseño de vRealize Automation.

Pestaña **General**

Ajuste la configuración general del componente de contenedor de blueprint en el lienzo de diseño.

Tabla 3-33. Configuración de la pestaña **General**

Configuración	Descripción
Nombre	Escriba un nombre para el componente de contenedor en el blueprint.
Descripción	Resuma el componente de contenedor en provecho de otros arquitectos.
Imagen	Introduzca el nombre completo de una imagen en un registro administrado, como un registro privado o un registro de Docker Hub (por ejemplo: registry.hub.docker.com/library/python).
Comandos	Introduzca un comando que se aplique a la imagen especificada, como python app.py. El comando se ejecuta cuando se inicia el proceso de aprovisionamiento de contenedores.
Vínculos	Los vínculos ofrecen otra manera de conectar contenedores en un solo host o entre hosts. Especifique uno o varios servicios a los que este contenedor debe vincularse, como redis o datadog.

Pestaña **Red**

Ajuste la configuración de red del componente de contenedor de blueprint en el lienzo de diseño.

Puede adjuntar un contenedor a una red. La red se muestra como un componente de red de contenedor en el lienzo de diseño. La información sobre las redes disponibles se indica en la página Red del formulario del componente de contenedor.

Tabla 3-34. Configuración de la pestaña **Red**

Configuración	Descripción
Redes	Especifique las redes existentes que se han definido para la imagen seleccionada. También puede crear una nueva red. Cuando añada un componente de contenedor de red al formulario de diseño, las redes que especifique aquí se mostrarán como opciones que se pueden seleccionar.
Enlaces de puerto	Especifique los enlaces de puerto de la red seleccionada. Los enlaces de punto constan de un host de protocolo, un puerto de host y un puerto de contenedor.
Publicar todos los puertos	Active la casilla de verificación para exponer los puertos que se utilizan en la imagen de contenedor a todos los usuarios.
Nombre del host	Especifique el nombre de host de contenedor. Si no indica ningún nombre, se utilizará el valor predeterminado, el cual es el nombre del componente de contenedor del blueprint.
Modo de red	Especifique la pila de red del contenedor. Si no se especifica ningún valor, el contenedor estará configurado en modo de red de puente.

Pestaña **Almacenamiento**

Ajuste la configuración de almacenamiento del componente de contenedor de blueprint en el lienzo de diseño.

Tabla 3-35. Configuración de la pestaña **Almacenamiento**

Configuración	Descripción
Volúmenes	Especifique los volúmenes de almacenamiento que están asignados desde el host para que el contenedor los utilice.
Volúmenes de	Especifique los volúmenes de almacenamiento que se heredarán de otro contenedor.
Directorio operativo	Especifique el directorio desde el que se ejecutan los comandos.

Pestaña **Política**

Ajuste la configuración de políticas, como la política de implementación y las restricciones de afinidad, para el componente de contenedor de blueprint en el lienzo de diseño.

Tabla 3-36. Configuración de la pestaña **Política**

Configuración	Descripción
Política de implementación	<p>Especifique una política de implementación para configurar las preferencias correspondientes al conjunto de hosts que se utilizará para la implementación de este contenedor. Puede asociar políticas de implementación a hosts, políticas y definiciones de contenedores para definir una preferencia para los hosts, las políticas y las cuotas al implementar un contenedor.</p> <p>Es posible añadir una política de implementación mediante la pestaña Contenedores de vRealize Automation.</p>
Tamaño del clúster	Especifique el número de instancias que desea generar como un clúster a partir de este contenedor.
Reiniciar política	Especifique una política de reinicio para la manera en que se debe reiniciar un contenedor al salir.
Reinicio máx.	Si seleccionó Tras un error como política de reinicio, puede especificar la cantidad máxima de reinicios.
Recursos de CPU compartidos	Especifique la cantidad de recursos compartidos de CPU asignados al recurso aprovisionado.
Límite de memoria	Indique un número entre 0 y la cantidad de memoria disponible en la zona de colocación. Este valor corresponde a la memoria total disponible para los recursos en esta colocación. 0 significa sin límite.
Intercambio de memoria	Límite de memoria total.
Restricciones de afinidad	<p>Define reglas para el aprovisionamiento de contenedores en el mismo host o en hosts diferentes.</p> <ul style="list-style-type: none"> ■ Tipo de afinidad <p>Para usar antiafinidad, los contenedores se colocan en hosts diferentes; en caso contrario, se colocan en el mismo host.</p> ■ Servicio <p>El nombre del servicio que está disponible en el menú desplegable coincide con el nombre del componente de contenedor especificado en el campo Nombre de la pestaña General.</p> ■ Restricción <p>Una restricción estricta especifica que, si no se cumple la restricción, el aprovisionamiento fallará. Una restricción flexible especifica que, aunque no se cumpla la restricción, el aprovisionamiento continuará.</p>

Pestaña **Entorno**

Ajuste la configuración del entorno (como los enlaces de propiedades) para el componente de contenedor de blueprint en el lienzo de diseño.

Tabla 3-37. Configuración de la pestaña **Entorno**

Configuración	Descripción
Nombre	El nombre de la variable.
Enlace	Se enlaza la variable a otra propiedad, que forma parte de la plantilla. Cuando se selecciona el enlace, es necesario introducir un valor en la sintaxis <code>_resource~TemplateComponent~TemplateComponentProperty</code> .
Valor	El valor de la variable de entorno o, si se seleccionó el enlace, el valor de la propiedad que se desea enlazar.

Pestaña Propiedades

Configure propiedades personalizadas individuales y grupos de propiedades personalizadas para el componente de contenedor de blueprint en el lienzo de diseño.

Si selecciona la pestaña **Grupos de propiedades** y hace clic en **Añadir**, se ofrecerán las siguientes opciones:

- Propiedades del host de contenedor con autenticación con certificado
- Propiedades del host de contenedor con autenticación con usuario/contraseña

También aparecerán los grupos de propiedades adicionales que se hayan definido.

Si selecciona la pestaña **Propiedades personalizadas** y hace clic en **Añadir**, puede agregar propiedades personalizadas individuales al componente de contenedor.

Tabla 3-38. Configuración de la pestaña **Propiedades** para propiedades personalizadas

Configuración	Descripción
Nombre	Escriba el nombre de una propiedad personalizada o seleccione una de las propiedades personalizadas disponibles en el menú desplegable.
Valor	Escriba o edite un valor para asociarlo al nombre de propiedad personalizada.
Cifrado	Puede optar por cifrar el valor de la propiedad si, por ejemplo, el valor es una contraseña.
Reemplazable	Puede especificar que la próxima persona u otra más adelante que utilice la propiedad pueda reemplazar el valor de la propiedad. Por lo general, suele ser otro arquitecto, pero, si selecciona Mostrar en solicitud , los usuarios empresariales podrán ver y editar valores de propiedades cuando soliciten elementos del catálogo.
Mostrar en solicitud	Si desea mostrar el nombre y el valor de la propiedad a los usuarios finales, puede seleccionar la opción para mostrar la propiedad en el formulario de solicitud cuando se solicite el aprovisionamiento de la máquina. También debe seleccionar Reemplazable si desea que los usuarios proporcionen un valor.

Pestaña **Configuración de estado**

Especifique un modo de configuración de estado para el componente de contenedor de blueprint en el lienzo de diseño.

Tabla 3-39. Opciones de la pestaña **Configuración de estado**

Tipo de modo	Descripción
Ninguno	Predeterminado. No se configura ninguna comprobación de estado.
HTTP	<p>Si selecciona HTTP, debe proporcionar una API para acceder, así como el método y la versión de HTTP que se utilizarán. La API es relativa y no es necesario que introduzca la dirección del contenedor. También puede especificar un período de tiempo de espera para la operación y definir umbrales de estado.</p> <p>Por ejemplo, un umbral de buen estado con un valor de 2 significa que deben producirse dos llamadas consecutivas con éxito para que se considere que el contenedor está en buen estado y en ejecución (estado RUNNING). Un umbral de mal estado con un valor de 2 significa que deben producirse errores en dos llamadas para que se considere que el contenedor está en mal estado y en situación de error (estado ERROR). Para todos los casos intermedios entre los umbrales de buen estado y mal estado, el estado del contenedor es DEGRADED.</p>
Conexión TCP	Si selecciona Conexión TCP , solo debe especificar un puerto para el contenedor. La comprobación de estado intenta establecer una conexión TCP con el contenedor en el puerto indicado. También puede especificar un valor de tiempo de espera para la operación y definir umbrales de buen estado o de mal estado, al igual que con HTTP.
Comando	Si selecciona Comando , debe introducir el comando que se ejecutará en el contenedor. El estado de salida del comando determina el éxito de la comprobación de estado.
Omitir comprobación de estado en aprovisionamiento	Desactive esta opción para forzar la comprobación del estado durante el aprovisionamiento. Al hacerlo, no se considerará que un contenedor está aprovisionado hasta que supere correctamente una comprobación de estado.
AutoDeploy	Reimplementación automática de los contenedores cuando se encuentran en el estado ERROR.

Pestaña **Configuración de log**

Especifique un modo de registro y opciones de registro adicionales para el componente de contenedor de blueprint en el lienzo de diseño.

Tabla 3-40. Configuración de la pestaña **Configuración de log**

Configuración	Descripción
Controlador	Seleccione un formato de registro del menú desplegable.
Opciones	Introduzca las opciones del controlador utilizando un formato de nombre y de valor que sea coherente con el formato de registro.

Usar propiedades de contenedor y grupos de propiedades en un blueprint

Puede añadir grupos de propiedades predefinidos a un componente de contenedor de un blueprint de vRealize Automation. Cuando las máquinas se aprovisionan utilizando un blueprint que contiene estas propiedades, la máquina aprovisionada se registra como máquina host de Docker Container.

Contenedores para vRealize Automation ofrecía los dos grupos de propiedades siguientes de propiedades personalizadas específicas de contenedor. Cuando agrega un componente de contenedor a un blueprint, puede agregar estos grupos de propiedades al contenedor para registrar las máquinas aprovisionadas como hosts de contenedor.

- Propiedades del host de contenedor con autenticación con certificado
- Propiedades del host de contenedor con autenticación con usuario/contraseña

Estos grupos de propiedades se pueden encontrar en vRealize Automation cuando se selecciona **Administración > Diccionario de propiedades > Grupos de propiedades**.

Puesto que todos los tenants comparten los grupos de propiedades, se recomienda clonar y personalizar las propiedades si trabaja en un entorno de varios tenants. Al asignar nombres exclusivos a los grupos de propiedades y a las propiedades en los grupos, puede editarlos para definir valores personalizados que se utilizarán en un tenant específico.

Las propiedades usadas con mayor frecuencia son `Container.Auth.PublicKey` y `Container.Auth.PrivateKey`, que permiten al administrador de contenedores proporcionar el certificado de cliente para realizar la autenticación en el host de contenedor.

Tabla 3-41. Propiedades personalizadas de Contenedores

Propiedad	Descripción
<code>containers.ipam.driver</code>	Solo se puede utilizar con contenedores. Especifica el controlador de IPAM que se usará cuando se añada un componente de red de Contenedores a un blueprint. Los valores admitidos dependen de los controladores que están instalados en el entorno de host de contenedor en el que se utilizan. Por ejemplo, según los complementos de IPAM que estén instalados en el host de contenedor, un valor admitido podría ser <code>infoblox</code> o <code>calico</code> .
<code>containers.network.driver</code>	Solo se puede utilizar con contenedores. Especifica el controlador de red que se empleará cuando se añada un componente de red de Contenedores a un blueprint. Los valores admitidos dependen de los controladores que están instalados en el entorno de host de contenedor en el que se utilizan. De forma predeterminada, los controladores de red suministrados por Docker incluyen <code>bridge</code> , <code>overlay</code> y <code>macvlan</code> , mientras que los controladores de red proporcionados por el host de contenedor virtual (Virtual Container Host, VCH) incluyen el controlador <code>bridge</code> . También puede que estén disponibles controladores de red de terceros, como <code>weave</code> y <code>calico</code> , en función de los complementos de red que estén instalados en el host de contenedor.
<code>Container</code>	Solo se puede utilizar con contenedores. El valor predeterminado, <code>App.Docker</code> , es obligatorio. No modifique esta propiedad.
<code>Container.Auth.User</code>	Solo se puede utilizar con contenedores. Especifica el nombre de usuario para la conexión al host de Contenedores.
<code>Container.Auth.Password</code>	Solo se puede utilizar con contenedores. Indica la contraseña del nombre de usuario o la contraseña de clave pública o privada que se utilizará. Se admite el cifrado del valor de la propiedad.
<code>Container.Auth.PublicKey</code>	Solo se puede utilizar con contenedores. Especifica la clave pública para la conexión al host de Contenedores.
<code>Container.Auth.PrivateKey</code>	Solo se puede utilizar con contenedores. Especifica la clave privada para la conexión al host de Contenedores. Se admite el cifrado del valor de la propiedad.
<code>Container.Connection.Protocol</code>	Solo se puede utilizar con contenedores. Especifica el protocolo de comunicación. El valor predeterminado, <code>API</code> , es obligatorio. No modifique esta propiedad.
<code>Container.Connection.Scheme</code>	Solo se puede utilizar con contenedores. Especifica el esquema de comunicación. El valor predeterminado es <code>https</code> .
<code>Container.Connection.Port</code>	Solo se puede utilizar con contenedores. Especifica el puerto de conexión de Contenedores. El valor predeterminado es <code>2376</code> .

Tabla 3-41. Propiedades personalizadas de Contenedores (continuación)

Propiedad	Descripción
Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.MachineActivated	Solo se puede utilizar con contenedores. Especifica la propiedad de agente de eventos para exponer todas las propiedades de Contenedores y se utiliza con el fin de registrar un host aprovisionado. El valor predeterminado, Container*, es obligatorio. No modifique esta propiedad.
Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.Disposing	Solo se puede utilizar con contenedores. Especifica la propiedad de agente de eventos para exponer todas las propiedades de Contenedores anteriores y se utiliza con el fin de eliminar un host aprovisionado del registro. El valor predeterminado, Container*, es obligatorio. No modifique esta propiedad.

Usar Contenedores componentes de red en el lienzo de diseño

Puede añadir uno o varios componentes de red de Contenedores al lienzo de diseño y configurar las opciones de los componentes de máquina de vSphere en el blueprint.

Puede agregar `containers.ipam.driver` y `containers.network.driver` al componente al añadirlo al blueprint.

Añadir un componente de red de contenedor

Puede añadir información de red de contenedor a un blueprint de vRealize Automation que contenga componentes de contenedor.

Puede configurar contenedores en Contenedores para vRealize Automation usando la pestaña **Contenedores** de vRealize Automation. Puede añadir estos contenedores y sus configuraciones de red como componentes en un blueprint utilizando las opciones de la pestaña **Diseño** de vRealize Automation.

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto de contenedores**.
- Abra un blueprint nuevo o uno ya existente en el lienzo de diseño mediante la pestaña **Diseño**.

Procedimiento

- 1 Haga clic en **Redes y seguridad** en la sección Categorías para mostrar la lista de componentes de red y seguridad disponibles.
- 2 Arrastre un componente **Red de contenedor** al lienzo de diseño.
- 3 Introduzca un nombre en el cuadro de texto **Nombre** para etiquetar el componente de forma exclusiva en el lienzo de diseño.
- 4 (opcional) Escriba una descripción del componente en el cuadro de texto **Descripción**.

- 5 (opcional) Active la casilla de verificación **Externo** si no desea especificar la configuración de IPAM externo.

Si activa la casilla de verificación **Externo**, se quita la pestaña **Configuración de IPAM**.

- 6 Haga clic en la pestaña **Configuración de IPAM** para especificar una subred, un rango de IP y una puerta de enlace nuevos, o bien editar una subred, un rango de IP y una puerta de enlace existentes, para la red especificada en un componente de contenedor del blueprint.

La configuración de IPAM se aplica a las nuevas redes creadas por vRealize Automation, no a las que se han creado previamente en Docker o en otra aplicación de contenedor compatible. Esta configuración no está validada y se producirán errores en el aprovisionamiento si se superpone con la de otras redes. Por ejemplo, la subred y la puerta de enlace deben ser únicas en el host de contenedor.

- 7 Haga clic en la pestaña **Propiedades** para especificar propiedades personalizadas para el componente.

Si selecciona la pestaña **Grupos de propiedades** y hace clic en **Añadir**, se ofrecerán las siguientes opciones:

- Propiedades del host de contenedor con autenticación con certificado
- Propiedades del host de contenedor con autenticación con usuario/contraseña

También aparecerán los grupos de propiedades adicionales que se hayan definido.

Si selecciona la pestaña **Propiedades personalizadas** y hace clic en **Añadir**, puede agregar propiedades personalizadas individuales al componente de contenedor.

Tabla 3-42. Configuración de la pestaña **Propiedades para propiedades personalizadas**

Configuración	Descripción
Nombre	Escriba el nombre de una propiedad personalizada o seleccione una de las propiedades personalizadas disponibles en el menú desplegable.
Valor	Escriba o edite un valor para asociarlo al nombre de propiedad personalizada.
Cifrado	Puede optar por cifrar el valor de la propiedad si, por ejemplo, el valor es una contraseña.
Reemplazable	Puede especificar que la próxima persona u otra más adelante que utilice la propiedad pueda reemplazar el valor de la propiedad. Por lo general, suele ser otro arquitecto, pero, si selecciona Mostrar en solicitud , los usuarios empresariales podrán ver y editar valores de propiedades cuando soliciten elementos del catálogo.
Mostrar en solicitud	Si desea mostrar el nombre y el valor de la propiedad a los usuarios finales, puede seleccionar la opción para mostrar la propiedad en el formulario de solicitud cuando se solicite el aprovisionamiento de la máquina. También debe seleccionar Reemplazable si desea que los usuarios proporcionen un valor.

- 8 Haga clic en **Finalizar** para guardar el blueprint como un borrador o seguir con la configuración del blueprint.

Pasos siguientes

Puede seguir ajustando la configuración de red de contenedor en la pestaña **Red** de un componente de contenedor en el lienzo de diseño.

Insertar plantillas de contenedores para su utilización en blueprints

Puede hacer que una plantilla de contenedor esté disponible para ser utilizada en un blueprint de vRealize Automation.

Una plantilla de contenedor puede incluir varios contenedores. Cuando se inserta una plantilla de varios contenedores en vRealize Automation, se crea una plantilla como un blueprint de varios componentes en vRealize Automation.

El blueprint de vRealize Automation reconoce las propiedades específicas de contenedor que agrega a la plantilla de contenedor. Consulte [Usar propiedades de contenedor y grupos de propiedades en un blueprint](#).

Cuando solicita el aprovisionamiento de un blueprint publicado en el catálogo de vRealize Automation, se aprovisiona la aplicación de contenedor de origen de ese blueprint.

Puede añadir otros componentes al blueprint de vRealize Automation, incluidos los siguientes tipos de componente:

- Tipos de máquina
- Componentes de software
- Otros blueprints
- Componentes de red y de seguridad de NSX
- Componentes de XaaS
- Componentes personalizados

Puede insertar una plantilla de Contenedores en vRealize Automation. Los cambios que realice al blueprint de vRealize Automation no afectan a la plantilla de Contenedores.

Puede aplicar cambios adicionales en la plantilla de Contenedores e insertarla de nuevo para sobrescribir el blueprint de vRealize Automation. El blueprint se sobrescribe al insertar la plantilla en vRealize Automation, y se perderá cualquier cambio realizado en el blueprint de vRealize Automation entre las inserciones. Para evitar perder los cambios de un blueprint, use vRealize CloudClient para clonar un nuevo blueprint o para exportar el blueprint.

Aprovisionar un host o un contenedor Docker a partir de un blueprint

Puede crear y utilizar blueprints de vRealize Automation para aprovisionar máquinas como hosts de contenedores Docker registrados.

Las máquinas aprovisionadas deben cumplir con los siguientes requisitos para poder registrarlas como hosts de contenedores:

- Un blueprint que contiene propiedades personalizadas específicas de Contenedores aprovisiona la máquina.

Las propiedades personalizadas específicas del contenedor que se requieren se suministran en dos grupos de propiedades. Consulte [Usar propiedades de contenedor y grupos de propiedades en un blueprint](#).

Para obtener información sobre la utilización de propiedades personalizadas y grupos de propiedades en vRealize Automation, consulte *Referencia de propiedades personalizadas*.

- La máquina es accesible por la red.

Por ejemplo, la máquina debe tener una dirección IP válida y debe estar encendida.

Puede definir un blueprint de vRealize Automation para que contenga propiedades personalizadas específicas que establezcan una máquina como un host de contenedores cuando se aprovisiona mediante un blueprint.

Cuando se aprovisiona correctamente una máquina con las propiedades de blueprint requeridas, esta se registra en Contenedores, y recibe eventos y acciones de vRealize Automation.

Crear blueprints de Microsoft Azure e incorporar acciones personalizadas

Como administrador de nube o tejido, puede crear blueprints de máquina virtual de Microsoft Azure que los administradores de grupo empresarial podrán usar para crear máquinas aprovisionadas personalizadas para consumidores. Los administradores de DevOps (desarrollo y operaciones) también pueden crear blueprints de máquina de Azure, o bien usar blueprints de máquina de Azure existentes cuando creen blueprints compuestos.

- [Crear un blueprint para Microsoft Azure](#)

Puede crear blueprints de máquinas virtuales de Microsoft Azure que proporcionen acceso a recursos de máquinas virtuales de Azure.

- [Crear acciones personalizadas de Azure](#)

Puede crear y utilizar acciones personalizadas para controlar máquinas virtuales de Azure.

Crear un blueprint para Microsoft Azure

Puede crear blueprints de máquinas virtuales de Microsoft Azure que proporcionen acceso a recursos de máquinas virtuales de Azure.

Se muestra una plantilla predeterminada Máquina de Azure en la categoría **Tipos de máquina** de la página Editar blueprint de vRealize Automation. Puede utilizar esta plantilla de máquina virtual como base de un blueprint de Azure como se describe en el siguiente procedimiento. Después de crear un blueprint de Azure, puede publicarlo e implementarlo tal como lo ha diseñado, o bien puede utilizarlo junto con recursos de Azure personalizados o con otros blueprints para crear un blueprint compuesto.

Después de crear y publicar el blueprint, los usuarios con los privilegios adecuados pueden solicitar y aprovisionar una instancia de Azure a través del catálogo de servicios de vRealize Automation.

Recuerde que los blueprints de Azure definen requisitos de máquinas virtuales. vRealize Automation usa estos requisitos para seleccionar la reserva más adecuada para la implementación.

Para obtener información sobre las pestañas Propiedades y Configuración de NSX en el cuadro de diálogo Nuevo blueprint, consulte *Configuración de vRealize Automation*.

Si desea crear dos máquinas virtuales a partir de una única implementación de manera simultánea, debe crear dos nombres de interfaz de red y dos nombres de máquina virtual.

Nota Evite el aprovisionamiento de una implementación en Azure y vSphere con el mismo prefijo de nombre, ya que esto puede provocar nombres duplicados en Azure y vSphere; a su vez, esto puede causar problemas para algunos usuarios.

Requisitos previos

- Obtenga un identificador de suscripción a Azure válido y la información relacionada (incluida la información del grupo de recursos, la cuenta de almacenamiento y la red virtual) que podría necesitar para crear un blueprint.
- Configure un endpoint de Azure para crear una conexión con Azure para su uso con la implementación de vRealize Automation.
- Configure reservas de Azure según corresponda para sus grupos empresariales.

Procedimiento

1 Seleccione **Diseño > Blueprints**.

2 Haga clic en el icono **Nuevo** (+).

3 Escriba un nombre de blueprint en el cuadro de texto **Nombre**.

El cuadro de texto **ID** también se rellenará con el nombre que escriba. En la mayoría de los casos, puede ignorar las pestañas **Configuración de NSX** y **Propiedades**.

4 Haga clic en **Aceptar**.

5 Haga clic en **Tipos de máquina** en el menú Categorías.

6 Arrastre la plantilla de máquina virtual **Máquina Azure** al lienzo de diseño.

Si ha creado un recurso de Azure personalizado para utilizarlo como base de un blueprint, puede seleccionar ese recurso desde la categoría asignada en la lista Categorías.

- 7 Especifique la información necesaria para la máquina virtual de Azure en los cuadros de texto de las páginas con pestañas ubicadas en la mitad inferior del lienzo de diseño que se muestran al arrastrar la plantilla Máquina Azure al lienzo de diseño.

Las selecciones disponibles para los cuadros de texto y otros parámetros de todas estas pestañas están determinadas principalmente por el endpoint de Azure que se ha configurado como una base para blueprints.

Para la mayoría de parámetros, cuando hace clic en el cuadro de texto junto al nombre de parámetro, se abre un panel nuevo en el lado derecho de la página. En este panel puede introducir los valores de los parámetros en el cuadro de texto **Valor** e indicar si es obligatorio en **Obligatorio**. Tenga en cuenta que en algunos casos también puede especificar los valores mínimos y máximos en **Valor mínimo** y **Valor máximo**. Haga clic en **Aplicar** en el panel derecho para rellenar el cuadro de texto inicial.

Figura 3-1. Menú del lado derecho del blueprint de Azure

The screenshot shows the configuration interface for an Azure Machine blueprint. The 'Storage' tab is selected. Under 'Resource Group', the 'Use Existing' radio button is chosen, and the 'Resource Group Name' is 'RG1-vAficionado'. Under 'Availability Set', the 'None' radio button is chosen. A red arrow indicates that the value from the 'Resource Group Name' field is being used in the 'Value' field of the right-hand panel. The 'Required' dropdown is set to 'No'.

La mayoría de los parámetros también cuentan con un botón **Opciones avanzadas**. Estas opciones le permiten especificar longitudes de parámetro e incluso ocultar parámetros de los usuarios finales.

Nota Debe rellenar los parámetros que se requieren en cada pestaña para poder continuar con la configuración del blueprint. Si quiere dejar un campo en blanco, puede regresar y eliminar la entrada antes de guardar.

Pestaña	Descripción	Parámetros importantes
General	Seleccione información de conexión básica de la máquina virtual de Azure, como el endpoint que se usará.	<p>ID: permite identificar la máquina virtual de Azure que se está creando. Si cambia este nombre, también se actualizará de forma automática la imagen de la máquina virtual de Azure en el lienzo de diseño.</p> <p>Descripción: permite identificar la máquina virtual que se está creando y determinar si es obligatoria.</p> <p>Instancias: esta selección le permite crear una máquina virtual escalable. Use los campos Mínimo y Máximo para identificar el número de instancias de Azure que se pueden generar a partir de esta máquina.</p> <p>Usar autenticación de contraseñas: seleccione Sí para usar autenticación de contraseñas o No para usar SSH.</p> <p>Nombre de usuario del administrador: deje este campo en blanco para que lo asigne el usuario que aprovisiona la máquina.</p> <p>Contraseña de administrador: deje este campo en blanco para que la persona que aprovisiona la máquina suministre la contraseña adecuada.</p>
Información de creación	Le permite configurar información sobre la máquina virtual que se está creando.	<p>Ubicación: seleccione el lugar geográfico en el que se implementará la máquina virtual.</p> <p>Prefijo de máquina: seleccione el botón de opción apropiado para indicar si desea utilizar el prefijo de máquina del grupo empresarial asociado o crear un prefijo personalizado. Si desea utilizar un prefijo personalizado, escríbalo en el cuadro de texto Prefijo de máquina personalizado.</p> <p>Tipo de imagen de máquina virtual: seleccione el botón de opción apropiado para una imagen de máquina virtual de los tipos Personalizada o Estándar. Una máquina virtual personalizada se crea a partir de la implementación clásica de Azure y ofrece más opciones de configuración en cuanto a servicios de nube, cuentas de almacenamiento y conjuntos de disponibilidad.</p> <p>Imagen de la máquina virtual: identifique la imagen de máquina virtual de Azure en la cual se basará el blueprint.</p> <ul style="list-style-type: none"> ■ Para una imagen de máquina virtual estándar, el URN de la imagen de máquina debe tener el siguiente formato: (publicador):(oferta):(sku):(versión). ■ Para una imagen de máquina virtual personalizada, el URN de imagen de la máquina debe tener el siguiente formato: <code>https://storageaccount.blob.core.windows.net/container/image.vhd</code> <p>También se debe completar el cuadro de texto Tipo de imagen de SO (Windows o Linux) para imágenes personalizadas.</p> <p>Usuario administrador: escriba el nombre del usuario administrador designado que se ha configurado para las máquinas virtuales basadas en este blueprint. Opcionalmente, este campo puede dejarse en blanco y la información puede introducirse en el formulario de solicitud.</p>

Pestaña	Descripción	Parámetros importantes
		<p>Autenticación: seleccione el botón de opción apropiado para indicar si las máquinas virtuales basadas en este blueprint requieren autenticación SSH o con contraseña.</p> <p>Contraseña de admin: contraseña de administrador de la instancia de máquina virtual.</p> <p>Serie: define el tamaño general de una instancia de máquina virtual. Consulte la documentación de Azure en https://azure.microsoft.com/es-es/documentation/articles/virtual-machines-windows-sizes/ para obtener información acerca de las series.</p> <p>Tamaño: define el tamaño de una instancia de máquina virtual específica dentro de una serie. El tamaño está relacionado con la serie seleccionada. Si cuenta con una conexión válida a una instancia de Azure, los tamaños disponibles se rellenan de manera dinámica en función de la suscripción y de la ubicación y la serie seleccionadas. Consulte la documentación de Azure para obtener información acerca del tamaño.</p> <p>Detalles de tamaño de instancia: información opcional del tamaño y la serie de la instancia de máquina virtual.</p>

Pestaña	Descripción	Parámetros importantes
Recursos de máquinas	<p>Organice los recursos de la máquina virtual en cubos. Un grupo de recursos es una construcción organizativa que agrupa recursos de máquinas virtuales como sitios web, cuentas, bases de datos y redes.</p> <p>Un conjunto de disponibilidad en un mecanismo para administrar dos o más máquinas virtuales y admitir redundancia. Consulte https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-manage-availability/ para obtener más información acerca de los conjuntos de disponibilidad de Azure.</p> <hr/> <p>Nota Si configura un blueprint de manera que el número máximo de instancias de Azure se establezca como un valor mayor que 1, entonces deberá utilizar el grupo de recursos y el conjunto de disponibilidad existentes en lugar de crear nuevos valores. Al utilizar nuevos grupos de recursos o nuevos conjuntos de disponibilidad en más de una instancia de la misma implementación, se producirán errores y otros problemas si se asocian con equilibradores de carga.</p>	<p>Crear o reutilizar grupo de recursos: seleccione el botón de opción apropiado para indicar si desea utilizar el grupo de recursos de Azure existente o crear uno nuevo. Puede encontrar el nombre del grupo de recursos existente en la página Grupos de recursos del portal de Azure. Si decide crear un nuevo grupo de recursos, en el cuadro de texto Grupo de recursos se muestra automáticamente un nombre apropiado para el nuevo grupo.</p> <p>Crear o reutilizar conjunto de disponibilidad: seleccione el botón de opción apropiado en función de lo que desea hacer. Si selecciona Crear nuevo, en el cuadro de texto se mostrará la información apropiada para el nuevo conjunto de disponibilidad.</p>

Pestaña	Descripción	Parámetros importantes
Almacenamiento	Le permite organizar las cuentas de almacenamiento de Azure. Una cuenta de almacenamiento proporciona acceso a los diferentes tipos de almacenamientos de Azure, como blobs de Azure, tablas de cola y almacenamiento de archivos. Para la mayoría de blueprints, puede aceptar los valores predeterminados.	<p>Cuenta de almacenamiento: escriba el nombre de la cuenta de almacenamiento de la máquina virtual si corresponde. El disco del sistema operativo de la máquina virtual de Azure se implementa en esta cuenta de almacenamiento. Puede encontrar información del grupo de almacenamiento en el portal de Azure. Puede tener una o varias cuentas de almacenamiento.</p> <hr/> <p>Nota Los nombres de cuentas de almacenamiento con guiones bajos u otros caracteres especiales pueden causar errores.</p> <hr/> <p>Añadir almacenamiento para diagnósticos: active esta casilla de verificación si utiliza datos de diagnóstico con su instancia de Azure.</p> <p>Número de discos de almacenamiento: seleccione el número apropiado de discos de almacenamiento de datos que se utilizan con la máquina virtual. Podrá especificar hasta cuatro discos. Estos discos son adicionales al disco del sistema operativo que se especifica en el cuadro de texto Cuenta de almacenamiento.</p> <p>N.º de disco de almacenamiento</p> <ul style="list-style-type: none"> ■ Nombre de disco: nombre de identificación que se ha asignado al disco. ■ Tipo de disco: tipo de dispositivo de almacenamiento. ■ Tamaño de disco: espacio de almacenamiento. ■ Replicación: método de redundancia utilizado para la creación de copias de seguridad de discos. ■ Almacenamiento en caché de host: indica si las lecturas y las escrituras se almacenan en caché para aumentar el rendimiento.

Pestaña	Descripción	Parámetros importantes
Red	<p>Le permite seleccionar la red del blueprint de la máquina virtual. En la mayoría de blueprints, puede aceptar los valores predeterminados y el consumidor introducirá la información de red apropiada durante la implementación.</p> <p>Nota Solo puede crear una máquina virtual por interfaz, pero cada máquina virtual puede tener hasta cuatro interfaces.</p>	<p>Haga clic en la tabla para abrir un cuadro de diálogo a la derecha que contiene otra tabla editable con los siguientes campos.</p> <ul style="list-style-type: none"> ■ Nombre del equilibrador de carga: equilibrador de carga utilizado con la instancia de Azure. ■ Número de interfaces de red: seleccione el número de interfaces de red utilizadas con la instancia de Azure. El número de interfaces de red debe ser compatible con el tamaño de la máquina virtual que se ha definido en la pestaña de Almacenamiento. ■ Interfaz de red: seleccione la interfaz de red adecuada para el blueprint de la máquina virtual. Si introduce una red existente, puede ignorar todas las demás pestañas de red. Si introduce el nombre de interfaz de red que no existe, se creará una nueva interfaz con ese nombre y podrá usar las demás pestañas de Red para configurarla. ■ Prefijo del nombre de NIC: prefijo de la tarjeta de interfaz de red. ■ Tipo de dirección IP: indique si la máquina virtual utiliza una dirección IP estática o dinámica. ■ Configuración de redes: introduzca la configuración de redes adecuada. Se admiten los perfiles de red. Hay dos opciones, Especificar redes de Azure y Usar perfil de red, y los campos que siguen cambian en función de la opción seleccionada. <ul style="list-style-type: none"> ■ Las siguientes opciones están disponible si selecciona Especificar redes de Azure. Si deja estos cuadros de texto en blanco, se utilizan las construcciones de red predeterminadas en función de la información especificada en la reserva aplicable. <ul style="list-style-type: none"> ■ Nombre de vNet: nombre de la red virtual. ■ Nombre de subred: nombre del dominio de la subred de Azure. <p>Nota Puede establecer la dirección IP pública para Azure durante las operaciones de día 2.</p> <ul style="list-style-type: none"> ■ Si selecciona Usar perfil de red, la configuración de red se separa de las construcciones subyacentes de Azure y, en su lugar, se une al perfil de red de vRealize Automation. <ul style="list-style-type: none"> ■ Si deja el cuadro de texto Perfil de red en blanco, el par de vNet y subred predeterminado de Azure se resuelven con base en las reservas aplicables para las que se ha especificado un perfil de red. ■ Si introduce un perfil de red, entonces la vNet y la subred de Azure se resuelven con base en la reserva que coincide.
Propiedades	Permite añadir propiedades personalizadas al blueprint. Las propiedades personalizadas que se	Existen dos opciones para añadir propiedades personalizadas, las cuales se representan mediante dos pestañas en el cuadro de diálogo Propiedades.

Pestaña	Descripción	Parámetros importantes
	<p>aplican aquí se pueden reemplazar con propiedades asignadas posteriormente en la cadena de prioridad. Para obtener más información sobre el orden de prioridad de las propiedades personalizadas, consulte <i>Referencia de propiedades personalizadas</i>.</p>	<ul style="list-style-type: none"> ■ Grupos de propiedades: son grupos reutilizables que simplifican el proceso de adición de propiedades personalizadas. Existen cuatro opciones para seleccionar grupos de propiedades: <ul style="list-style-type: none"> ■ Añadir: permite añadir un grupo de propiedades disponibles al blueprint. ■ Subir/Bajar: permiten controlar la prioridad de los grupos de propiedades. El primer grupo tiene la mayor prioridad y sus propiedades personalizadas ocupan el primer puesto en el orden de prioridad. ■ Ver propiedades: permite ver las propiedades personalizadas en el grupo seleccionado. ■ Ver propiedades combinadas: si una propiedad personalizada se incluye en más de un grupo de propiedades, el valor del grupo de propiedades con la mayor prioridad ocupará el primer puesto en el orden de prioridad. Consulte estas propiedades combinadas para que le resulte más fácil asignar la prioridad a los grupos de propiedades. ■ Propiedades personalizadas: emplee esta pestaña para añadir propiedades personalizadas individuales. <ul style="list-style-type: none"> ■ Nuevo: permite añadir una propiedad personalizada individual al blueprint. ■ Nombre: escriba un nombre para identificar la propiedad. Para obtener una lista de las propiedades personalizadas y sus definiciones, consulte <i>Referencia de propiedades personalizadas</i>. ■ Valor: escriba un valor para la propiedad personalizada. ■ Cifrado: permite cifrar la propiedad. ■ Reemplazable: permite especificar que un usuario siguiente puede reemplazar el valor de propiedad. Por lo general, este usuario suele ser otro arquitecto, pero, si selecciona Mostrar en solicitud, los usuarios empresariales podrán ver y editar valores de propiedades cuando soliciten elementos del catálogo. ■ Mostrar en solicitud: si desea mostrar el nombre y el valor de la propiedad a los usuarios finales, puede seleccionar la opción para mostrar la propiedad en el formulario de solicitud cuando se solicite el aprovisionamiento de máquina. También debe seleccionar Reemplazable si desea que los usuarios proporcionen un valor.

- 8 Haga clic en **Finalizar** para guardar la configuración del blueprint y volver a la página Blueprints principal.

Pasos siguientes

Si ha configurado propiedades personalizadas en la reserva de Azure para admitir un túnel VPN, puede agregar componentes de software a los blueprints de Azure.

- 1 Seleccione **Componentes de software** en el menú Categorías. Los componentes de software que haya configurado en los blueprints de Azure aparecen en el panel inferior.
- 2 Seleccione Máquina virtual de Azure en los valores de lista desplegable del contenedor.
- 3 Seleccione el componente de software que desee y arrástrelo hasta la máquina virtual de Azure en el lienzo de diseño.
- 4 Si el componente de software requiere de algunas propiedades, introdúzcalas en los cuadros de texto de parámetro apropiados debajo del lienzo de diseño.
- 5 Haga clic en **Guardar**.

Si desea publicar el blueprint, selecciónelo en la página Blueprints principal y haga clic en **Publicar**. Los blueprints publicados están disponibles en la página Elementos del catálogo. De igual forma, un administrador de grupo empresarial o equivalente puede crear un blueprint compuesto a partir de este blueprint publicado.

Crear acciones personalizadas de Azure

Puede crear y utilizar acciones personalizadas para controlar máquinas virtuales de Azure.

La implementación de Azure de vRealize Automation se suministra con dos acciones personalizadas listas para usar:

- Iniciar máquina virtual
- Detener máquina virtual

Además, puede crear acciones personalizadas mediante flujos de trabajo a los que se pueda acceder mediante la biblioteca de vRealize Orchestrator disponible en la interfaz de vRealize Automation.

Puede trabajar con acciones personalizadas de Azure como lo haría con cualquier otra acción personalizada de XaaS en vRealize Automation. Consulte *Crear blueprints XaaS y acciones personalizadas* e *Integración de vRealize Orchestrator en vRealize Automation* de *Configuración de vRealize Automation* si desea más información sobre las acciones personalizadas de XaaS.

Requisitos previos

Configure un endpoint de Azure válido para su implementación de vRealize Automation.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Haga clic en **Nuevo**.
- 3 Acceda a **Orchestrator > Biblioteca > Azure** en la biblioteca de flujos de trabajo de vRealize Orchestrator.

- 4 Seleccione el flujo de trabajo y la carpeta deseados.
- 5 Configure la acción según sus necesidades, al igual que haría con cualquier otra acción personalizada de XaaS.

Crear blueprints de vSphere habilitados para Puppet

Puede crear blueprints de vSphere habilitados para Puppet que admitan la administración de configuración basada en Puppet de máquinas virtuales de vSphere.

La administración de configuración basada en Puppet suele hacer uso de funciones y entornos para definir y administrar la configuración de software. Tenga en cuenta que el significado de función y entorno en Puppet es distinto del usado en TI, más genérico.

Un endpoint establece una conexión con una implementación de Puppet Enterprise existente. Cuando el endpoint se crea, vRealize Automation recupera la lista de entornos y funciones asociados a las implementaciones especificadas. Estos entornos y funciones se pueden usar en situaciones de enlace temprano o enlace tardío al configurar un blueprint de máquina virtual habilitado para Puppet.

Nota Actualmente, los componentes de Puppet solo son compatibles con blueprints y máquinas virtuales de vSphere.

Agregar un componente de Puppet a un blueprint de vSphere

Es posible agregar un componente de administración para la configuración de Puppet a un blueprint de vSphere a fin de forzar la administración de máquinas virtuales de vSphere con un maestro de Puppet.

Al añadir un componente de Puppet a un blueprint de vSphere, se agrega un agente de Puppet a las máquinas virtuales que se hayan creado a partir de ese blueprint.

Al crear blueprints de vSphere habilitados para Puppet, debe elegir si desea crear una configuración de enlace anticipado o de enlace en tiempo de ejecución.

Con el enlace anticipado, los usuarios definen la configuración del entorno y la función de Puppet para todas las máquinas virtuales que están basadas en un blueprint particular cuando el componente de Puppet se agrega al blueprint. Esta configuración se mantiene estática durante el ciclo de vida del blueprint. Se ofrecen varias opciones para el enlace en tiempo de ejecución.

- Deje los cuadros de texto **Entorno de Puppet** y **Función Puppet** vacíos en el blueprint para que los usuarios proporcionen estas opciones en el momento de la solicitud.
- Especifique un **Entorno de Puppet** y deje vacío el cuadro **Función Puppet**. Los usuarios deben introducir la función en el momento de la solicitud.

Requisitos previos

Cree un blueprint de vSphere adecuado. Consulte [Configuración de los componentes de máquina de vSphere](#) para obtener más información.

Procedimiento

- 1 Seleccione **Diseño > Blueprints**.
- 2 Seleccione **Administración de configuración** en el menú Categorías de la página Diseño de los blueprints.
- 3 Seleccione el componente de Puppet y arrástrelo hasta el componente de vSphere en el lienzo de diseño.
- 4 Introduzca un **ID** y una **Descripción** para el componente de Puppet en la pestaña General en la parte inferior de la página.

El ID y la descripción son arbitrarios.

- 5 Haga clic en la pestaña Servidor.
- 6 Haga clic en el menú desplegable y seleccione el maestro de Puppet adecuado para el blueprint.
- 7 Seleccione la opción de **Entorno de Puppet** y **Función Puppet** que sea adecuada en cada caso si desea usar el enlace anticipado en este componente.

Para configurar el enlace anticipado, seleccione un entorno de Puppet y una función Puppet. Si desea crear un componente con enlace en tiempo de ejecución, seleccione **Entorno de Puppet** o deje los cuadros de texto **Entorno de Puppet** y **Función Puppet** vacíos, y active las casillas **Establecer en formulario de solicitud**.

Nota Las casillas **Establecer en formulario de solicitud** están vinculadas. Si selecciona una, la otra se selecciona automáticamente.

- 8 Haga clic en **Finalizar** para guardar la configuración del componente de Puppet y volver a la página principal Diseño del blueprint.

Añadir soporte para la conexión RDP a los blueprints de máquina de Windows

Si quiere que los administradores del catálogo permitan a los usuarios utilizar la acción Conectar mediante RDP en los blueprints de Windows, añada propiedades personalizadas de RDP al blueprint y haga referencia al archivo de RDP que el administrador del sistema haya preparado.

Nota Si el administrador de tejido crea un grupo de propiedades con las propiedades personalizadas necesarias y lo incluye en el blueprint, no es necesario que añada una a una las propiedades personalizadas al blueprint.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador de grupo empresarial**.
- Obtenga el nombre del archivo RDP personalizado que el administrador del sistema creó para usted. Consulte [Crear un archivo RDP personalizado para admitir conexiones RDP para máquinas aprovisionadas](#).

- Cree al menos un blueprint de máquina de Windows.

Procedimiento

- 1 Seleccione **Diseño > Blueprints**.
- 2 Seleccione el blueprint para actualizar y haga clic en **Editar**.
- 3 Seleccione el componente de máquina en el lienzo para editar los detalles.
- 4 Haga clic en la pestaña **Propiedades**.
- 5 Haga clic en la pestaña **Propiedades personalizadas**.
- 6 Configure la configuración RDP.
 - a Haga clic en **Nueva propiedad**.
 - b Escriba los nombres de propiedad personalizados de RDP en el cuadro de texto **Nombre** y los valores correspondientes en el cuadro de texto **Valor**.

Opción	Descripción y valor
VirtualMachine.Rdp.File	Especifica un archivo RDP del que se obtienen valores de configuración (por ejemplo, <code>My_RDP_Settings.rdp</code>). El archivo debe estar en el subdirectorio <code>Website\Rdp</code> del directorio de instalación de vRealize Automation.
VirtualMachine.Rdp.SettingN	Especifica la configuración de RDP que se va a usar al abrir un vínculo RDP en la máquina. <i>N</i> es un número único que sirve para distinguir una configuración de RDP de otra. Por ejemplo, para especificar un nivel de autenticación de RDP en el que no es necesario ningún requisito de autenticación, defina la propiedad personalizada <code>VirtualMachine.Rdp.Setting1</code> y establezca el valor en el nivel de autenticación <code>i:3</code> . Para obtener información sobre los ajustes de RDP disponibles y su sintaxis correcta, consulte la documentación de RDP de Microsoft Windows, como Configuración de RDP para los servicios de escritorio remoto de Windows Server .
VirtualMachine.Admin.NameCompletion	Especifica el nombre de dominio que se va a incluir en el nombre de dominio completo de la máquina que los archivos RDP o SSH generan en las opciones de interfaz de usuario Conectar mediante RDP o Conectar mediante SSH . Por ejemplo, establezca el valor en <code>miEmpresa.com</code> para generar el nombre de dominio completo <code>my-machine-name.myCompany.com</code> en el archivo RDP o SSH.

- c Haga clic en **Guardar**.
- 7 Seleccione la fila del blueprint y haga clic en **Publicar**.

Resultados

Los administradores del catálogo pueden permitir a los usuarios utilizar la acción **Conectar mediante RDP** en las máquinas aprovisionadas desde su blueprint. Si los usuarios no están autorizados a la acción, no podrán conectarse mediante RDP.

Añadir limpieza de Active Directory al blueprint CentOS

Como arquitecto de IaaS, desea configurar vRealize Automation para que limpie el entorno de Active Directory cuando se quiten máquinas aprovisionadas de los hipervisores. Por lo tanto, debe editar el blueprint para configurar el complemento de limpieza de Active Directory.

El complemento de limpieza de Active Directory le permite especificar que se ejecuten las siguientes acciones de cuenta de Active Directory cuando se elimine una máquina de un hipervisor:

- Eliminar la cuenta de AD
- Desactivar la cuenta de AD
- Cambiar el nombre de la cuenta de AD
- Mover la cuenta de AD a otra unidad organizativa (OU) de AD

Requisitos previos

Nota Esta información no se aplica a Amazon Web Services.

- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Recopile la siguiente información acerca del entorno de Active Directory:
 - Un nombre de usuario y una contraseña de cuenta de Active Directory con suficientes derechos para eliminar, desactivar, cambiar de nombre o mover cuentas de AD. El nombre de usuario debe tener el formato dominio\nombre de usuario.
 - (Opcional) El nombre de la OU a la que se trasladarán las máquinas destruidas.
 - (Opcional) El prefijo que se añadirá a las máquinas destruidas.
- Cree un blueprint de máquina. Consulte [Configurar un blueprint de máquina](#).

Procedimiento

- 1 Seleccione **Diseño > Blueprints**.
- 2 Señale un blueprint y haga clic en **Editar**.
- 3 Seleccione el componente de máquina en el lienzo para mostrar la pestaña Detalles.
- 4 Haga clic en la pestaña **Propiedades**.
- 5 Haga clic en la pestaña **Propiedades personalizadas** para configurar el complemento de limpieza de Active Directory.
 - a Haga clic en **Nueva propiedad**.
 - b Escriba `Plugin.AdMachineCleanup.Execute` en el cuadro de texto **Nombre**.
 - c Escriba `true` en el cuadro de texto **Valor**.
 - d Haga clic en el icono **Guardar** (✓).

- 6 Configure el complemento de limpieza de Active Directory añadiéndole propiedades personalizadas.

Opción	Descripción y valor
<code>Plugin.AdMachineCleanup.UserName</code>	Escriba el nombre de usuario de la cuenta de Active Directory en el cuadro de texto Valor . Este usuario debe tener privilegios suficientes para eliminar, desactivar, mover y cambiar el nombre de las cuentas de Active Directory. El nombre de usuario debe tener el formato dominio\nombre de usuario.
<code>Plugin.AdMachineCleanup.Password</code>	Escriba la contraseña de la cuenta de Active Directory en el cuadro de texto Valor .
<code>Plugin.AdMachineCleanup.Delete</code>	Establézcala en True para eliminar las cuentas de las máquinas destruidas, en lugar de deshabilitarlas.
<code>Plugin.AdMachineCleanup.MoveToOu</code>	Mueve la cuenta de las máquinas destruidas a una nueva unidad organizativa de Active Directory. El valor es la unidad organizativa a la que va a mover la cuenta. Este valor debe tener el formato <code>ou=OU, dc=dc</code> (por ejemplo, <code>ou=trash,cn=computers,dc=lab,dc=local</code>).
<code>Plugin.AdMachineCleanup.RenamePrefix</code>	Añade un prefijo para cambiar de nombre las cuentas de las máquinas destruidas. El valor es la cadena de prefijo que se antepone (por ejemplo, <code>destroyed_</code>).

- 7 Haga clic en **Aceptar**.

Resultados

Cuando se eliminan del hipervisor las máquinas aprovisionadas desde el blueprint, se actualiza el entorno de Active Directory.

Escenario: Permitir que los solicitantes especifiquen el nombre de host de la máquina

Como arquitecto de blueprint, debe permitir que los usuarios elijan los nombres de sus máquinas cuando soliciten sus blueprints. Por lo tanto, edita el blueprint vSphere de CentOS existente para añadir la propiedad personalizada del nombre del host y configurarlo para solicitar a los usuarios un valor durante sus solicitudes.

Nota Si el administrador de tejido crea un grupo de propiedades con las propiedades personalizadas necesarias y lo incluye en el blueprint, no es necesario que añada una a una las propiedades personalizadas al blueprint.

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Cree un blueprint de máquina. Consulte *Instalación y configuración de vRealize Automation para el escenario de Rainpole*.

Procedimiento

- 1 Seleccione **Diseño > Blueprints**.

- 2 Apunte al blueprint **Centos en vSphere** y haga clic en **Editar**.
- 3 Seleccione el componente de máquina en el lienzo para mostrar la pestaña de detalles.
- 4 Haga clic en la pestaña **Propiedades**.
- 5 Haga clic en **Nueva propiedad**.
- 6 Escriba **Hostname** en el cuadro de texto **Nombre**.
- 7 Deje el cuadro de texto **Valor** vacío.
- 8 Configure vRealize Automation para solicitar a los usuarios un valor de nombre del host durante la solicitud.
 - a Seleccione **Reemplazable**.
 - b Seleccione **Mostrar en solicitud**

Dado que los nombres de host deben ser únicos, los usuarios solo puede solicitar una máquina cada vez de este blueprint.
- 9 Haga clic en el icono **Guardar** (✓).
- 10 Haga clic en **Aceptar**.

Resultados

Los usuarios que soliciten una máquina de su blueprint deberán especificar un nombre del host para su máquina. vRealize Automation comprueba que el nombre del host especificado sea único.

Escenario: Permitir a los usuarios seleccionar ubicaciones de centros de datos para implementaciones entre regiones

Como arquitecto de blueprints, le interesa permitir a los usuarios que elijan si aprovisionarán las máquinas en la infraestructura de Boston o de Londres. Por este motivo, necesita editar el blueprint de CentOS de vSphere para habilitar la característica de ubicaciones.



Tiene un centro de datos en Londres y otro en Boston, y no quiere que los usuarios de Boston aprovisionen máquinas en la infraestructura de Londres y viceversa. Para asegurarse de que los usuarios de Boston aprovisionan en la infraestructura de Boston, y los usuarios de Londres aprovisionan en la infraestructura de Londres, le interesa permitir a los usuarios que seleccionen una ubicación adecuada para el aprovisionamiento cuando estos soliciten máquinas.

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Como administrador del sistema, defina las ubicaciones de los centros de datos. Consulte [Escenario: Añadir ubicaciones de centros de datos para implementaciones en varias regiones](#).
- Como administrador de tejidos, aplique las ubicaciones adecuadas a los recursos informáticos. Consulte [Escenario: Aplicar una ubicación a un recurso informático para implementaciones entre regiones](#).
- Cree un blueprint de máquina. Consulte *Instalación y configuración de vRealize Automation para el escenario de Rainpole*.

Procedimiento

- 1 Seleccione **Diseño > Blueprints**.
- 2 Apunte al blueprint **Centos en vSphere** y haga clic en **Editar**.
- 3 Seleccione el componente de máquina en el lienzo para mostrar la pestaña de detalles **General**.
- 4 Seleccione la casilla de verificación **Mostrar ubicación al solicitar**.
- 5 Haga clic en **Finalizar**.
- 6 Apunte al blueprint de **Centos en vSphere** y haga clic en **Publicar**.

Resultados

Ahora, cuando los usuarios del grupo empresarial soliciten una máquina para aprovisionarla desde el blueprint, se les pedirá que seleccionen una ubicación del centro de datos.

Diseñar componentes de Software

Como arquitecto de software, crea componentes de software reutilizables. Para ello, estandariza propiedades de configuración y usa scripts de acción para especificar exactamente el modo en que los componentes se instalan, se configuran, se desinstalan o se actualizan durante las operaciones de escalado de implementación. Puede describir estos scripts de acción en cualquier momento y publicarlos para insertar cambios en los componentes de software aprovisionados.

Si desea diseñar sus scripts de acción para que sean genéricos y puedan reutilizarse, defina y consuma pares de nombre y valor, denominados propiedades de software, y pase estas propiedades como parámetros a los scripts de acción. Si sus propiedades de software tienen valores desconocidos o necesitan definirse en el futuro, puede requerir o permitir que otros arquitectos de blueprints o usuarios finales proporcionen los valores. Si necesita un valor de otro componente en un blueprint, por ejemplo, la dirección IP de una máquina, puede enlazar la

propiedad de software a la propiedad de dirección IP de esa máquina. El uso de propiedades de software para parametrizar los scripts de acción hace posible convertir los scripts en genéricos y reutilizables. Esto permite implementar componentes de software en distintos entornos sin modificar los scripts.

Tabla 3-43. Acciones de ciclo de vida

Acciones de ciclo de vida	Descripción
Instalar	Instala el software. Por ejemplo, puede descargar bits de instalación del servidor Tomcat e instalar un servicio de Tomcat. Los scripts que escribe para la acción de ciclo de vida Instalar se ejecutan cuando se aprovisiona por primera vez el software, ya sea durante una solicitud de implementación inicial o como parte de un escalado horizontal.
Configurar	Configura el software. En el ejemplo de Tomcat, podría establecer JAVA_OPTS y CATALINA_OPTS. Los scripts de configuración se ejecutan después de que se haya completado la acción de instalación.
Iniciar	Inicia el software. Por ejemplo, puede iniciar el servicio de Tomcat mediante el comando start en el servidor Tomcat. Los scripts de inicio se ejecutan después de que se haya completado la acción de configuración.
Actualizar	Si diseña el componente de software para que admita blueprints que se puedan escalar, controla las actualizaciones necesarias después de una operación de escalado vertical o escalado horizontal. Por ejemplo, podría cambiar el tamaño de clúster en una implementación escalada y administrar los nodos en clúster mediante un equilibrador de carga. Diseñe sus scripts de actualización para que se ejecuten varias veces (idempotentes) y para que controlen los casos tanto de escalado vertical como de escalado horizontal. Cuando se realiza una operación de escalado, los scripts de actualización se ejecutan en todos los componentes de software dependientes.
desinstalar	Desinstala el software. Por ejemplo, podría realizar acciones específicas en la aplicación antes de destruir una implementación. Los scripts de desinstalación se ejecutan cuando se destruyen componentes de software.

Puede descargar componentes de Software predefinidos para una variedad de aplicaciones y servicios de middleware desde VMware Solution Exchange. Si utiliza la API de REST de vRealize CloudClient o vRealize Automation, podrá importar mediante programación los componentes de Software predefinidos en su instancia de vRealize Automation.

- Para visitar VMware Solution Exchange, consulte https://solutionexchange.vmware.com/store/category_groups/cloud-management.
- Para obtener información sobre la API de REST de vRealize Automation, consulte *Guía de programación* y *API del servicio de contenido de vRealize Automation* en <https://code.vmware.com>.
- Para obtener información sobre vRealize CloudClient, consulte <https://developercenter.vmware.com/tool/cloudclient>.

Tipos de propiedades y opciones de configuración

Si desea diseñar sus scripts de acción para que sean genéricos y puedan reutilizarse, defina y consuma pares de nombre y valor, denominados propiedades de software, y pase estas

propiedades como parámetros a los scripts de acción. Puede crear propiedades de software que esperen valores de tipo cadena, matriz, contenido, booleano o entero. Puede proporcionar el valor usted mismo, solicitar a otra persona que lo proporcione o recuperarlo de otro componente de blueprint mediante la creación de un enlace.

Opciones de propiedades

Puede computar el valor de cualquier propiedad de cadena seleccionando la casilla de verificación computada y puede convertir cualquier propiedad en cifrada, reemplazable o necesaria seleccionando las casillas de verificación adecuadas cuando configure las propiedades de Software. Combine estas opciones con sus valores para lograr diferentes propósitos. Por ejemplo, desea solicitar a los arquitectos de blueprints que proporcionen un valor para una contraseña y que lo cifren cuando usen el componente de software en un blueprint. Cree la propiedad de contraseña, pero deje el cuadro de texto del valor en blanco. Seleccione Reemplazable, Obligatorio y Cifrado. Si la contraseña que espera pertenece a su usuario final, el arquitecto de blueprints puede seleccionar **Mostrar en solicitud** para requerir que los usuarios escriban la contraseña cuando rellenen el formulario de solicitud.

Opción	Descripción
Cifrado	Marque las propiedades como cifradas para enmascarar el valor y mostrarlo como una serie de asteriscos en vRealize Automation. Si cambia una propiedad de cifrada a no cifrada, vRealize Automation restablecerá el valor de la propiedad. Por seguridad, debe definir un nuevo valor para la propiedad.
Reemplazable	Requiere que los arquitectos editen el valor de la propiedad al ensamblar blueprints de aplicación. Si especifica un valor, se mostrará como valor predeterminado.
Obligatorio	Permite que los arquitectos editen el valor de la propiedad al ensamblar blueprints de aplicación.
Computada	Los valores de las propiedades computadas se asignan mediante los scripts de ciclo de vida de INSTALACIÓN, CONFIGURACIÓN, INICIO o ACTUALIZACIÓN. Los valores asignados se propagan a las etapas del ciclo de vida posteriores y a componentes que se vinculan a esas propiedades en un blueprint. Si se selecciona Computada para una propiedad que no es una propiedad de cadena, el tipo de propiedad se cambia a cadena.

Si selecciona la opción de propiedad computada, deje en blanco el valor de su propiedad personalizada. Diseñe sus scripts para los valores computados.

Tabla 3-44. Ejemplos de scripts para la opción de propiedad computada

Ejemplo de propiedad de cadena	Sintaxis del script	Ejemplo de uso
my_unique_id = ""	Bash - \$my_unique_id	export my_unique_id="0123456789"
	Símbolo del sistema de Windows - %my_unique_id%	set my_unique_id=0123456789
	Windows PowerShell - \$my_unique_id	\$my_unique_id = "0123456789"

Propiedad de cadena

Las propiedades de cadena esperan valores de cadena. Puede proporcionar la cadena usted mismo, solicitar a otra persona que proporcione el valor o recuperarlo de otro componente de blueprint mediante la creación de un enlace a otra propiedad de cadena. Los valores de cadena pueden contener cualquier carácter ASCII. Para crear un enlace de propiedad, utilice la pestaña **Propiedades** del lienzo de diseño para seleccionar la propiedad adecuada para enlazar. A continuación, el valor de la propiedad se transferirá a los scripts de acción como datos de cadena sin procesar. Cuando cree un enlace a una propiedad de cadena de blueprint, asegúrese de que el componente de blueprint al que se enlaza no pueda agruparse en un clúster. Si el componente está en un clúster, el valor de cadena se convierte en una matriz y no se recupera el valor esperado.

Ejemplo de propiedad de cadena	Sintaxis de script	Ejemplo de uso
admin_email = "admin@email987.com"	Bash - \$admin_email	echo \$admin_email
	Símbolo del sistema de Windows - %admin_email%	echo %admin_email%
	Windows PowerShell - \$admin_email	write-output \$admin_email

Propiedad de matriz

Las propiedades de matriz esperan una matriz de valores de tipo cadena, entero, decimal o booleano definidos como ["value1", "value2", "value3"...]. Puede proporcionar los valores usted mismo, solicitar a otra persona que los proporcione o recuperarlos de otro componente de blueprint mediante la creación de un enlace de propiedad.

Cuando se crea una propiedad de software de tipo matriz, donde el tipo de datos es entero o decimal, debe usar un punto y coma como separador elemento de matriz, independientemente de la configuración regional. No utilice una coma (,) o un punto (.). Para algunas configuraciones regionales, puede utilizar una coma (,) como separador decimal. Por ejemplo:

- Una matriz válida en francés tendría el siguiente aspecto: [1,11 2,22; 3,33]

- Una matriz válida en inglés tendría el siguiente aspecto: [1.11,2.22,3.33]

Al pasar grandes cantidades a una matriz, no utilice el formato de agrupación. Por ejemplo: no utilice **4444 444.000** (francés), **4.444.444,000** (italiano) o **4,444,444.000** (inglés), ya que los archivos de datos que contienen los formatos específicos de la configuración regional se podrían malinterpretar cuando se transfieran a un equipo que tenga una configuración regional diferente. No se permite el formato de agrupación, porque un número como **4,444,444.000** se consideraría como tres números diferentes. En su lugar, escriba **4444444.000**.

Al definir los valores de una propiedad de matriz, debe incluir la matriz entre corchetes. En una matriz de cadenas, el valor de los elementos de la matriz puede contener cualquier carácter ASCII. Para cifrar correctamente un carácter de barra inversa en un valor de propiedad de matriz, añada una barra inversa adicional, como en este ejemplo: ["c:\\test1\\test2"]. Para una propiedad enlazada, utilice la pestaña **Propiedades** del lienzo de diseño para seleccionar la propiedad correspondiente para enlazar. Si enlaza a una matriz, debe diseñar los componentes de software para que no esperen una matriz de valores en un orden concreto.

Por ejemplo, piense en una máquina virtual de equilibrador de carga que equilibra la carga para un clúster de máquinas virtuales de servidor de aplicaciones. En tal caso, se define una propiedad de matriz para el servicio del equilibrador de carga y se establece en la matriz de direcciones IP de las máquinas virtuales del servidor de aplicaciones.

Estos scripts de configuración del servicio del equilibrador de carga utilizan la propiedad de matriz para configurar el esquema de equilibrado de carga adecuado en sistemas operativos Red Hat, Windows y Ubuntu.

Ejemplo de propiedad de matriz	Sintaxis de script	Ejemplo de uso
operating_systems = ["Red Hat","Windows","Ubuntu"]	Bash - \${operating_systems[@]} para toda la matriz de cadenas \${operating_systems[N]} para un elemento de matriz individual	for ((i = 0 ; i < \$ {#operating_systems[@]}; i++)); do echo \${operating_systems[i]} done
	Símbolo del sistema de Windows - %operating_systems_% donde <i>N</i> representa la posición del elemento en la matriz	for /F "delims== tokens=2" %A in ('set operating_systems_') do (echo %A)
	Windows PowerShell - \$operating_systems para toda la matriz de cadenas \$operating_systems[N] para un elemento de matriz individual	foreach (\$os in \$operating_systems){ write-output \$os }

Propiedad de contenido

El valor de una propiedad de contenido es una URL a un archivo para descargar contenido. El agente de Software descarga el contenido de la URL en la máquina virtual y transfiere la ubicación del archivo local en la máquina virtual al script.

Las propiedades de contenido deben definirse como una URL válida con el protocolo HTTP o HTTPS. Por ejemplo, el componente Software del servidor de aplicaciones JBOSS de la aplicación de muestra de Dukes Bank especifica una propiedad de contenido `cheetah_tgz_url`. Los artefactos se alojan en el dispositivo de Software y la dirección URL apunta a esa ubicación en el dispositivo. El agente de Software descarga los artefactos de la ubicación especificada en la máquina virtual implementada.

Para obtener información sobre los valores de configuración de `software.http.proxy` que puede usar con las propiedades de contenido, consulte *Referencia de propiedades personalizadas*.

Ejemplo de propiedad de cadena	Sintaxis de script	Ejemplo de uso
<code>cheetah_tgz_url = "http:// app_content_server_ip:port/artifacts/ software/jboss/cheetah-2.4.4.tar.gz"</code>	Bash - <code>\$cheetah_tgz_url</code>	<code>tar -zxvf \$cheetah_tgz_url</code>
	Símbolo del sistema de Windows - <code>%cheetah_tgz_url%</code>	<code>start /wait c:\unzip.exe %cheetah_tgz_url%</code>
	Windows PowerShell - <code>\$cheetah_tgz_url</code>	<code>& c:\unzip.exe \$cheetah_tgz_url</code>

Propiedad booleana

Use el tipo de propiedad booleana para proporcionar opciones de True y False en el menú desplegable Valor.

Propiedad de valor entero

Use el tipo de propiedad de valor entero para los ceros, o los enteros positivos o negativos.

Propiedad decimal

Use el tipo de propiedad decimal para los valores que representan fracciones decimales que no se repiten.

Si su componente de Software necesita información de otro componente

En varios escenarios de implementación, un componente necesita el valor de propiedad de otro componente para personalizarse a sí mismo. Para ello, se pueden crear enlaces de propiedad con vRealize Automation. Aunque puede diseñar sus propios scripts de acción de Software para enlaces de propiedad, el arquitecto que ensambla el blueprint es quien debe configurar los enlaces reales.

Además de establecer una propiedad en un valor codificado de forma rígida, un arquitecto de software, un arquitecto de IaaS o un arquitecto de aplicaciones puede enlazar propiedades de componentes de Software a otras propiedades del blueprint, como una dirección IP o una ubicación de instalación. Cuando se enlaza una propiedad de Software a otra propiedad, puede personalizar un script basado en el valor de otra propiedad de componente o de máquina virtual. Por ejemplo, un componente WAR podría necesitar la ubicación de instalación del servidor Apache Tomcat. En sus scripts, podrá configurar el componente WAR para establecer el valor de

la propiedad `server_home` en el valor de la propiedad `install_path` del servidor Apache Tomcat de su script. Siempre y cuando el arquitecto que ensambla el blueprint enlace la propiedad `server_home` a la propiedad `install_path` del servidor Apache Tomcat, el valor de la propiedad `server_home` se establecerá correctamente.

En sus scripts de acción solo puede usar las propiedades que defina en tales scripts, y solo puede crear enlaces de propiedad con valores de cadena y de matriz. Las matrices de propiedades de blueprint no se devuelven en ningún orden específico, de modo que el enlace a componentes que puedan escalarse o agruparse en un clúster podría no producir los valores previstos. Por ejemplo, su componente de software requiere todos los identificadores de máquina de un clúster de máquinas, y permite que los usuarios soliciten un clúster de 1 a 10 y que escalen la implementación de 1 a 10 máquinas. Si configura su propiedad de software como un tipo de cadena, obtiene un identificador de máquina seleccionado de forma aleatoria del clúster. Si configura su propiedad de software como un tipo de matriz, obtiene una matriz de todos los identificadores de máquina del clúster, pero sin ningún orden concreto. Si sus usuarios escalan la implementación, el orden de los valores podría ser distinto en cada operación. Para asegurarse de nunca perder los valores de los componentes en clúster, puede usar el tipo de matriz en cualquier propiedad de software. Sin embargo, debe diseñar los componentes de software para que no esperen una matriz de valores en un orden concreto.

Consulte la tabla Ejemplos de enlaces de propiedad de cadena para obtener ejemplos de un valor de propiedad de una cadena cuando se enlazan los diferentes tipos de propiedades.

Tabla 3-45. Ejemplos de enlaces de propiedad de cadena

Ejemplo de tipo de propiedad	Tipo de propiedad que enlazar	Resultado de enlace (A se enlaza a B)
Cadena (propiedad A)	Cadena (propiedad B="Hi")	A="Hi"
Cadena (propiedad A)	Contenido (propiedad B="http://my.com/content")	A="http://my.com/content"
Cadena (propiedad A)	Matriz (propiedad B=["1","2"])	A=["1","2"]
Cadena (propiedad A)	Computada (propiedad B="Hello")	A="Hello"

Consulte la tabla Ejemplos de enlaces de propiedad de matriz para obtener ejemplos de un valor de propiedad de matriz cuando se enlazan los diferentes tipos de propiedades.

Tabla 3-46. Ejemplos de enlaces de propiedad de matriz

Ejemplo de tipo de propiedad	Tipo de propiedad que enlazar	Resultado de enlace (A se enlaza a B)
Matriz (propiedad A)	Cadena (propiedad B="Hi")	A="Hi"
Matriz (propiedad A)	Contenido (propiedad B="http://my.com/content")	A="http://my.com/content"
Matriz (propiedad A)	Computada (propiedad B="Hello")	A="Hello"

Consulte [Tipos de propiedades y opciones de configuración](#) para obtener una explicación detallada de los tipos de propiedad compatibles.

Transferir valores de propiedad entre etapas del ciclo de vida

Puede modificar y transferir valores de propiedad entre etapas del ciclo de vida mediante scripts de acción.

Para una propiedad computada, puede modificar el valor de la propiedad y transferirlo a la siguiente etapa del ciclo de vida del script de acción. Por ejemplo, si el componente A tiene el valor `progress_status` definido como `staged`, en las etapas de **INSTALACIÓN** y **CONFIGURACIÓN** del ciclo de vida debe cambiar el valor a `progress_status=installed` en los scripts de acción respectivos. Si el componente B está enlazado al componente A, los valores de propiedad de `progress_status` en las etapas del ciclo de vida del script de acción serán iguales que en el componente A.

Defina en el componente de software que el componente B depende del A. Esta dependencia define la transferencia de valores de propiedad correctos entre componentes tanto si están en el mismo nodo como en nodos distintos.

Por ejemplo, puede actualizar un valor de propiedad en un script de acción utilizando los scripts compatibles.

- Bash `progress_status="completed"`
- Símbolo del sistema de Windows `set progress_status=completed`
- Windows PowerShell `$progress_status="completed"`

Nota Las propiedades de matriz y de contenido no permiten transferir valores de propiedad modificados entre scripts de acción de etapas del ciclo de vida.

Recomendaciones para desarrollar componentes

Para familiarizarse con las recomendaciones para definir propiedades y scripts de acción, puede descargar e importar componentes de Software y blueprints de aplicación desde VMware Solution Exchange.

Siga estas prácticas recomendadas cuando desarrolle componentes de Software.

- Para que un script se ejecute sin interrupciones, el valor de retorno debe definirse en cero (0). Este valor permite al agente recopilar todas las propiedades y enviarlas al servidor de Software.
- Es posible que algunos instaladores necesiten acceder a la consola `tty`. Redirija la entrada desde `/dev/console`. Por ejemplo, un componente de Software de RabbitMQ podría utilizar el comando `./rabbitmq_rhel.py --setup-rabbitmq < /dev/console` en su script de instalación.
- Si un componente usa varias etapas del ciclo de vida, el valor de la propiedad se puede cambiar en la etapa de **INSTALACIÓN** del ciclo de vida. El nuevo valor se envía a la siguiente etapa del ciclo de vida. Los scripts de acción pueden calcular el valor de una propiedad durante la implementación para proporcionar el valor a otros scripts dependientes. Por ejemplo, en la aplicación de muestra Clustered Dukes Bank, el servicio JBossAppServer

calcula la propiedad JVM_ROUTE durante la etapa de instalación del ciclo de vida. El servicio JBossAppServer utiliza esta propiedad para configurar el ciclo de vida. A continuación, el servicio del equilibrador de carga Apache enlaza su propiedad JVM_ROUTE a la propiedad (appserver:JBossAppServer:JVM_ROUTE) para obtener el valor calculado definitivo de node0 y node1. Si un componente requiere un valor de propiedad de otro componente para completar correctamente una implementación de la aplicación, debe indicar dependencias explícitas en el blueprint de la aplicación.

Nota No es posible cambiar el valor de la propiedad de contenido por un componente que use varias etapas del ciclo de vida.

Crear un componente de Software

Configure y publique un componente de Software que pueda ser utilizado por otros arquitectos de software, arquitectos de IaaS y arquitectos de aplicaciones para ensamblar los blueprints de la aplicación.

Requisitos previos

Inicie sesión en vRealize Automation como **arquitecto de software**.

Procedimiento

- 1 Seleccione **Diseño > Componentes de software**.
- 2 Haga clic en el icono **Añadir** (+).
- 3 Especifique un nombre y, opcionalmente, una descripción.

Con el nombre que ha especificado para el componente de Software, vRealize Automation crea un identificador para el componente de Software único en el tenant. Si desea editar este campo, hágalo ahora, pues en cuanto guarde el blueprint ya no podrá cambiarlo. Dado que los identificadores son permanentes y únicos en el tenant, puede usarlos para interactuar con los blueprints mediante programación y para crear enlaces de propiedades.

- 4 (opcional) Si desea controlar el modo en que el componente de Software se incluye en los blueprints, seleccione un tipo de contenedor en el menú desplegable **Contenedor**.

Opción	Descripción
Máquinas	El componente de Software debe colocarse directamente en una máquina.
Uno de los componentes de Software publicados	Si va a diseñar un componente de Software específicamente para instalarlo sobre otro componente de Software que haya creado, seleccione el componente de Software de la lista. Por ejemplo, si va a diseñar un componente de EAR para instalarlo sobre el componente de JBOSS creado anteriormente, seleccione el componente de JBOSS en la lista.
Componentes de software	Si va a diseñar un componente de Software que no debe instalarse directamente en una máquina, pero que se puede instalar en varios componentes de Software, seleccione la opción de componentes de software. Por ejemplo, si va a diseñar un componente de WAR y desea instalarlo en el componente de Software de Tomcat Server y el componente de Software de Tcserver, seleccione el tipo de contenedor de componentes de software.

- 5 Haga clic en **Siguiente**.

- 6 Defina las propiedades que quiera usar en sus scripts de acción.

- Haga clic en el icono **Añadir** (+).
- Escriba un nombre para la propiedad.
- Escriba una descripción para la propiedad.

Esta descripción se muestra a los arquitectos que usan el componente de Software en los blueprints.

- Seleccione el tipo esperado para el valor de la propiedad.
- Defina el valor de la propiedad.

Opción	Descripción
Usar el valor que proporciona ahora	<ul style="list-style-type: none"> ■ Escriba un valor. ■ Anule la selección de Reemplazable. ■ Seleccione Obligatorio.
Exigir a los arquitectos que proporcionen un valor	<ul style="list-style-type: none"> ■ Para proporcionar un valor predeterminado, escriba un valor. ■ Seleccione Reemplazable. ■ Seleccione Obligatorio.
Permitir a los arquitectos proporcionar un valor si lo prefieren	<ul style="list-style-type: none"> ■ Para proporcionar un valor predeterminado, escriba un valor. ■ Seleccione Reemplazable. ■ Anule la selección de Obligatorio.

Los arquitectos pueden configurar las propiedades de Software para mostrárselas a los usuarios en el formulario de solicitud. Los arquitectos pueden usar la opción Mostrar en solicitud para requerir o solicitar que los usuarios proporcionen valores para las propiedades que marque como reemplazables.

- 7 Siga las indicaciones para proporcionar un script para al menos una de las acciones de ciclo de vida del software.

Tabla 3-47. Acciones de ciclo de vida

Acciones de ciclo de vida	Descripción
Instalar	Instala el software. Por ejemplo, puede descargar bits de instalación del servidor Tomcat e instalar un servicio de Tomcat. Los scripts que escribe para la acción de ciclo de vida Instalar se ejecutan cuando se aprovisiona por primera vez el software, ya sea durante una solicitud de implementación inicial o como parte de un escalado horizontal.
Configurar	Configura el software. En el ejemplo de Tomcat, podría establecer JAVA_OPTS y CATALINA_OPTS. Los scripts de configuración se ejecutan después de que se haya completado la acción de instalación.
Iniciar	Inicia el software. Por ejemplo, puede iniciar el servicio de Tomcat mediante el comando start en el servidor Tomcat. Los scripts de inicio se ejecutan después de que se haya completado la acción de configuración.
Actualizar	Si diseña el componente de software para que admita blueprints que se puedan escalar, controla las actualizaciones necesarias después de una operación de escalado vertical o escalado horizontal. Por ejemplo, podría cambiar el tamaño de clúster en una implementación escalada y administrar los nodos en clúster mediante un equilibrador de carga. Diseñe sus scripts de actualización para que se ejecuten varias veces (idempotentes) y para que controlen los casos tanto de escalado vertical como de escalado horizontal. Cuando se realiza una operación de escalado, los scripts de actualización se ejecutan en todos los componentes de software dependientes.
desinstalar	Desinstala el software. Por ejemplo, podría realizar acciones específicas en la aplicación antes de destruir una implementación. Los scripts de desinstalación se ejecutan cuando se destruyen componentes de software.

Incluya códigos de salida y de estado en sus scripts de acción. Cada tipo de script admitido tiene unos requisitos únicos de código de salida y de estado.

Tipo de script	Estado correcto	Estado de error	Comandos no admitidos
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	Ninguno
Símbolo del sistema de Windows	exit /b 0	exit /b non-zero	No use los códigos exit 0 o exit non-zero.
PowerShell	exit 0	exit non-zero;	No use las llamadas warning, verbose, debug o host.

- 8 Marque la casilla de verificación **Reiniciar** para cualquier script que requiera que reinicie la máquina.

Después de ejecutarse el script, la máquina se reinicia antes de iniciar el siguiente script del ciclo de vida.

- 9 Haga clic en **Finalizar**.

- 10 Seleccione el componente de Software y haga clic en **Publicar**.

Resultados

Ha configurado y publicado un componente de Software. Ahora, otros arquitectos de software, arquitectos de IaaS y arquitectos de aplicaciones pueden usar este componente de Software para añadir software a blueprints de aplicaciones.

Pasos siguientes

Añada su componente de Software publicado a un blueprint de aplicación. Consulte [Ensamblar blueprints compuestos](#).

Configuración de los componentes de Software

Configure los ajustes generales, cree propiedades y cree scripts de acción personalizados para instalar, configurar, actualizar o desinstalar el componente de Software en máquinas aprovisionadas.

Como arquitecto de software, haga clic en **Diseño > Componentes de software** y haga clic en el icono **Agregar** para crear un nuevo componente de Software.

Configuración general del nuevo Software

Aplique la configuración general al componente de Software.

Tabla 3-48. Configuración general del nuevo Software

Configuración	Descripción
Nombre	Escriba un nombre para el componente de Software..
ID	Con el nombre que ha especificado para el componente de Software, vRealize Automation crea un identificador para el componente de Software único en el tenant. Si desea editar este campo, hágalo ahora, pues en cuanto guarde el blueprint ya no podrá cambiarlo. Dado que los identificadores son permanentes y únicos en el tenant, puede usarlos para interactuar con los blueprints mediante programación y para crear enlaces de propiedades.

Tabla 3-48. Configuración general del nuevo Software (continuación)

Configuración	Descripción
Descripción	Incluya un resumen del componente de Software para proporcionar información a otros arquitectos.
Contenedor	<p>En el lienzo de diseño, los arquitectos de blueprints solo pueden colocar el componente de Software en el tipo de contenedor que usted seleccione.</p> <ul style="list-style-type: none"> ■ Seleccione Máquinas para que los arquitectos coloquen el componente de Software directamente en un componente de máquina en el lienzo de diseño. ■ Seleccione Componentes de software si está diseñando un componente de Software que nunca debería colocarse directamente en un componente de máquina, pero que puede anidarse en alguno de los distintos componentes de Software. ■ Seleccione un componente de Software publicado concreto si está diseñando un componente de Software específicamente para anidarlo en otro componente de Software que haya creado. ■ Seleccione Máquina virtual de Azure si va a diseñar un componente de Software específicamente para un blueprint de Azure.

Propiedades de nuevo Software

Las propiedades de componente de Software se usan para parametrizar scripts con el objetivo de transferir las propiedades definidas como variables de entorno a scripts en ejecución en una máquina. Antes de ejecutar los scripts, el agente de Software de la máquina aprovisionada se comunica con vRealize Automation para resolver las propiedades. A continuación, el agente crea las variables específicas del script a partir de estas propiedades y las transfiere a los scripts.

Tabla 3-49. Propiedades de nuevo Software

Configuración	Descripción
Nombre	Escriba un nombre para la propiedad de Software. Los nombres de las propiedades distinguen entre mayúsculas y minúsculas, y solo pueden contener caracteres alfanuméricos, guiones (-) o guiones bajos (_).
Descripción	Incluya un resumen de la propiedad y los requisitos del valor para proporcionar información a otros usuarios.
Tipo	Software admite los tipos cadena, matriz, booleano y entero. Consulte Tipos de propiedades y opciones de configuración para obtener una explicación detallada de los tipos de propiedad compatibles. Para obtener información sobre los enlaces de propiedad, consulte Si su componente de Software necesita información de otro componente y Crear enlaces de propiedad entre componentes de blueprint .

Tabla 3-49. Propiedades de nuevo Software (continuación)

Configuración	Descripción
Valor	<ul style="list-style-type: none"> ■ Para usar el valor que usted proporciona: <ul style="list-style-type: none"> ■ Escriba un Valor. ■ Seleccione Obligatorio. ■ Anule la selección de Reemplazable. ■ Para exigir a los arquitectos que proporcionen un valor: <ul style="list-style-type: none"> ■ (Opcional) Escriba un Valor para proporcionar una opción predeterminada. ■ Seleccione Reemplazable. ■ Seleccione Obligatorio. ■ Para permitir a los arquitectos que proporcionen un valor o que dejen el valor en blanco: <ul style="list-style-type: none"> ■ (Opcional) Escriba un Valor para proporcionar una opción predeterminada. ■ Seleccione Reemplazable. ■ Anule la selección de Obligatorio.
Cifrado	<p>Marque las propiedades como cifradas para enmascarar el valor y mostrarlo como una serie de asteriscos en vRealize Automation. Si cambia una propiedad de cifrada a no cifrada, vRealize Automation restablecerá el valor de la propiedad. Por seguridad, debe definir un nuevo valor para la propiedad.</p> <p>Importante Si las propiedades protegidas se imprimen en el script mediante el comando echo u otros comandos similares, estos valores aparecen como texto sin formato en los archivos log. Los valores de los archivos log no se enmascaran.</p>
Reemplazable	Requiere que los arquitectos editen el valor de la propiedad al ensamblar blueprints de aplicación. Si especifica un valor, se mostrará como valor predeterminado.
Obligatorio	Permite que los arquitectos editen el valor de la propiedad al ensamblar blueprints de aplicación.
Computada	Los valores de las propiedades computadas se asignan mediante los scripts de ciclo de vida de INSTALACIÓN, CONFIGURACIÓN, INICIO o ACTUALIZACIÓN. Los valores asignados se propagan a las etapas del ciclo de vida posteriores y a componentes que se vinculan a esas propiedades en un blueprint. Si se selecciona Computada para una propiedad que no es una propiedad de cadena, el tipo de propiedad se cambia a cadena.

Acciones del nuevo Software

Los scripts de acción de Bash, símbolo del sistema de Windows o PowerShell se crean para especificar exactamente la manera en la que los componentes se instalan, configuran, actualizan o desinstalan durante las operaciones de escalado de implementación.

Tabla 3-50. Acciones de ciclo de vida

Acciones de ciclo de vida	Descripción
Instalar	Instala el software. Por ejemplo, puede descargar bits de instalación del servidor Tomcat e instalar un servicio de Tomcat. Los scripts que escribe para la acción de ciclo de vida Instalar se ejecutan cuando se aprovisiona por primera vez el software, ya sea durante una solicitud de implementación inicial o como parte de un escalado horizontal.
Configurar	Configura el software. En el ejemplo de Tomcat, podría establecer JAVA_OPTS y CATALINA_OPTS. Los scripts de configuración se ejecutan después de que se haya completado la acción de instalación.
Iniciar	Inicia el software. Por ejemplo, puede iniciar el servicio de Tomcat mediante el comando start en el servidor Tomcat. Los scripts de inicio se ejecutan después de que se haya completado la acción de configuración.
Actualizar	Si diseña el componente de software para que admita blueprints que se puedan escalar, controla las actualizaciones necesarias después de una operación de escalado vertical o escalado horizontal. Por ejemplo, podría cambiar el tamaño de clúster en una implementación escalada y administrar los nodos en clúster mediante un equilibrador de carga. Diseñe sus scripts de actualización para que se ejecuten varias veces (idempotentes) y para que controlen los casos tanto de escalado vertical como de escalado horizontal. Cuando se realiza una operación de escalado, los scripts de actualización se ejecutan en todos los componentes de software dependientes.
desinstalar	Desinstala el software. Por ejemplo, podría realizar acciones específicas en la aplicación antes de destruir una implementación. Los scripts de desinstalación se ejecutan cuando se destruyen componentes de software.

Marque la casilla de verificación **Reiniciar** para cualquier script que requiera que reinicie la máquina. Después de ejecutarse el script, la máquina se reinicia antes de iniciar el siguiente script del ciclo de vida. Asegúrese de que no haya ningún proceso que requiera la interacción del usuario cuando se esté ejecutando el script. Las interrupciones detienen el script, lo que provoca que permanezca en un estado inactivo de manera indefinida y que, finalmente, se produzca un error. Además, los scripts deben incluir códigos de salida adecuados que puedan aplicarse a la implementación de aplicación. Si el script no tiene códigos de salida y retorno, el último comando que se ejecutó en el script se convierte en el estado de salida. Los códigos de salida y de retorno son distintos en los diversos tipos de scripts admitidos: Bash, símbolo del sistema de Windows y PowerShell.

Tipo de script	Estado correcto	Estado de error	Comandos no admitidos
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	Ninguno
Símbolo del sistema de Windows	exit /b 0	exit /b non-zero	No use los códigos exit 0 o exit non-zero.
PowerShell	exit 0	exit non-zero;	No use las llamadas warning, verbose, debug o host.

Diseñar acciones personalizadas y blueprints XaaS

Los blueprints de XaaS se pueden publicar como elementos del catálogo, o se pueden usar en el lienzo de diseño de blueprints. Las acciones personalizadas son acciones que se ejecutan en elementos implementados.

XaaS usa vRealize Orchestrator para ejecutar flujos de trabajo que aprovisionan elementos o para ejecutar acciones. Por ejemplo, puede configurar los flujos de trabajo para crear máquinas virtuales de vSphere o usuarios de Active Directory en grupos, o bien para ejecutar scripts de PowerShell. Si crea un flujo de trabajo personalizado de vRealize Orchestrator, puede proporcionar dicho flujo de trabajo como un elemento en el catálogo del servicio, lo que permite a los usuarios autorizados ejecutar el flujo de trabajo.

Puede usar un blueprint XaaS como componente en un blueprint que haya creado en el lienzo de diseño, o bien publicarlo directamente en el catálogo de servicios.

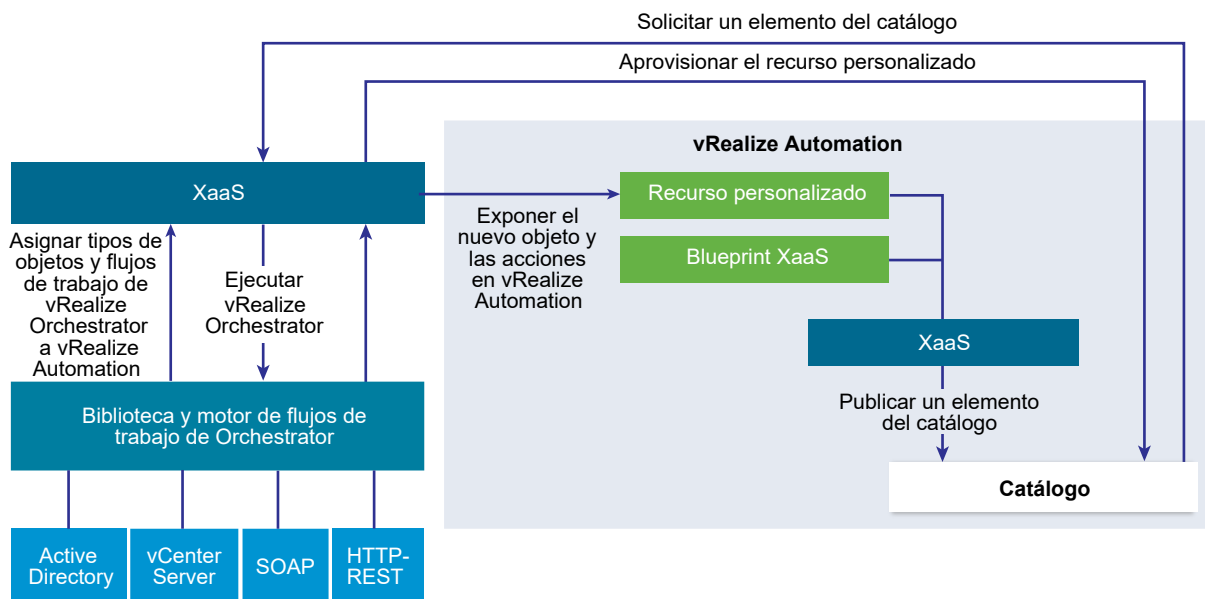
Si utiliza un blueprint como componente de otro blueprint, puede configurarlo de modo que se escale cuando aplique al blueprint implementado un escalado vertical u horizontal.

Integración de vRealize Orchestrator en vRealize Automation

vRealize Orchestrator es el motor de flujos de trabajo integrado en vRealize Automation.

El servidor de vRealize Orchestrator distribuido con vRealize Automation está preconfigurado y, por lo tanto, cuando el administrador del sistema implementa el dispositivo de vRealize Automation, el servidor de vRealize Orchestrator está listo y en ejecución.

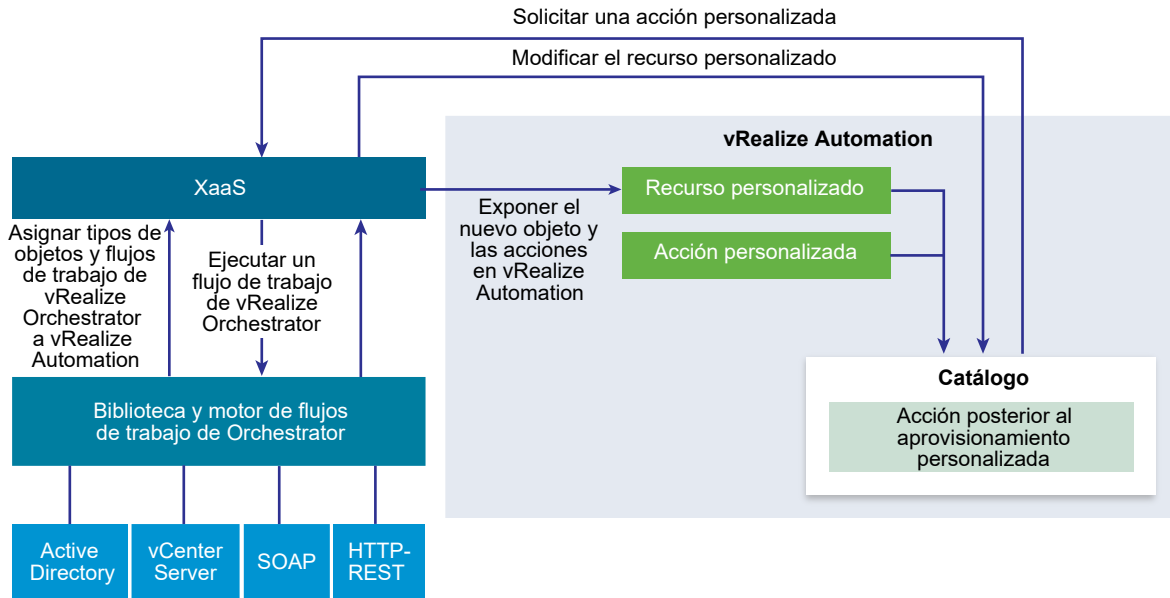
Figura 3-2. Crear y solicitar elementos del catálogo incluidos en XaaS para aprovisionar un recurso personalizado



Los arquitectos de XaaS añaden recursos personalizados relacionados con los endpoints compatibles y los flujos de trabajo proporcionados, y después crean blueprints y acciones XaaS basándose en esos recursos. Los administradores de tenant y de grupos empresariales pueden añadir los blueprints y las acciones XaaS al catálogo de servicios. El blueprint XaaS también se puede usar en el diseñador de blueprints.

Cuando el usuario del catálogo de servicios solicita un elemento, vRealize Automation ejecuta un flujo de trabajo de vRealize Orchestrator para aprovisionar el recurso personalizado.

Figura 3-3. Crear y solicitar acciones personalizadas para modificar un recurso personalizado



Los arquitectos de XaaS también pueden añadir flujos de trabajo de vRealize Orchestrator como acciones personalizadas para ampliar las funciones de vRealize Automation. Después de aprovisionar un recurso personalizado, los usuarios del catálogo de servicios pueden ejecutar la acción posterior al aprovisionamiento. De esta forma, los consumidores ejecutan un flujo de trabajo de vRealize Orchestrator y modifican el recurso personalizado aprovisionado.

Cuando un usuario del catálogo de servicios solicita un blueprint o una acción personalizada XaaS como elemento del catálogo, el servicio XaaS ejecuta el flujo de trabajo de vRealize Orchestrator correspondiente y pasa los siguientes datos como parámetros globales al flujo de trabajo:

Tabla 3-51. Parámetros globales de XaaS

Parámetro	Descripción
__asd_tenantRef	El tenant del usuario que solicita el flujo de trabajo.
__asd_subtenantRef	El grupo empresarial del usuario que solicita el flujo de trabajo.
__asd_catalogRequestId	El ID de solicitud del catálogo para esta ejecución del flujo de trabajo.

Tabla 3-51. Parámetros globales de XaaS (continuación)

Parámetro	Descripción
__asd_requestedFor	El usuario de destino de la solicitud. Si la solicitud se realiza en nombre de un usuario, esto corresponde al usuario en nombre del cual se solicita el flujo de trabajo; de lo contrario, es el usuario que lo solicita.
__asd_requestedBy	El usuario que solicita el flujo de trabajo.

Si un blueprint o una acción personalizada XaaS usan un flujo de trabajo de vRealize Orchestrator que contiene un elemento de esquema de interacción del usuario, cuando un consumidor solicita el servicio, se suspende la ejecución del flujo de trabajo y se espera a que el usuario proporcione los datos requeridos. Para responder a una interacción del usuario en espera, el usuario debe ir a **Bandeja de entrada > Acción de usuario manual**.

El inventario del servidor de vRealize Orchestrator predeterminado se comparte entre todos los tenants y no se puede usar según el tenant. Por ejemplo, si un arquitecto de servicio crea un blueprint de servicio para crear un recurso informático de clúster, los consumidores de diferentes tenants deben examinar los elementos del inventario de todas las instancias de vCenter Server aunque pertenezcan a un tenant distinto.

Los administradores del sistema pueden instalar vRealize Orchestrator o implementar el vRealize Orchestrator Appliance por separado para configurar una instancia de vRealize Orchestrator externa y configurar vRealize Automation para que funcione con esa instancia de vRealize Orchestrator externa.

Además, los administradores del sistema pueden también configurar categorías de flujo de trabajo de vRealize Orchestrator según el tenant y definir qué flujos de trabajo están disponibles para cada tenant.

Por último, los administradores de tenant también pueden configurar una instancia de vRealize Orchestrator externa, pero solamente para sus propios tenants.

Para obtener información sobre cómo configurar una instancia de vRealize Orchestrator externa y categorías de flujo de trabajo de vRealize Orchestrator, consulte *Configuración de vCenter Orchestrator y complementos*.

Lista de complementos de vRealize Orchestrator

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

Puede utilizar el conjunto de complementos de vRealize Orchestrator estándar para incorporar en los flujos de trabajo tecnologías externas tales como la API de vCenter Server y funciones de correo electrónico. Además, puede utilizar la arquitectura abierta de complementos de vRealize Orchestrator para desarrollar complementos que le permitan acceder a otras aplicaciones.

Tabla 3-52. Complementos incluidos de forma predeterminada en vRealize Orchestrator

Complemento	Propósito
vCenter Server	Proporciona acceso a la API de vCenter Server para que pueda incorporar todos los objetos de funciones de vCenter Server en los procesos de administración que automatice mediante vRealize Orchestrator.
Configuración	Proporciona flujos de trabajo para configurar la autenticación de vRealize Orchestrator, la conexión de base de datos, los certificados SSL, etc.
Biblioteca de vCO	Proporciona flujos de trabajo que actúan como bloques de creación básicos para personalizar y automatizar procesos de cliente. La biblioteca de flujos de trabajo incluye plantillas para procesos de administración de ciclo de vida, aprovisionamiento, recuperación ante desastres, copia de seguridad en caliente y otros procesos estándar. Puede copiar y editar las plantillas para modificarlas según sus necesidades.
SQL	Proporciona la API JDBC (Java Database Connectivity), que es la norma en el sector relativa a la conectividad independiente de base de datos entre el lenguaje de programación Java y una amplia gama de bases de datos. Pueden ser bases de datos SQL y otras fuentes de datos tabulares, como hojas de cálculo o archivos sin formato. La API JDBC proporciona una API de nivel de llamada que permite el acceso a bases de datos basadas en SQL desde los flujos de trabajo.
SSH	Proporciona una implementación del protocolo Secure Shell v2 (SSH-2). Permite las sesiones remotas de transferencia de archivos y comandos con autenticación basada en contraseña y clave pública en los flujos de trabajo. Admite la autenticación con teclado interactivo. Opcionalmente, el complemento SSH puede proporcionar la exploración remota del sistema de archivos directamente en el inventario de cliente de vRealize Orchestrator.
XML	Un completo analizador XML DOM (Document Object Model) que se puede implementar en los flujos de trabajo. Alternativamente, se puede usar la implementación ECMAScript for XML (E4X) en la API JavaScript de vRealize Orchestrator.
Correo	Utiliza el Protocolo simple de transferencia de correo (SMTP) para enviar correo electrónico desde los flujos de trabajo.
Red	Contiene la biblioteca Jakarta Apache Commons Net. Proporciona implementaciones de Telnet, FTP, POP3 e IMAP. La parte POP3 e IMAP se utiliza para leer correo electrónico. Si se utiliza el complemento Red en combinación con el complemento Correo, se proporcionan funciones completas de envío y recepción de correo electrónico en los flujos de trabajo.
Enumeración	Proporciona tipos enumerados comunes que otros complementos pueden usar en los flujos de trabajo.

Tabla 3-52. Complementos incluidos de forma predeterminada en vRealize Orchestrator (continuación)

Complemento	Propósito
Documentación de flujo de trabajo	Proporciona flujos de trabajo que permiten generar información en formato PDF acerca de un flujo de trabajo o una categoría de flujo de trabajo.
HTTP-REST	Permite administrar servicios web REST, ya que proporciona interacción entre vCenter Orchestrator y los hosts de REST.
SOAP	Permite administrar servicios web SOAP, ya que proporciona interacción entre vCenter Orchestrator y los hosts de SOAP.
AMQP	Permite la interacción con servidores AMQP (Advanced Message Queuing Protocol), también denominados agentes.
SNMP	Permite la conexión de vCenter Orchestrator a sistemas y dispositivos compatibles con SNMP para recibir información.
Active Directory	Proporciona interacción entre vCenter Orchestrator y Microsoft Active Directory.
vCO WebOperator	Una vista web que permite acceder a los flujos de trabajo de la biblioteca de vRealize Orchestrator e interactuar con ellos en una red, a través de un navegador web.
Tipos dinámicos	Permite definir tipos dinámicos, y crear y utilizar objetos de dichos tipos dinámicos.
PowerShell	Permite administrar hosts de PowerShell y ejecutar operaciones personalizadas de PowerShell.
Multinodo	Contiene flujos de trabajos para la orquestación jerárquica, la administración de instancias de Orchestrator y el escalado de actividades de Orchestrator.
vRealize Automation	Permite crear y ejecutar flujos de trabajo para la interacción entre vRealize Orchestrator y vRealize Automation.

Para obtener más información acerca de los complementos de vRealize Orchestrator que implementa y distribuye VMware, consulte la página de inicio de la documentación de VMware vRealize™ Orchestrator™.

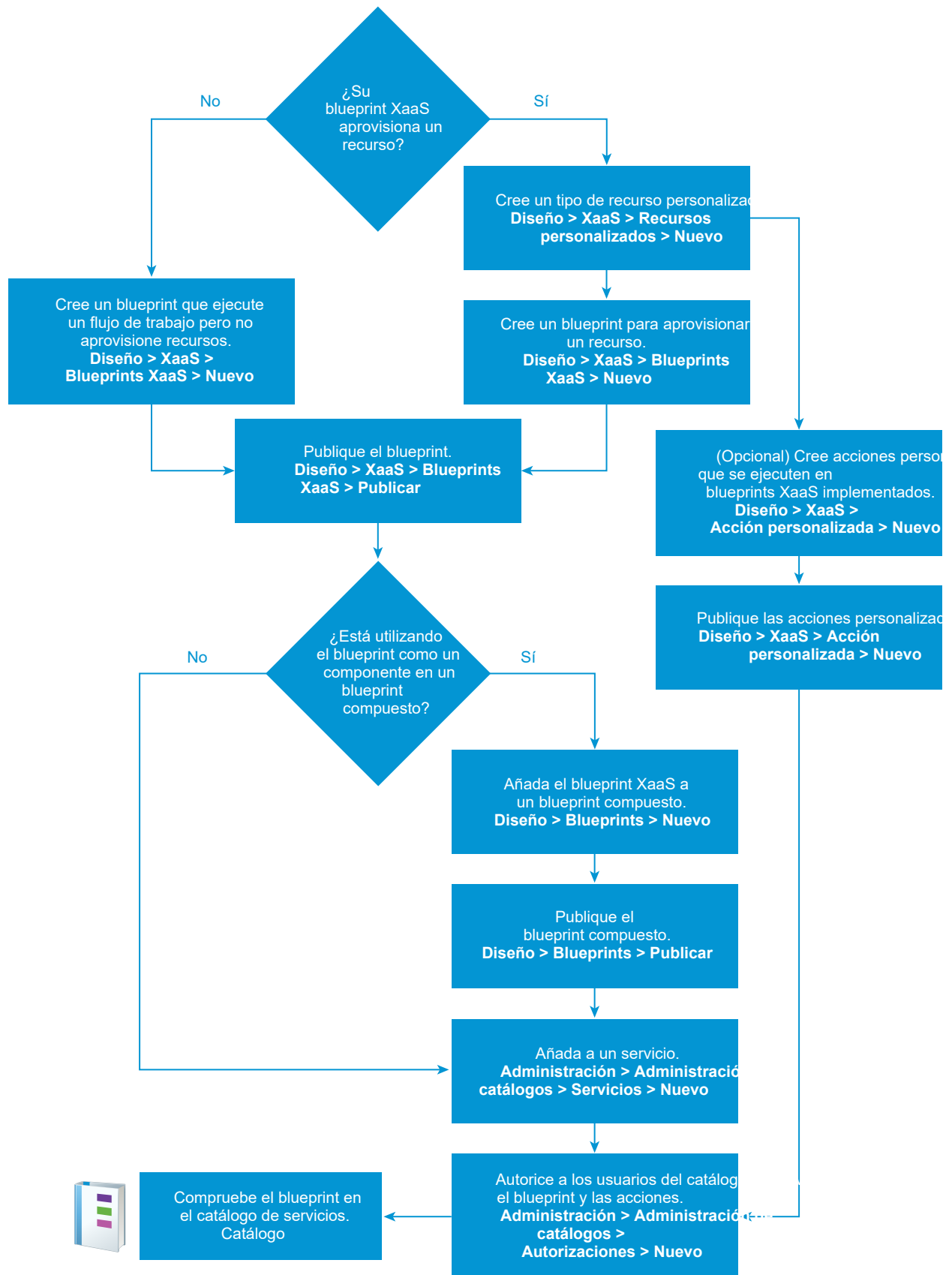
Crear blueprints de XaaS y acciones personalizadas

Los blueprints de XaaS se pueden autorizar a usuarios como elementos del catálogo o se pueden ensamblar en un blueprint compuesto mediante el lienzo de diseño. Las acciones personalizadas se ejecutan en los elementos aprovisionados para administrar los elementos después de aprovisionarlos.

Por ejemplo, puede usar un blueprint de XaaS para crear usuarios de Active Directory en un grupo. Después, puede usar una acción personalizada para que el usuario cambie la contraseña.

Flujo de trabajo de blueprint XaaS

El flujo de trabajo que se sigue para crear un blueprint XaaS y cualquier acción personalizada opcional varía según la manera en la que pretende usar el blueprint. El siguiente flujo de trabajo proporciona el proceso básico.



Terminología de blueprint XaaS

Los blueprints XaaS son flujos de trabajo de vRealize Orchestrator que pueden aprovisionar recursos, hacer cambios en los recursos aprovisionados o comportarse como un servicio que realiza una tarea en el entorno. Los blueprints y las acciones personalizadas tienen varios matices que debe comprender cuando diseña blueprints para los usuarios del catálogo de servicios.

Las siguientes definiciones le permiten comprender los términos utilizados al trabajar con blueprints XaaS.

Recurso personalizado

Un tipo de objeto de vRealize Orchestrator que se expone como recurso mediante la API de un complemento de vRealize Orchestrator. El recurso personalizado se crea para definir el parámetro de salida de un blueprint de aprovisionamiento XaaS, así como para definir un parámetro de entrada de una acción personalizada.

Componente de blueprint XaaS

Un blueprint de aprovisionamiento o de no aprovisionamiento que se puede utilizar en el lienzo de diseño del blueprint. Este blueprint también puede ser un blueprint XaaS independiente.

Blueprint XaaS independiente

Un blueprint de aprovisionamiento o de no aprovisionamiento que se publica y se autoriza directamente en el catálogo de servicios.

Blueprint de aprovisionamiento

Blueprint de aprovisionamiento que ejecuta un flujo de trabajo de vRealize Orchestrator para aprovisionar recursos en el endpoint de destino utilizando la API del complemento de vRealize Orchestrator del endpoint. Por ejemplo, añadir NIC virtuales a un dispositivo de red en vSphere. Para crear un blueprint de aprovisionamiento, debe contar con un recurso personalizado que defina el tipo de recurso de vRealize Orchestrator.

Cuando un usuario del catálogo de servicios solicita este tipo de elementos del catálogo, el flujo de trabajo aprovisiona el elemento y el elemento implementado se almacena en la pestaña **Elementos**. Puede definir operaciones posteriores al aprovisionamiento para este tipo de recursos aprovisionados. También puede añadir o quitar instancias cuando sea necesario para hacer que los blueprints sean escalables.

Blueprint de no aprovisionamiento

Un blueprint de no aprovisionamiento ejecuta un flujo de trabajo de vRealize Orchestrator para realizar una tarea que no requiera la API para hacer cambios en un endpoint. Por ejemplo, el flujo de trabajo que se ejecuta genera un informe y lo envía por correo electrónico a un sistema de comunicación de destino o lo publica en él.

Cuando un usuario del catálogo de servicios solicita este tipo de elemento del catálogo, el flujo de trabajo se ejecuta para llevar a cabo la tarea generada por script, pero el elemento no se añade a la pestaña **Elementos**. En este tipo de blueprint no se pueden llevar a cabo

operaciones posteriores al aprovisionamiento. Puede utilizar blueprints de no aprovisionamiento como flujos de trabajo de apoyo en blueprints escalables. Por ejemplo, puede crear un blueprint para actualizar un equilibrador de carga de alta disponibilidad.

Blueprint compuesto

Un blueprint que se crea utilizando el lienzo de diseño. El blueprint compuesto utiliza uno o varios componentes. Por ejemplo, un componente de máquina, un componente de software o un componente XaaS. Cuando se añade a un servicio, se muestra como una implementación. Cuando se añade a una autorización para ponerlo a disposición de los usuarios del catálogo de servicios, se muestra como blueprint compuesto. Un blueprint compuesto puede tener un componente de blueprint, o bien puede incluir una aplicación completa con varias máquinas, software y redes.

Acción personalizada

Un flujo de trabajo que se puede ejecutar en un blueprint de aprovisionamiento implementado. El blueprint implementado puede ser un blueprint XaaS o un componente de blueprint, o bien puede ser un tipo de máquina asignado a un tipo de recurso de vRealize Orchestrator.

Consideraciones de diseño de blueprints XaaS

Antes de crear un blueprint XaaS, debe conocer el propósito del blueprint de manera que pueda diseñar uno que aprovisiones los recursos de forma correcta.

Puede crear y utilizar blueprints XaaS como un componente de blueprint en el lienzo de diseño o como un blueprint independiente. El blueprint puede ser un blueprint de aprovisionamiento o de no aprovisionamiento.

Tabla 3-53. Resultados y tipos de blueprint XaaS

Tipo de blueprint XaaS	¿Es obligatorio utilizar un recurso personalizado?	¿Es el blueprint escalable en una implementación?	¿Se puede ejecutar una acción personalizada en el blueprint implementado?
Componente de blueprint que aprovisiona recursos	Sí.	Sí. Si está configurado para el escalado, escalará junto con la implementación.	Sí. Escala junto con la implementación y puede ejecutar otras acciones personalizadas en el componente implementado. El componente de blueprint se muestra en la pestaña Elementos.
Componente de blueprint que ejecuta un flujo de trabajo, pero no aprovisiona recursos	No. El blueprint utiliza la configuración del servidor de vRealize Orchestrator, pero no requiere un recurso personalizado XaaS.	No. No aprovisiona recursos, pero puede ejecutarse como parte de una operación de escalado. Por ejemplo, actualice un equilibrador de carga con la nueva configuración basada en la operación de escalado.	No. No puede ejecutar una acción personalizada en un componente de no aprovisionamiento.
Blueprint independiente que aprovisiona recursos	Sí.	No. Debe crear acciones personalizadas para añadir o destruir instancias.	Sí. Puede ejecutar acciones personalizadas en el recurso implementado, incluida cualquier acción creada para admitir el escalado. El blueprint se muestra en la pestaña Elementos.
Blueprint independiente que ejecuta un flujo de trabajo, pero no aprovisiona recursos	No. El blueprint utiliza la configuración del servidor de vRealize Orchestrator, pero no requiere un recurso personalizado XaaS.	No. No aprovisiona recursos, pero puede ejecutarse como parte de una acción personalizada.	No. No puede ejecutar una acción personalizada en un componente de no aprovisionamiento.

Añadir un recurso personalizado de XaaS

Puede crear un recurso personalizado para definir el elemento de XaaS para el aprovisionamiento. Antes de crear una acción o un blueprint XaaS, debe contar con un recurso personalizado compatible con el tipo de objeto del flujo de trabajo del blueprint o la acción.

Al crear un recurso personalizado, se asigna un tipo de objeto expuesto mediante la API de un complemento de vRealize Orchestrator como un recurso. El recurso personalizado define el parámetro de salida de un blueprint XaaS para aprovisionar y definir un parámetro de entrada de una acción personalizada.

Si un flujo de trabajo de un blueprint o una acción personalizada no aprovisiona un recurso ni se ejecuta en un blueprint implementado, no es necesario que cree un recurso personalizado. Por ejemplo, no es necesario que cree un recurso personalizado si su flujo de trabajo actualiza un valor de base de datos o envía un mensaje de correo electrónico después de una operación de aprovisionamiento.

Al crear un recurso personalizado, puede especificar los campos del formulario de solo lectura en los detalles de un elemento aprovisionado. Consulte [Diseñar un formulario de recurso personalizado](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto XaaS**.
- Use la información de las opciones detalladas para configurar el recurso personalizado. Consulte [Opciones del asistente de recursos personalizados de XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Recursos personalizados**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Configure los valores de la pestaña **Tipo de recurso**.
 - a Introduzca o seleccione el tipo de objeto de vRealize Orchestrator en el cuadro de texto **Tipo de orquestador**.
 Por ejemplo, escriba **v** para ver los tipos que contienen la letra v. Para ver todos los tipos, introduzca un espacio.
 - b Especifique un nombre y, opcionalmente, una descripción.
 - c Escriba una versión.
 El formato admitido se amplía a versión principal.secundaria.micro.
 - d Haga clic en **Siguiente**.
- 4 Edite la pestaña **Formulario de detalles** según corresponda.
 Puede editar el formulario del recurso personalizado si elimina, edita y cambia el orden de los elementos. También puede añadir formularios y páginas de formulario, y arrastrar elementos al nuevo formulario o página del formulario.
- 5 Haga clic en **Finalizar**.

Resultados

Ha creado un recurso personalizado que ahora se muestra en la página Recursos personalizados. Puede crear acciones o blueprints XaaS a partir de este recurso personalizado.

Pasos siguientes

- Cree un blueprint XaaS. Consulte [Añadir un blueprint XaaS](#).

- Cree una acción personalizada de XaaS. Consulte [Crear una acción personalizada de XaaS](#).

Opciones del asistente de recursos personalizados de XaaS

Estas opciones de recursos personalizados se utilizan para crear o modificar un recurso personalizado con el fin de poder ejecutar flujos de trabajo de acciones personalizadas y blueprints XaaS que aprovisionan recursos o modifican recursos aprovisionados.

Para un tipo de objeto, solo se puede crear un recurso personalizado. El recurso personalizado puede utilizarse para varios blueprints y acciones personalizadas.

Para crear una acción personalizada, seleccione **Diseño > XaaS > Recursos personalizados**

Tipo de recurso

La lista de los posibles tipos de objeto que aparece en la pestaña **Tipo de recurso** con base en los complementos instalados en la instancia configurada de vRealize Orchestrator. vRealize Automation recopila los valores de la instancia configurada de vRealize Orchestrator.

Tabla 3-54. Opciones de Tipo de recursos

Opción	Descripción
Tipo de orquestador	<p>Introduzca o seleccione el tipo que admite el flujo de trabajo que utiliza para aprovisionar.</p> <p>El tipo se compone del nombre de complemento que aparece en la API de creación de scripts (por ejemplo, VC para vCenter) y el tipo de objeto (por ejemplo, VirtualMachine). En este ejemplo, la API utiliza el valor VC:VirtualMachine.</p> <p>Este tipo puede ser el parámetro de salida del flujo de trabajo del blueprint o el parámetro de entrada del flujo de trabajo de la acción personalizada.</p>
Nombre	<p>Escriba un nombre que le permita identificar el recurso personalizado cuando crea blueprints XaaS o acciones personalizadas.</p>
Descripción	<p>Escriba una descripción detallada.</p>
Versión	<p>El formato admitido llega hasta versión_principal.versión_secundaria.revisión_mínima.</p>

Formulario de detalles

Los campos de este formulario se muestran como valores de solo lectura cuando los usuarios del catálogo de servicios aprovisionan un elemento que utiliza este recurso personalizado. Puede modificar los campos existentes y añadir nuevos campos definidos de manera externa.

Para obtener más información sobre la configuración de los formularios, consulte [Diseñar un formulario de recurso personalizado](#).

Dónde se usa

Puesto que solo se puede crear un recurso personalizado por tipo de objeto, puede utilizar esta página del asistente para comprender la manera en la que se utiliza el recurso personalizado.

Esta pestaña está disponible para recursos personalizados que se hayan guardado, no al crear el recurso.

Tabla 3-55. Opciones de Dónde se usa

Opción	Descripción
Blueprints XaaS	<p>Una lista de los blueprints que están configurados para utilizar este recurso personalizado.</p> <p>Desde esta página se pueden realizar las siguientes acciones:</p> <ul style="list-style-type: none"> ■ Editar. Abre el blueprint para que pueda determinar su configuración o para modificarlo. ■ Publicar/Cancelar la publicación. Cambia el estado del blueprint poniéndolo a disposición para utilizarlo en un blueprint compuesto o para añadirlo a un servicio. Si cancela la publicación de un blueprint, es posible que pueda hacer que no esté disponible para utilizarlo en blueprints compuestos, para añadirlo a un servicio, o para hacer que no aparezca el catálogo de servicios. ■ Eliminar. Quita un blueprint del sistema.
Acciones personalizadas	<p>Una lista de las acciones personalizadas que están configuradas para utilizar este recurso personalizado.</p> <p>Desde esta página se pueden realizar las siguientes acciones:</p> <ul style="list-style-type: none"> ■ Editar. Abre la acción personalizada para que pueda determinar su configuración o para modificarla. ■ Publicar/Cancelar la publicación. Cambia el estado de la acción personalizada poniéndola a disposición en una autorización. Si cancela la publicación de una acción personalizada, es posible que pueda hacer que no esté disponible para añadirla a un servicio o para ejecutarla en blueprints implementados. ■ Eliminar. Quita esta acción personalizada del sistema.

Crear un blueprint XaaS

Un blueprint XaaS es un blueprint de aprovisionamiento o de no aprovisionamiento. Algunos de los flujos de trabajo de aprovisionamiento de vRealize Orchestrator proporcionados incluyen la creación de máquinas virtuales, la adición de usuarios a Active Directory o la captura de snapshots de máquinas virtuales. Algunos de los flujos de trabajo de no aprovisionamiento que puede crear incluyen la actualización del equilibrador de carga o la creación de un informe y su envío a los destinatarios.

Puede crear blueprints XaaS basados en flujos de trabajo proporcionados en vRealize Orchestrator o utilizar flujos de trabajo que usted cree para alcanzar los objetivos específicos de su entorno.

Procedimiento

1 [Añadir un blueprint XaaS](#)

Un blueprint XaaS es una especificación para ejecutar un flujo de trabajo de vRealize Orchestrator que realiza un cambio en un sistema de destino de su entorno. El blueprint incluye el flujo de trabajo y puede incluir los parámetros de entrada, los formularios de envío y de solo lectura, la secuencia de acciones y la operación de aprovisionamiento o de no aprovisionamiento.

2 [Añadir un blueprint XaaS a un blueprint compuesto](#)

La adición de un blueprint XaaS como componente de un blueprint compuesto se realiza de forma similar a la adición de otros componentes de blueprint en el lienzo de diseño.

Añadir un blueprint XaaS

Un blueprint XaaS es una especificación para ejecutar un flujo de trabajo de vRealize Orchestrator que realiza un cambio en un sistema de destino de su entorno. El blueprint incluye el flujo de trabajo y puede incluir los parámetros de entrada, los formularios de envío y de solo lectura, la secuencia de acciones y la operación de aprovisionamiento o de no aprovisionamiento.

Puede crear blueprints XaaS que podrá usar de las siguientes maneras:

- Crear un componente de blueprint XaaS. Un blueprint de componentes es un blueprint de aprovisionamiento o de no aprovisionamiento que puede utilizar en el lienzo de diseño de blueprints como parte de un blueprint compuesto. Si lo usa como un componente, debe configurar las opciones del ciclo de vida del componente que admitan operaciones de escalado vertical y horizontal en el blueprint compuesto implementado.

Este tipo de blueprint también puede publicarse como un blueprint independiente.
- Cree un blueprint XaaS independiente. Un blueprint independiente es un blueprint de aprovisionamiento o de no aprovisionamiento que se publica y se autoriza directamente en el catálogo de servicios.

Para obtener un ejemplo de cómo crear usuarios de Active Directory mediante un blueprint XaaS, consulte [Crear un blueprint y acción de XaaS para crear y modificar un usuario](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto XaaS**.
- Si el blueprint debe aprovisionar recursos, cree un recurso personalizado correspondiente al parámetro de salida del blueprint de servicio. Consulte [Añadir un recurso personalizado de XaaS](#). Si el blueprint no utiliza una API de complemento de vRealize Orchestrator, no es necesario que configure un recurso personalizado.

- Al crear un blueprint XaaS, se publica un flujo de trabajo de vRealize Orchestrator como posible blueprint de componentes o elemento del catálogo. El blueprint incluye un formulario que puede editar. Consulte [Diseñar un formulario de blueprint de XaaS](#).
- Utilice la información de las opciones detalladas para configurar el blueprint. Consulte [Opciones del asistente para editar o crear nuevo blueprint XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Blueprints XaaS**.

- 2 Haga clic en el icono **Nuevo** (+).

- 3 En la pestaña **Flujo de trabajo**, seleccione el flujo de trabajo que se ejecuta cuando el blueprint aprovisiona el recurso.

Esta pestaña no está disponible cuando se está editando un blueprint.

- a Desplácese por la biblioteca de flujos de trabajo de vRealize Orchestrator y seleccione un flujo de trabajo relevante para su recurso personalizado.
- b Revise los parámetros de entrada y de salida para asegurarse de que después pueda indicar los valores correctos.
- c Haga clic en **Siguiente**.

- 4 En la pestaña **General**, configure las opciones y haga clic en **Siguiente**.

- a En el cuadro de texto **Nombre**, escriba un nombre que permita diferenciar este blueprint frente a blueprints similares.
- b Si no desea utilizar este blueprint como componente de un blueprint compuesto, desactive la casilla de verificación **Facilitar como un componente en el lienzo de diseño**.

- 5 En la pestaña **Formulario de blueprint**, modifique el formulario según corresponda y haga clic en **Siguiente**.

- 6 En la página **Recurso aprovisionado**, seleccione un valor y haga clic en **Siguiente**.

Opción	Descripción
Sin aprovisionamiento	Si el flujo de trabajo no aprovisiona recursos, puede seleccionar esta opción o dejar el campo vacío.
<Un recurso personalizado creado anteriormente>	Seleccione el recurso personalizado que admite este flujo de trabajo de aprovisionamiento.

- 7 En la pestaña **Ciclo de vida del componente**, indique cómo se comportará este blueprint durante las operaciones de escalado vertical, escalado horizontal y destrucción.

Estos flujos de trabajo se ejecutan en un blueprint compuesto implementado en el que este blueprint es un componente. La disponibilidad de las diferentes opciones depende del blueprint. No todos los flujos de trabajo de blueprint admiten o requieren todas las opciones.

- 8 Haga clic en **Finalizar**.

9 Seleccione la fila del blueprint y haga clic en **Publicar**.

Resultados

Ha creado y publicado un blueprint XaaS.

Pasos siguientes

- Para añadir este blueprint directamente al catálogo de servicios como un blueprint independiente, agregue un servicio y, a continuación, añada el blueprint a un servicio. Consulte [Añadir un servicio](#).
- Para utilizar este blueprint como un componente en un blueprint compuesto, consulte [Añadir un blueprint XaaS a un blueprint compuesto](#).

Opciones del asistente para editar o crear nuevo blueprint XaaS

Estas opciones se utilizan para crear un blueprint XaaS que ejecuta un flujo de trabajo de vRealize Orchestrator cuando se implementa el blueprint. El flujo de trabajo cambia un sistema de destino en el entorno.

Para conocer los pasos que se deben seguir para crear el blueprint, consulte [Añadir un blueprint XaaS](#).

Para utilizar este asistente, seleccione **Diseño > XaaS > Blueprints XaaS**.

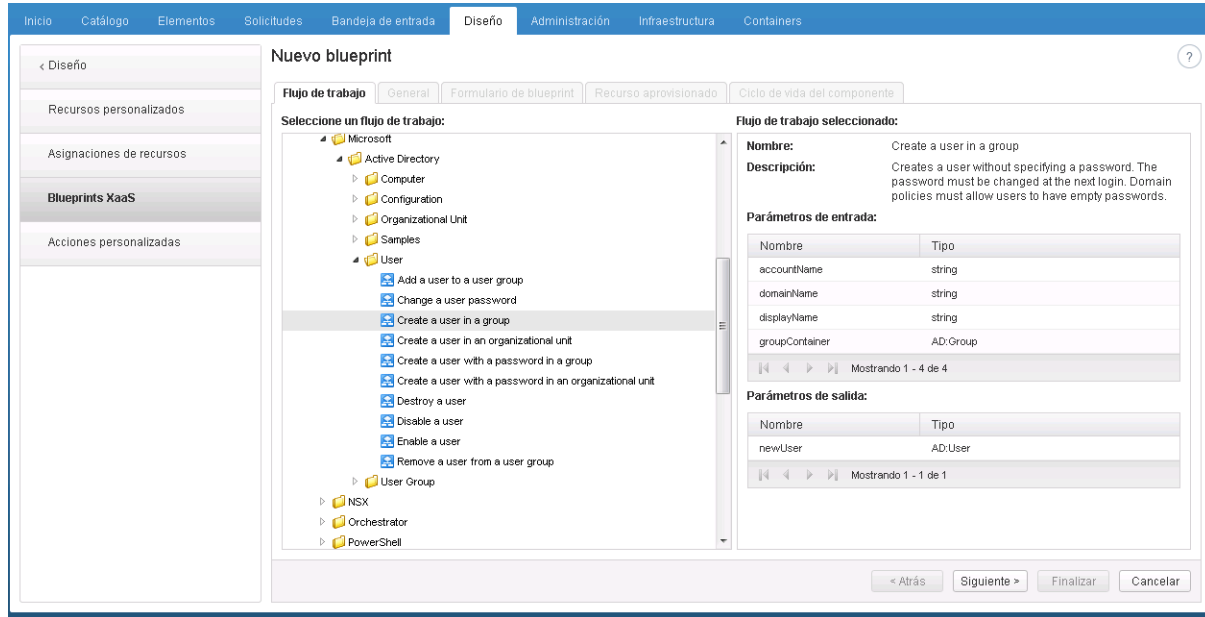
Pestaña Flujo de trabajo

Seleccione el flujo de trabajo que se ejecuta cuando el blueprint aprovisiona el recurso.

Esta pestaña no está disponible cuando se está editando un blueprint.

En la siguiente imagen, el árbol de flujo de trabajo se encuentra a la izquierda y los parámetros se encuentran a la derecha.

Figura 3-4. Pestaña Flujo de trabajo en el asistente de blueprint XaaS



Revise los parámetros de entrada y de salida para asegurarse de que usted o los usuarios del catálogo de servicios pueden proporcionar los valores correctos en los siguientes casos:

- Si se personaliza el formulario de blueprint en este asistente o en el lienzo de diseño del blueprint.
- Si se dejan en blanco todos los parámetros de entrada, los usuarios del catálogo de servicios pueden definir los valores.

Pestaña General

Configure el comportamiento del blueprint y los metadatos relacionados con este.

Tabla 3-56. Opciones de la pestaña General

Opción	Descripción
Nombre	<p>El nombre del blueprint tal como se desea que aparezca en las siguientes ubicaciones:</p> <ul style="list-style-type: none"> ■ Lienzo de diseño. Si selecciona Facilitar como un componente en el lienzo de diseño, este valor es el nombre que se muestra en la lista de categorías. ■ Servicios. Si utiliza este blueprint como blueprint independiente, este valor es el nombre que se muestra al añadir elementos del catálogo al servicio. ■ Autorizaciones. Si autoriza el blueprint como elemento individual, este valor es el nombre que se muestra en la lista Añadir elementos.
Descripción	<p>Proporcione una descripción detallada que le permita a diferenciar entre elementos similares.</p>

Tabla 3-56. Opciones de la pestaña General (continuación)

Opción	Descripción
Ocultar página de información de solicitudes del catálogo	Active la casilla de verificación cuando no desee pedir a los consumidores del catálogo de servicios que proporcionen una descripción y un motivo al solicitar el elemento. La casilla de verificación está activada de forma predeterminada.
Versión	El formato admitido se amplía a versión principal.secundaria.micro.
Facilitar como un componente en el lienzo de diseño	<p>Si tiene previsto utilizar el blueprint como un componente en un blueprint de lienzo de diseño, seleccione esta opción. Cuando se publica, el blueprint está disponible en la categoría que ha seleccionado al configurar el recurso personalizado.</p> <p>Si no selecciona esta opción, el blueprint no se mostrará en el lienzo de diseño. No obstante, aún puede añadirlo a un servicio y autorizar a los usuarios para implementarlo como un blueprint independiente.</p>

Pestaña Formulario de blueprint

Los campos que se muestran en esta página del asistente son los parámetros de entrada del flujo de trabajo. Puede hacer uno o varios de los siguientes cambios:

- Añadir campos al formulario.
- Modificar los campos existentes (eliminarlos o reorganizarlos).
- Indicar valores predeterminados como parámetros de entrada.

Cualquier cambio afecta al formulario que se presenta a las siguientes personas:

- El arquitecto de aplicaciones que trabaja en el lienzo de diseño cuando se utiliza el blueprint XaaS como un componente de blueprint.
- El usuario del catálogo de servicios si se publica el blueprint como un blueprint independiente.

Para obtener más información sobre la configuración de los formularios, consulte [Diseñar un formulario de blueprint de XaaS](#).

Recurso aprovisionado

El recurso aprovisionado vincula el blueprint con un recurso personalizado relevante de XaaS configurado en la página Recurso personalizado en **Diseño > XaaS > Recurso personalizado**.

Tabla 3-57. Opciones de Recurso aprovisionado

Opción	Descripción
Recurso personalizado que creó antes	<p>Seleccione el recurso personalizado que define el tipo de recurso de vRealize Orchestrator que se necesita para ejecutar el blueprint de aprovisionamiento.</p> <p>Un blueprint de aprovisionamiento ejecuta un flujo de trabajo de vRealize Orchestrator para aprovisionar recursos en el endpoint de destino utilizando la API del complemento de vRealize Orchestrator para el endpoint. Por ejemplo, añadir NIC virtuales a un dispositivo de red en vSphere.</p> <p>Puede definir operaciones posteriores al aprovisionamiento para este tipo de recursos aprovisionados. También puede añadir o quitar instancias cuando sea necesario para hacer que el blueprint sea escalable.</p> <p>Resultados</p> <ul style="list-style-type: none"> ■ El blueprint se puede escalar. ■ El blueprint se muestra en el lienzo de diseño en la categoría especificada para el recurso personalizado seleccionado. ■ El blueprint se muestra en la pestaña Elementos cuando se implementa un blueprint que lo incluye. Puede ejecutar cualquier acción en el elemento después de implementarlo.
Sin aprovisionamiento	<p>Un blueprint de no aprovisionamiento ejecuta un flujo de trabajo de vRealize Orchestrator para realizar una tarea que no requiera la API para hacer cambios en un endpoint. Por ejemplo, generar un informe y enviarlo por correo electrónico a un sistema de comunicación de destino o publicarlo en él.</p> <p>Resultados</p> <ul style="list-style-type: none"> ■ El blueprint no se puede escalar. Puede utilizar blueprints de no aprovisionamiento como flujos de trabajo de apoyo en blueprints escalables. Por ejemplo, puede crear un blueprint para actualizar un equilibrador de carga de alta disponibilidad. ■ El blueprint se muestra en la categoría XaaS del lienzo de diseño. ■ El blueprint no se muestra en la pestaña Elementos cuando se implementa un blueprint que lo incluye. Asimismo, tampoco puede ejecutar ninguna acción en el elemento después de implementarlo.

Pestaña Ciclo de vida del componente

La pestaña Ciclo de vida del componente está disponible si se selecciona **Facilitar como un componente en el lienzo de diseño** en la pestaña **General**.

Estas opciones se utilizan para definir cómo se comporta el blueprint después de la implementación durante las operaciones de escalado vertical y horizontal cuando se utiliza como componente en un blueprint compuesto.

La disponibilidad de las distintas opciones depende del blueprint. No todos los flujos de trabajo de blueprint admiten o requieren todas las opciones. Puesto que XaaS podría utilizarse en un blueprint compuesto, debería configurar las opciones de actualización y destrucción, así como las de asignación y desasignación (si están disponibles para el blueprint) de modo que el blueprint se escale correctamente.

Tabla 3-58. Opciones de Ciclo de vida del componente

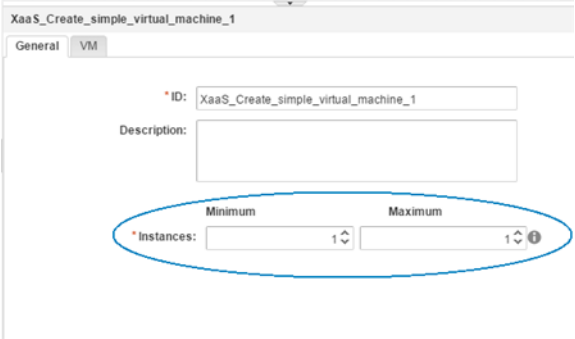
Opción	Descripción
Escalable	<p>Seleccione esta opción para permitir al usuario del catálogo de servicios cambiar el número de instancias de este componente de blueprint después de su implementación como parte de una operación de escalado vertical o escalado horizontal.</p> <p>Esta opción está disponible si se selecciona un recurso personalizado en la pestaña Recurso aprovisionado. No está disponible si se selecciona la opción Sin aprovisionamiento.</p> <p>Si hace que este blueprint sea escalable, se añade la opción Instancias a la pestaña General del lienzo de diseño. Consulte el ejemplo siguiente. Si no selecciona Escalable, la opción Instancias no está disponible en el lienzo de diseño.</p> 
Flujo de trabajo de aprovisionamiento	<p>El flujo de trabajo que se ejecuta durante una operación de escalado horizontal o aprovisionamiento. Este flujo de trabajo se selecciona cuando se crea el blueprint; no se puede editar el valor.</p>

Tabla 3-58. Opciones de Ciclo de vida del componente (continuación)

Opción	Descripción
Flujo de trabajo de asignación	<p>Seleccione el flujo de trabajo que se ejecuta antes de cualquier operación de escalado horizontal o aprovisionamiento inicial.</p> <p>Este tipo de flujo de trabajo de ciclo de vida está disponible para asignaciones de Azure. Si crea un flujo de trabajo de asignación para una operación de escalado, debe incluir los siguientes valores:</p> <ul style="list-style-type: none"> ■ Parámetros de entrada <ul style="list-style-type: none"> ■ El nombre del parámetro es <code>requestData</code> y el tipo de parámetro es <code>Properties</code>. ■ El nombre del parámetro es <code>subtenant</code> y el tipo de parámetro es <code>Properties</code>. ■ <code>reservations</code> y el tipo de parámetro es <code>Arrays/Properties</code>. ■ Parámetro de salida <ul style="list-style-type: none"> ■ Debe incluir un parámetro cuyo tipo sea <code>Properties</code>.
Flujo de trabajo de actualización	<p>Seleccione el flujo de trabajo que se ejecuta durante las operaciones de actualización, incluidos el escalado vertical o el escalado horizontal cuando un componente no es escalable, pero puede actualizarse.</p> <p>Por ejemplo, un equilibrador de carga se actualiza con la nueva configuración creada con la operación de escalado vertical o escalado horizontal de cualquiera de los componentes del blueprint compuesto.</p> <p>El flujo de trabajo de actualización se podría aplicar a un componente que no es escalable, pero que está vinculado con el componente escalado. Este flujo de trabajo de actualización puede cambiar componentes no escalables basándose en una operación de actualización.</p> <p>Si crea un flujo de trabajo de actualización para una operación de escalado, debe incluir los siguientes valores:</p> <ul style="list-style-type: none"> ■ Parámetros de entrada. <ul style="list-style-type: none"> ■ Debe incluir un parámetro de cualquier nombre que coincida con el tipo de parámetro de salida del flujo de trabajo de aprovisionamiento. ■ El nombre del parámetro es <code>data</code> y el tipo de parámetro es <code>Properties</code>.

Tabla 3-58. Opciones de Ciclo de vida del componente (continuación)

Opción	Descripción
Flujo de trabajo de destrucción	<p>Seleccione el flujo de trabajo que se ejecuta durante una operación de escalado vertical o destrucción.</p> <p>Si crea un flujo de trabajo de destrucción para una operación de escalado, debe incluir el siguiente valor:</p> <ul style="list-style-type: none"> ■ Parámetro de entrada. <ul style="list-style-type: none"> ■ Debe incluir un parámetro de cualquier nombre que coincida con el tipo de parámetro de salida del flujo de trabajo de aprovisionamiento. <p>Por ejemplo, si el flujo de trabajo de aprovisionamiento Crear máquina virtual simple incluye el parámetro de salida VC:VirtualMachine, el flujo de trabajo de destrucción debe incluir un parámetro de entrada cuyo tipo sea VC:VirtualMachine.</p>
Flujo de trabajo de desasignación	<p>Seleccione el flujo de trabajo que se ejecuta después de cualquier operación de escalado vertical o destrucción. Si se producen errores en la desasignación durante la operación, el flujo de trabajo de destrucción sigue ejecutándose según lo previsto.</p> <p>Cuando se escala verticalmente o se destruye un blueprint compuesto, la desasignación es el proceso final, la cual se ejecuta para liberar recursos después de la operación de destrucción.</p> <p>Este tipo de flujo de trabajo de ciclo de vida está disponible para asignaciones de Azure. Si crea un flujo de trabajo de desasignación para una operación de escalado, debe incluir el siguiente valor:</p> <ul style="list-style-type: none"> ■ Parámetro de entrada. <ul style="list-style-type: none"> ■ El nombre del parámetro es <code>data</code> y el tipo de parámetro es <code>Properties</code>.
Categoría	<p>Para especificar dónde se muestra el blueprint XaaS en el lienzo de diseño, seleccione un valor del menú desplegable Categoría de lienzo de diseño.</p> <p>Si no se selecciona ninguna categoría, el blueprint se añade a la categoría XaaS cuando se publica.</p>

Añadir un blueprint XaaS a un blueprint compuesto

La adición de un blueprint XaaS como componente de un blueprint compuesto se realiza de forma similar a la adición de otros componentes de blueprint en el lienzo de diseño.

Utilice este método para añadir XaaS a un blueprint compuesto. Este blueprint puede ser el único componente del blueprint, o bien uno de varios componentes que integran un blueprint de aplicación.

Si el blueprint XaaS es lo único que quiere ofrecer a sus usuarios, puede añadirlo a un servicio y autorizar a los usuarios para que lo usen sin tener que añadirlo a un blueprint compuesto.

Si ejecuta una operación de escalado vertical u horizontal en un blueprint de aplicación implementado, el blueprint XaaS se escala en función de la manera en la que ha configurado las opciones del ciclo de vida del blueprint.

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Cree y publique un blueprint XaaS. Consulte [Crear un blueprint XaaS](#). Cuando creó el blueprint, especificó la categoría en la que se encuentra el blueprint en el lienzo de diseño.
- Revise cómo personalizar los formularios de blueprint XaaS en el blueprint compuesto. Consulte [Diseñar formularios para blueprints y acciones de XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > Blueprints**.
- 2 Seleccione el nombre del blueprint al que añade XaaS.
Aparecerá el lienzo de diseño. Contiene los blueprints de componentes actuales de la aplicación, así como otros componentes.
- 3 En la lista Categorías, busque el blueprint.
- 4 Arrastre su blueprint al lienzo.
- 5 Configure los valores predeterminados en las pestañas General y Crear.
Estos son los valores predeterminados que aparecen en el formulario del catálogo de servicios cuando un usuario solicita el elemento.
- 6 Haga clic en **Finalizar**.
- 7 Seleccione el blueprint y haga clic en **Publicar**.

Resultados

El blueprint XaaS ahora forma parte del blueprint compuesto.

Pasos siguientes

Añada el blueprint compuesto a un servicio. Consulte [Administrar el catálogo de servicios](#).

Crear una acción personalizada de XaaS

La acción personalizada se crea para poder administrar los elementos aprovisionados mediante flujos de trabajo de vRealize Orchestrator.

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto XaaS**.
- Compruebe que dispone de un recurso personalizado que admita la acción. Consulte [Añadir un recurso personalizado de XaaS](#).

- Si crea acciones para ejecutarlas en elementos no aprovisionados como elementos del catálogo de XaaS, compruebe que ha asignado los recursos de destino. Consulte [Asignar otros recursos para que funcionen con acciones personalizadas de XaaS](#).

Procedimiento

1 Crear una acción personalizada

Un acción personalizada es un flujo de trabajo de XaaS que los usuarios del catálogo de servicios pueden ejecutar en elementos del catálogo aprovisionados. Como arquitecto de XaaS, puede crear acciones personalizadas para definir las operaciones que los consumidores van a poder realizar en los elementos aprovisionados.

2 Publicar una acción personalizada

La acción personalizada recién publicada tiene el estado de borrador y se debe publicar.

3 Asignar un icono a una acción de recursos de XaaS

Después de crear y publicar una acción personalizada, puede editarla y asignarle un icono.

Crear una acción personalizada

Un acción personalizada es un flujo de trabajo de XaaS que los usuarios del catálogo de servicios pueden ejecutar en elementos del catálogo aprovisionados. Como arquitecto de XaaS, puede crear acciones personalizadas para definir las operaciones que los consumidores van a poder realizar en los elementos aprovisionados.

Al crear una acción personalizada, asocia un flujo de trabajo de vRealize Orchestrator como una operación posterior al aprovisionamiento. Durante este proceso, puede editar el envío predeterminado y los formularios de solo lectura. Consulte [Diseñar un formulario de acción personalizada](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto XaaS**.
- Cree un recurso personalizado que se corresponda con el parámetro de entrada de la acción personalizada.

Procedimiento

1 Seleccione **Diseño > XaaS > Acciones personalizadas**.

2 Haga clic en el icono **Nuevo** (+).

3 Desplácese por la biblioteca de flujos de trabajo de vRealize Orchestrator y seleccione un flujo de trabajo relevante para su recurso personalizado.

Puede ver el nombre y la descripción del flujo de trabajo seleccionado, y los parámetros de entrada y salida, tal y como están definidos en vRealize Orchestrator.

4 Haga clic en **Siguiente**.

5 Seleccione el recurso personalizado que creó anteriormente en el menú desplegable **Tipo de recurso**.

- 6 Seleccione el parámetro de entrada correspondiente a la acción personalizada en el menú desplegable **Parámetro de entrada**.

- 7 Haga clic en **Siguiente**.

- 8 Especifique un nombre y, opcionalmente, una descripción.

Los cuadros de texto **Nombre** y **Descripción** se rellenan previamente con el nombre y la descripción del flujo de trabajo, tal y como están definidos en vRealize Orchestrator.

- 9 (opcional) Si no desea pedir a los consumidores que escriban una descripción y un motivo para la solicitud de esta acción personalizada, active la casilla **Ocultar página de información de solicitudes del catálogo**.

- 10 Escriba una versión.

El formato admitido se amplía a versión principal.secundaria.micro.

- 11 (opcional) Seleccione el tipo de la acción.

Opción	Descripción
Baja	El parámetro de entrada del flujo de trabajo de acciones personalizadas se da de baja y el elemento se quita de la pestaña Elementos . Por ejemplo, una acción personalizada para eliminar una máquina aprovisionada.
Aprovisionar	La acción personalizada es para aprovisionamiento. Por ejemplo, una acción personalizada para copiar un elemento del catálogo. Seleccione un parámetro de salida del menú desplegable. Puede seleccionar un recurso personalizado creado anteriormente para que, cuando los consumidores soliciten esta acción personalizada, los elementos aprovisionados se añadan en la pestaña Elementos . Si solo dispone de la opción sin aprovisionamiento , significa que la acción personalizada no sirve para aprovisionar, o bien que no creó un recurso personalizado adecuado para el parámetro de salida y, por lo tanto, no puede continuar.

En función de flujo de trabajo de acciones, puede seleccionar una de las opciones, ambas o ninguna de ellas.

- 12 Seleccione las condiciones en las que la acción personalizada está disponible para los usuarios y haga clic en **Siguiente**.

13 (opcional) Edite el formulario de la acción personalizada en la pestaña **Formulario**.

El formulario de la acción personalizada asigna la presentación de flujos de trabajo de vRealize Orchestrator. Si desea cambiar el formulario, elimine, edite o reorganice los elementos. También puede añadir un formulario nuevo o páginas de formulario y arrastrar los elementos necesarios al nuevo formulario o página del formulario.

Opción	Acción
Añadir un formulario	Haga clic en el icono Formulario nuevo (+) junto al nombre del formulario, proporcione la información necesaria y haga clic en Enviar .
Editar un formulario	Haga clic en el icono Editar (✎) junto al nombre de formulario, realice los cambios necesarios y haga clic en Enviar .
Regenerar la presentación de flujos de trabajo	Haga clic en el icono Reconstruir (↺) junto al nombre del formulario y haga clic en Aceptar .
Eliminar un formulario	Haga clic en el icono Eliminar (✖) junto al nombre de formulario y, en el cuadro de diálogo de confirmación, haga clic en Aceptar .
Añadir una página de formulario	Haga clic en el icono Página nueva (+) junto al nombre de la página de formulario, proporcione la información necesaria y haga clic en Enviar .
Editar una página de formulario	Haga clic en el icono Editar (✎) junto al nombre de la página de formulario, realice los cambios necesarios y haga clic en Enviar .
Eliminar una página de formulario	Haga clic en el icono Eliminar (✖) junto al nombre de formulario y, en el cuadro de diálogo de confirmación, haga clic en Aceptar .
Añadir un elemento a la página de formulario	Arrastre al panel de la derecha un elemento del panel Campos nuevos de la izquierda. A continuación, puede proporcionar la información necesaria y hacer clic en Enviar .
Editar un elemento	Haga clic en el icono Editar (✎) junto al elemento que desea editar, realice los cambios necesarios y haga clic en Enviar .
Eliminar un elemento	Haga clic en el icono Eliminar (✖) junto al elemento que desea eliminar y, en el cuadro de diálogo de confirmación, haga clic en Aceptar .

14 Haga clic en **Finalizar**.

Resultados

Ha creado una acción personalizada, que ahora aparece recogida en la página Acciones personalizadas.

Pasos siguientes

Publicar la acción personalizada. Consulte [Publicar una acción personalizada](#).

Publicar una acción personalizada

La acción personalizada recién publicada tiene el estado de borrador y se debe publicar.

Requisitos previos

Inicie sesión en vRealize Automation como **arquitecto XaaS**.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Seleccione la fila de la acción personalizada que se publicará y haga clic en **Publicar**.

Resultados

El estado de la acción personalizada cambiará a Publicada.

Pasos siguientes

Asigne un icono a la acción personalizada. Consulte [Asignar un icono a una acción de recursos de XaaS](#). Los administradores de grupos empresariales y los administradores de tenant podrán usar la acción cuando creen una autorización.

Asignar un icono a una acción de recursos de XaaS

Después de crear y publicar una acción personalizada, puede editarla y asignarle un icono.

Requisitos previos

Inicie sesión en vRealize Automation como **arquitecto XaaS**.

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Acciones**.
- 2 Seleccione la acción personalizada que ha creado.
- 3 Haga clic en **Configurar**.
- 4 Haga clic en **Examinar** y seleccione el icono que desea añadirle.
- 5 Haga clic en **Abrir**.
- 6 Haga clic en **Actualizar**.

Resultados

Ha asignado un icono a la acción personalizada. Los administradores de grupo empresarial y los administradores de tenants pueden usar la acción personalizada en una autorización.

Asignar otros recursos para que funcionen con acciones personalizadas de XaaS

Asigna elementos que no se aprovisionaron mediante XaaS para poder ejecutar acciones personalizadas en dichos elementos.

Flujos de trabajo y acciones de script para la asignación de recursos

Puede usar las asignaciones de recursos proporcionadas para máquinas virtuales de vSphere, vCloud Director o vCloud Air, o bien puede crear flujos de trabajo o acciones de script de

vRealize Orchestrator personalizados para asignar otros tipos de recursos del catálogo de vRealize Automation a tipos de inventario de vRealize Orchestrator.

Asignaciones de recursos proporcionadas con vRealize Automation

vRealize Automation incluye asignaciones de recursos para máquinas virtuales de vSphere de IaaS, vCloud Director de IaaS e implementaciones.

vRealize Automation incluye acciones de script de asignaciones de recursos de vRealize Orchestrator para cada una de las asignaciones de recursos de XaaS proporcionadas. Las acciones de script para las asignaciones de recursos proporcionadas se encuentran en el paquete `com.vmware.vcac.asd.mappings` del servidor de vRealize Orchestrator integrado.

Cuando crea una acción personalizada que se ejecuta en un blueprint compuesto implementado que usa un flujo de trabajo de vRealize Orchestrator con `vCACAFE:CatalogResource` como un parámetro de entrada, se aplica la asignación Implementación como el tipo de recurso de entrada. La asignación Implementación solo se aplica si el flujo de trabajo seleccionado incluye un `vCACAFE:CatalogResource` como un parámetro de entrada. Por ejemplo, si crea una acción para solicitar una acción personalizada en nombre de un usuario, el tipo de recurso en la pestaña Recurso de entrada es Implementación porque este flujo de trabajo usa `vCACAFE:CatalogResource`.

Una acción usa las asignaciones de recursos IaaS vCD VM e IaaS VC VirtualMachine para asignar las máquinas virtuales que coinciden con el recurso de IaaS con la máquina virtual de vRealize Orchestrator vSphere o de vCloud Director.

Desarrollo de asignaciones de recursos

En función de la versión de vRealize Orchestrator, puede crear un flujo de trabajo o una acción de script de vRealize Orchestrator para asignar recursos entre vRealize Orchestrator y vRealize Automation.

Para desarrollar la asignación de recursos, debe usar un parámetro de entrada de tipo `Properties`, que contenga un par clave-valor que defina el recurso aprovisionado, y un parámetro de salida de un tipo de inventario de vRealize Orchestrator esperado por el complemento de vRealize Orchestrator correspondiente. Las propiedades disponibles para la asignación dependen del tipo de recurso. Por ejemplo, la propiedad `EXTERNAL_REFERENCE_ID` es un parámetro de clave habitual que define máquinas virtuales individuales, y puede usar esta propiedad para consultar un recurso del catálogo. Si crea una asignación para un recurso que no utiliza `EXTERNAL_REFERENCE_ID`, puede usar una de las otras propiedades que se transfieren a las máquinas virtuales individuales. Por ejemplo, nombre, descripción, etc.

Para obtener más información acerca del desarrollo de flujos de trabajo y acciones de script, consulte el tema sobre el *desarrollo con VMware vCenter Orchestrator*.

Crear una asignación de recursos

vRealize Automation proporciona asignaciones de recursos para máquinas de vSphere, vCloud Director y vCloud Air. Puede crear asignaciones de recursos adicionales para otros tipos de recursos del catálogo.

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto XaaS**.
- Compruebe que el flujo de trabajo o el script de asignación esté disponible en vRealize Orchestrator. Consulte [Flujos de trabajo y acciones de script para la asignación de recursos](#)

Procedimiento

- 1 Seleccione **Diseño > XaaS > Asignaciones de recursos**.

- 2 Haga clic en el icono **Nuevo** (+).

- 3 Especifique un nombre y, opcionalmente, una descripción.

- 4 Escriba una versión.

El formato admitido se amplía a versión principal.secundaria.micro.

- 5 Escriba el tipo de recurso del catálogo en el cuadro de texto **Tipo del recurso del catálogo** y pulse Entrar.

El tipo de recurso del catálogo aparece en la vista de detalles del elemento aprovisionado.

- 6 Escriba el tipo de objeto de vRealize Orchestrator en el cuadro de texto **Tipo de orquestador** y pulse Entrar.

Este es el parámetro de salida del flujo de trabajo de asignación de recursos.

- 7 (opcional) Añada criterios de destino para restringir la disponibilidad de las acciones personalizadas creadas mediante esta asignación de recursos.

Las acciones personalizadas también están sujetas a restricciones según las aprobaciones y las autorizaciones.

- a Seleccione **Disponible según las condiciones**.

- b Seleccione el tipo de condición.

Opción	Descripción
Todos los siguientes	Si se cumplen todas las cláusulas que ha definido, las acciones personalizadas creadas mediante esta asignación de recursos estarán disponibles para el usuario.
Cualesquiera de los siguientes	Si se cumple alguna de las cláusulas que ha definido, las acciones personalizadas creadas mediante esta asignación de recursos estarán disponibles para el usuario.
No los siguientes	Si existe la cláusula que ha definido, las acciones personalizadas creadas mediante esta asignación de recursos no estarán disponibles.

- c Siga las indicaciones para crear las cláusulas y completar la condición.

- 8 Seleccione el flujo de trabajo o la acción de script de asignación de recursos en la biblioteca de vRealize Orchestrator.

- 9 Haga clic en **Aceptar**.

Diseñar formularios para blueprints y acciones de XaaS

XaaS incluye un diseñador de formularios que puede usar para diseñar formularios de envío y de detalles para los blueprints y acciones personalizadas. Basado en la presentación de los flujos de trabajo, el diseñador de formularios genera de forma dinámica formularios predeterminados y campos que puede usar para modificar estos formularios predeterminados.

Puede crear formularios interactivos que los usuarios pueden completar para enviar elementos del catálogo y acciones personalizadas. También puede crear formularios de solo lectura que definan la información que los usuarios pueden ver en la vista de detalles de un elemento del catálogo o un recurso aprovisionado.

A medida que se van creando recursos personalizados de XaaS, blueprints de XaaS y acciones personalizadas, se generan formularios para los casos de uso habituales.

Tabla 3-59. Tipos de objeto y formularios asociados de XaaS

Tipo de objeto	Formulario predeterminado	Formularios adicionales
Recurso personalizado	Formulario de detalles de recursos basado en los atributos del tipo de inventario del complemento vRealize Orchestrator (solo lectura).	■ Ninguno
Blueprint de XaaS	Formulario de envío de solicitudes basado en la presentación del flujo de trabajo seleccionado.	■ Detalles de elementos del catálogo (solo lectura) ■ Detalles de solicitudes enviadas (solo lectura)
Acción personalizada	Formulario de envío de acciones basado en la presentación del flujo de trabajo seleccionado.	■ Detalles de acciones enviadas (solo lectura)

Puede modificar los formularios predeterminados y diseñar formularios nuevos. Puede arrastrar campos para agregarlos y reordenarlos en el formulario. Puede poner restricciones en los valores de ciertos campos, especificar valores predeterminados o proporcionar textos con instrucciones para el usuario final que vaya a completar el formulario.

Debido a sus diferentes finalidades, las operaciones que puede realizar para diseñar formularios de solo lectura están limitadas en comparación con las operaciones para diseñar formularios de envío.

Campos en el diseñador de formularios

La presentación y las funciones de los flujos de trabajo se pueden ampliar añadiendo nuevos campos predefinidos a los formularios generados predeterminados de las acciones personalizadas y los blueprints de XaaS.

En vRealize Automation, los parámetros de entrada definidos en el flujo de trabajo de vRealize Orchestrator aparecerán en el formulario generado predeterminado. En caso de que no quiera utilizar estos campos generados predeterminados del formulario, puede eliminarlos y luego arrastrar y colocar otros nuevos desde la paleta. Los campos generados predeterminados se pueden reemplazar sin romper las asignaciones del flujo de trabajo si utiliza el mismo identificador que el del campo que vaya a reemplazar.

También se pueden añadir campos nuevos distintos de los generados a partir de las entradas de flujo de trabajo de vRealize Orchestrator, lo que le permitirá ampliar la presentación y las funciones del flujo de trabajo en las siguientes situaciones:

- Añadir limitaciones a los campos existentes

Por ejemplo, puede crear un menú desplegable y llamarlo **dd**. También puede crear las opciones predefinidas Gold, Silver, Bronze y Personalizado. Si hay un campo predefinido, como CPU, puede añadirle las siguientes limitaciones:

- Si dd equivale a Gold, la CPU es de 2000 MHz
- Si dd equivale a Silver, la CPU es de 1000 MHz
- Si dd equivale a Bronze, la CPU es de 500 MHz
- Si dd equivale a Personalizado, el campo de CPU es editable y el consumidor puede especificar un valor personalizado

- Añadir definiciones de valores externos a campos

Puede añadir una definición de valor externo a un campo para, de este modo, poder ejecutar acciones de script de vRealize Orchestrator y proporcionar más información a los consumidores sobre los formularios que diseñe. Por ejemplo, puede que quiera crear un flujo de trabajo para cambiar la configuración de firewall de una máquina virtual. En la página de solicitud de acción personalizada, quiere dar a los usuarios la posibilidad de cambiar la configuración de puerto abierto, pero, al mismo tiempo, también quiere restringir las opciones de los puertos abiertos. Puede añadir una definición de valor externo a un campo de lista dual y seleccionar una acción de script de vRealize Orchestrator que realiza una consulta sobre los puertos abiertos. Cuando el formulario de solicitud se carga, la acción de script se ejecuta y los puertos abiertos se muestran como opciones al usuario.

- Añadir nuevos campos que se controlan en el flujo de trabajo de vRealize Orchestrator como parámetros globales

Por ejemplo, el flujo de trabajo proporciona una integración con un sistema de terceros y los parámetros de entrada definidos por el desarrollador del flujo de trabajo que se van a controlar en los casos generales, pero ofrece también una forma de pasar campos personalizados. Por ejemplo, en un cuadro de script, se controlan todos los parámetros globales que empiezan por **my3rdparty**. Así, si el arquitecto de XaaS quiere pasar valores específicos para que los consumidores los proporcionen, el arquitecto de XaaS puede añadir un campo nuevo llamado **my3rdparty_CPU**.

Tabla 3-60. Campos nuevos en el formulario de acción personalizada o de blueprint de XaaS

Campo	Descripción
Campo de texto	Cuadro de texto con una sola línea.
Área de texto	Cuadro de texto con varias líneas.
Vínculo	Campo en el que los consumidores introducen una URL. Se puede utilizar http, https, ftp, mailto o /. No se puede utilizar file://.
Correo electrónico	Campo en el que los consumidores escriben una dirección de correo electrónico.
Campo de contraseña	Campo en el que los consumidores escriben una contraseña.
Campo de valor entero	Cuadro de texto en el que los consumidores escriben un entero. Este campo se puede convertir en un control deslizante con valores mínimo y máximo, así como un incremento.
Campo de valor decimal	Cuadro de texto en el que los consumidores escriben un decimal. Este campo se puede convertir en un control deslizante con valores mínimo y máximo, así como un incremento.
Fecha y hora	Cuadros de texto en el que los consumidores indican una fecha (seleccionando una fecha de un menú de calendario) y una hora (mediante flechas arriba y abajo).
Lista dual	Un generador de lista en el que los consumidores mueven un conjunto predefinido de valores entre dos listas (la primera contiene todas las opciones sin seleccionar y la segunda, las que el usuario ha escogido).
Casilla de verificación	Casilla de verificación
Sí/No	Menú desplegable para seleccionar Sí o No
Lista desplegable	Menú desplegable
Lista	Lista
Lista de casillas	Lista de casillas
Grupo de botones de opción	Grupo de botones de opción
Buscar	Cuadro de texto de búsqueda que completa automáticamente la consulta y donde los consumidores seleccionan un objeto
Árbol	Árbol que los consumidores usan para desplazarse por los objetos disponibles y seleccionarlos
Mapa	Tabla de asignación que los consumidores usan para definir pares clave-valor relativos a propiedades

También puede usar el campo de formulario **Encabezado de sección** para dividir páginas del formulario en secciones con encabezados independientes, así como el campo de formulario **Texto** para añadir texto de carácter informativo de solo lectura.

Restricciones y valores del diseñador de formularios

Al editar un elemento del blueprint o formulario de acción personalizada, se pueden implementar diversas restricciones y valores en el elemento.

Restricciones

Las restricciones que se pueden implementar en un elemento varían en función del tipo de elemento que se esté editando o añadiendo al formulario. Es probable que algunos valores de las restricciones estén configurados en el flujo de trabajo de vRealize Orchestrator. Dichos valores no aparecen en la pestaña Restricciones porque a menudo dependen de condiciones que se evalúan cuando se ejecuta el flujo de trabajo. Los valores de restricciones que configure para el formulario de blueprint anulan las restricciones incluidas en el flujo de trabajo de vRealize Orchestrator.

Después de calcularlos para un campo, los enlaces mínimos y máximos solo se vuelven a calcular cuando se solicita un blueprint.

Por cada restricción que se implemente en relación con un elemento, se puede seleccionar una de las siguientes opciones para definir dicha restricción:

No establecido

Obtiene la propiedad de la presentación del flujo de trabajo de vRealize Orchestrator.

Constante

Establece el elemento que se está editando como obligatorio u opcional.

Campo

Enlaza el elemento con otro elemento del formulario. Por ejemplo, se puede establecer que el elemento solamente sea necesario cuando se seleccione otro elemento (como una casilla).

Condicional

Aplica una condición. Use estas condiciones para crear diversas cláusulas y expresiones y aplicarlas al estado o a las restricciones del elemento.

Externo

Seleccione una acción de script de vRealize Orchestrator que defina el valor.

Tabla 3-61. Restricciones del diseñador de formularios

Restricción	Descripción
Obligatoria	Indica si el elemento es obligatorio.
Solo lectura	Indica si el campo es de solo lectura.
Valor	Establece un valor para el elemento.

Tabla 3-61. Restricciones del diseñador de formularios (continuación)

Restricción	Descripción
Visible	<p>Indica si el consumidor va a poder ver el elemento.</p> <p>Si aplica una restricción de visibilidad a un grupo de visualización en el flujo de trabajo vRealize Orchestrator, dicha restricción se omite en el formulario de detalles de solicitud enviados de XaaS y los campos que quiere que estén ocultos aparecen en el formulario.</p> <p>Para ocultar campos que no desea que aparezcan en el formulario de detalles de solicitud enviados, y que no sean necesarios para el usuario solicitante, elimine los campos del formulario de detalles de solicitud enviados en la pestaña del formulario de blueprint del diseñador de blueprints de XaaS. Para encontrar esta pestaña, consulte Añadir un nuevo formulario de blueprint XaaS.</p>
Longitud mínima	Establece una cantidad mínima de caracteres para el elemento de entrada de cadena.
Longitud máxima	Establece un número máximo permitido de caracteres para el elemento de entrada de cadena.
Valor mínimo	Establece un valor mínimo para el elemento de entrada de número.
Valor máximo	Establece un valor máximo para el elemento de entrada de número.
Incremento	Establece un incremento para un elemento como un campo Decimal o Entero . Por ejemplo, cuando quiera usar un campo Entero para que se represente como un Control deslizante , puede usar el valor del paso.
Cantidad mínima	<p>Establece un recuento mínimo de elementos que se pueden seleccionar.</p> <p>Por ejemplo, cuando añada o edite una Lista de casillas, puede establecer el número mínimo de casillas que el consumidor debe seleccionar para continuar.</p>
Cantidad máxima	<p>Establece un recuento máximo de elementos que se pueden seleccionar.</p> <p>Por ejemplo, cuando añada o edite una Lista de casillas, puede establecer el número máximo de casillas que el consumidor debe seleccionar para continuar.</p>

Valores

Se pueden aplicar valores a algunos de los elementos y definir lo que los consumidores van a ver en algunos de los campos. Las opciones disponibles dependen del tipo de elemento que se esté editando o añadiendo al formulario.

Tabla 3-62. Valores del diseñador de formularios

Valor	Descripción
No establecido	Establece el valor del elemento que se está editando de la presentación del flujo de trabajo de vRealize Orchestrator.
Valores predefinidos	Seleccione valores de una lista de objetos relacionados del inventario de vRealize Orchestrator.

Tabla 3-62. Valores del diseñador de formularios (continuación)

Valor	Descripción
Valor	Define un valor personalizado estático con etiquetas.
Valores externos	Seleccione una acción de script de vRealize Orchestrator que defina el valor con información que no queda expuesta directamente mediante el flujo de trabajo.

Definiciones de valores externos en el diseñador de formularios

Cuando se editan algunos elementos en el diseñador de formularios, puede asignar definiciones de valores externos que usan acciones de script de vRealize Orchestrator personalizadas para proporcionar información que el flujo de trabajo no expone directamente.

Por ejemplo, puede que quiera publicar una acción personalizada para instalar software en una máquina aprovisionada. En lugar de proporcionar al consumidor una lista estática con todo el software disponible para descargar, puede rellenar esa lista dinámicamente con software que sea relevante para el sistema operativo de la máquina, software que el usuario no haya instalado en la máquina con anterioridad o software que está obsoleto en la máquina y tiene que actualizarse.

Para proporcionar contenido dinámico personalizado para el consumidor, hay que crear una acción de script de vRealize Orchestrator que recupere la información que quiera que aparezca a los consumidores. Esta acción de script se asigna a un campo del diseñador de formularios como una definición de valor externo. Cuando el formulario de blueprint de servicio o recurso se muestra a los consumidores, la acción de script recupera la información personalizada y la muestra.

Puede usar definiciones de valores externos para proporcionar valores predeterminados o de solo lectura, para crear expresiones booleanas, para definir restricciones o para ofrecer opciones a los consumidores que les permitan seleccionar casillas, elementos de listas, etc.

Si se crea un blueprint con un flujo de trabajo que incluye un campo obligatorio, es obligatorio en el formulario de solicitud, incluso si se establece como no obligatorio.

Trabajar con el diseñador de formularios

Cuando crea blueprints, acciones personalizadas y recursos personalizados XaaS, puede editar los formularios de los blueprints, las acciones y los recursos con el diseñador de formularios. Puede editar la representación y definir lo que los consumidores del elemento o la acción verán cuando soliciten el elemento del catálogo o ejecuten la operación posterior al aprovisionamiento.

De forma predeterminada, cualquier formulario de blueprint, acción personalizada o recurso personalizado XaaS se genera basándose en la presentación del flujo de trabajo en vRealize Orchestrator.

Los pasos de la presentación de vRealize Orchestrator se representan como páginas de formulario y los grupos de presentaciones de vRealize Orchestrator se representan como secciones independientes. Los tipos de entrada del flujo de trabajo seleccionado se muestran como campos diversos en el formulario. Por ejemplo, el tipo de vRealize Orchestrator string se representa mediante un cuadro de texto. Un tipo complejo como VC:VirtualMachine se representa mediante un cuadro de búsqueda o un árbol, de forma que los clientes puedan escribir un valor alfanumérico para buscar una máquina virtual o examinar para seleccionar una máquina virtual.

Create cluster - Editar blueprint

Puede editar el modo en que se representa un objeto en el diseñador de formularios. Por ejemplo, puede editar la representación VC:VirtualMachine predeterminada y convertirla en un árbol en lugar de un cuadro de búsqueda. También puede añadir campos nuevos como casillas o menús desplegables, y aplicar diversas restricciones. Si los campos nuevos que añada no son válidos o no están correctamente asignados a las entradas de flujo de trabajo de vRealize Orchestrator, cuando el consumidor ejecute el flujo de trabajo, vRealize Orchestrator omitirá los campos no válidos o no asignados.

Diseñar un formulario de recurso personalizado

Al aprovisionar un recurso personalizado, todos los campos del formulario de detalles del recurso se muestran al consumidor como de solo lectura en la página Detalles del elemento. Se pueden realizar operaciones de edición básicas, como eliminar, modificar o reordenar los campos, o se pueden añadir nuevos campos definidos externamente que usan acciones de script de vRealize Orchestrator para suministrar más información de solo lectura a los consumidores.

- [Editar un elemento de recurso personalizado](#)

Algunas de las características de un elemento se pueden editar en la página Formulario de detalles del recurso personalizado. Cada campo predeterminado de la página representa una propiedad del recurso personalizado. No se puede modificar el tipo de una propiedad ni los valores predeterminados, pero sí el nombre, el tamaño y la descripción.

- [Añadir una nueva página del formulario de recursos personalizados](#)

Puede añadir una nueva página para reorganizar el formulario en varias pestañas.

- [Insertar un encabezado de sección en un formulario de recurso personalizado](#)

Puede insertar un encabezado de sección para dividir el formulario en dos secciones.

- [Insertar un elemento de texto en un formulario de recurso personalizado](#)

Puede insertar un cuadro de texto para añadir información descriptiva al formulario.

- [Insertar un campo definido externamente en un formulario de recurso personalizado](#)

Puede insertar un campo nuevo y asignarle una definición de valor externo para proporcionar dinámicamente información de solo lectura que los consumidores verán en la página de detalles de un elemento cuando aprovisionen un recurso personalizado.

Editar un elemento de recurso personalizado

Algunas de las características de un elemento se pueden editar en la página Formulario de detalles del recurso personalizado. Cada campo predeterminado de la página representa una propiedad del recurso personalizado. No se puede modificar el tipo de una propiedad ni los valores predeterminados, pero sí el nombre, el tamaño y la descripción.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Añadir un recurso personalizado de XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Recursos personalizados**.

- 2 Haga clic en el recurso personalizado para editarlo.
- 3 Haga clic en la pestaña **Formulario de detalles**.
- 4 Seleccione el elemento que quiera editar y haga clic en el icono **Editar**.
- 5 Escriba un nombre nuevo del campo en el cuadro de texto **Etiqueta** para cambiar la etiqueta.
- 6 Edite la descripción en el cuadro de texto **Descripción**.
- 7 Seleccione una opción del menú desplegable **Tamaño** para cambiar el tamaño del elemento.
- 8 Seleccione una opción del menú desplegable **Tamaño de etiqueta** para cambiar el tamaño de la etiqueta.
- 9 Haga clic en **Enviar**.
- 10 Haga clic en **Finalizar**.

Añadir una nueva página del formulario de recursos personalizados

Puede añadir una nueva página para reorganizar el formulario en varias pestañas.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Añadir un recurso personalizado de XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Recursos personalizados**.
- 2 Haga clic en el recurso personalizado para editarlo.
- 3 Haga clic en la pestaña **Formulario de detalles**.
- 4 Haga clic en el icono **Página nueva** (+) junto al nombre de la **página de formulario**.
- 5 Seleccione el tipo de pantalla que no se utiliza y haga clic en **Enviar**.

Si ya dispone de una vista de detalles del recurso o de lista de recursos, no podrá crear dos del mismo tipo.

- 6 Haga clic en **Enviar**.
- 7 Configure el formulario.
- 8 Haga clic en **Finalizar**.

Resultados

Puede eliminar algunos de los elementos de la página del formulario original e insertarlos en la nueva página del formulario, o bien puede añadir campos nuevos con definiciones de valores externos que ofrezcan a los consumidores información que no quede expuesta directamente mediante el flujo de trabajo de vRealize Orchestrator.

Insertar un encabezado de sección en un formulario de recurso personalizado

Puede insertar un encabezado de sección para dividir el formulario en dos secciones.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Añadir un recurso personalizado de XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Recursos personalizados**.
- 2 Haga clic en el recurso personalizado para editarlo.
- 3 Haga clic en la pestaña **Formulario de detalles**.
- 4 Arrastre el elemento **Encabezado de sección** del panel Formulario al panel Página de formulario.
- 5 Escriba un nombre para la sección.
- 6 Haga clic fuera del elemento para guardar los cambios.
- 7 Haga clic en **Finalizar**.

Insertar un elemento de texto en un formulario de recurso personalizado

Puede insertar un cuadro de texto para añadir información descriptiva al formulario.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Añadir un recurso personalizado de XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Recursos personalizados**.
- 2 Haga clic en el recurso personalizado para editarlo.
- 3 Haga clic en la pestaña **Formulario de detalles**.
- 4 Arrastre el elemento **Texto** del panel Formulario al panel Página de formulario.
- 5 Escriba el texto que desee añadir.
- 6 Haga clic fuera del elemento para guardar los cambios.
- 7 Haga clic en **Finalizar**.

Insertar un campo definido externamente en un formulario de recurso personalizado

Puede insertar un campo nuevo y asignarle una definición de valor externo para proporcionar dinámicamente información de solo lectura que los consumidores verán en la página de detalles de un elemento cuando aprovisionen un recurso personalizado.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Añadir un recurso personalizado de XaaS](#).

- Desarrolle o importe una acción de script de vRealize Orchestrator para obtener la información que quiera ofrecer a los consumidores.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Recursos personalizados**.
- 2 Haga clic en el recurso personalizado para editarlo.
- 3 Haga clic en la pestaña **Formulario de detalles**.
- 4 Arrastre un elemento del panel Campos nuevos y suéltelo en el panel Página de formulario.
- 5 Escriba el identificador del elemento en el cuadro de texto **ID**.
- 6 Especifique una etiqueta en el cuadro de texto **Etiqueta**.
Los consumidores ven las etiquetas en los formularios.
- 7 (opcional) Seleccione un tipo para el campo en el menú desplegable **Tipo**.
- 8 Escriba el tipo de resultado de su acción de script de vRealize Orchestrator en el cuadro de búsqueda **Tipo de entidad** y presione Entrar.
Por ejemplo, si quiere usar una acción de script para mostrar el usuario actual y el script devuelve un tipo de resultado de vRealize OrchestratorLdapUser, escriba **LdapUser** en el cuadro de búsqueda **Tipo de entidad** y presione Entrar.
- 9 Haga clic en **Añadir valor externo**.
- 10 Seleccione su acción de script de vRealize Orchestrator personalizada.
- 11 Haga clic en **Enviar**.
- 12 Haga clic en **Enviar** otra vez.
- 13 Haga clic en **Finalizar**.

Resultados

Cuando el formulario se muestra a los consumidores, la acción de script recupera la información personalizada y la muestra.

Diseñar un formulario de blueprint de XaaS

Al crear un blueprint de XaaS, puede editar el formulario del blueprint incluyendo en él nuevos campos, o bien modificando, reordenando o eliminando los ya existentes. También puede crear formularios y páginas de formulario, así como arrastrar y colocar en ellos nuevos campos.

- [Añadir un nuevo formulario de blueprint XaaS](#)

Al editar el formulario que se genera de forma predeterminada en un flujo de trabajo que desea publicar como un blueprint XaaS, puede añadir un nuevo formulario de blueprint XaaS.

- [Editar un elemento blueprint de XaaS](#)

Algunas de las características de un elemento se pueden editar en la página Formulario de blueprint de un blueprint de XaaS. Puede modificar el tipo de un elemento y sus valores predeterminados, así como aplicar diversas restricciones y valores.

- [Añadir un nuevo elemento](#)

Cuando edite el formulario generado de forma predeterminada de un blueprint XaaS, podrá añadir un nuevo elemento predefinido al formulario. Por ejemplo, si no desea utilizar un campo generado de forma predeterminada, puede eliminarlo y reemplazarlo por otro nuevo.

- [Insertar un encabezado de sección en un formulario de blueprint de XaaS](#)

Puede insertar un encabezado de sección para dividir el formulario en dos secciones.

- [Añadir un elemento de texto a un formulario de blueprint XaaS](#)

Puede insertar un cuadro de texto para añadir información descriptiva al formulario.

Añadir un nuevo formulario de blueprint XaaS

Al editar el formulario que se genera de forma predeterminada en un flujo de trabajo que desea publicar como un blueprint XaaS, puede añadir un nuevo formulario de blueprint XaaS.

Al añadir un nuevo formulario de blueprint XaaS, define el aspecto de las páginas de detalles del elemento del catálogo y de detalles de solicitud enviados. Si no añade formularios de detalles del elemento del catálogo y de detalles de solicitud enviados, el consumidor verá lo que se haya definido en el formulario de solicitud.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Añadir un blueprint XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Blueprints XaaS**.
- 2 Haga clic en el blueprint XaaS que desee editar.
- 3 Haga clic en la pestaña **Formulario de blueprint**.
- 4 Haga clic en el icono **Formulario nuevo** (+).
- 5 Especifique un nombre y, opcionalmente, una descripción.

6 Seleccione el tipo de pantalla en el menú **Tipo de pantalla**.

Opción	Descripción
Detalles del elemento del catálogo	Una página de detalles del elemento del catálogo que los consumidores ven al hacer clic en un elemento del catálogo.
Formulario de solicitud	El formulario de blueprint XaaS predeterminado. Los consumidores ven el formulario de solicitud cuando solicitan el elemento del catálogo.
Detalles de solicitud enviados	Una página de detalles de la solicitud que los consumidores ven cuando solicitan el elemento y deciden ver los detalles de la solicitud en la pestaña Solicitud .

7 Haga clic en **Enviar**.

Pasos siguientes

Puede añadir todos los campos que desee arrastrándolos desde el panel Campos nuevos hasta el panel Página de formulario.


Editar un elemento blueprint de XaaS

Algunas de las características de un elemento se pueden editar en la página Formulario de blueprint de un blueprint de XaaS. Puede modificar el tipo de un elemento y sus valores predeterminados, así como aplicar diversas restricciones y valores.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Añadir un blueprint XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Blueprints XaaS**.
- 2 Haga clic en el blueprint XaaS que desee editar.
- 3 Haga clic en la pestaña **Formulario de blueprint**.
- 4 Busque el elemento que desee editar.
- 5 Haga clic en el icono **Editar** (.
- 6 Escriba un nombre para el campo en el cuadro de texto **Etiqueta** para cambiar la etiqueta que ven los consumidores.
- 7 Edite la descripción en el cuadro de texto **Descripción**.
- 8 Seleccione una opción del menú desplegable **Tipo** para cambiar el tipo de visualización del elemento.

Las opciones varían en función del tipo de elemento que edite.

- 9 Seleccione una opción del menú desplegable **Tamaño** para cambiar el tamaño del elemento.

- 10** Seleccione una opción del menú desplegable **Tamaño de etiqueta** para cambiar el tamaño de la etiqueta.
- 11** Edite el valor predeterminado del elemento.

Opción	Descripción
No establecido	Obtiene el valor del elemento que está editando de la presentación de flujos de trabajo de vRealize Orchestrator.
Constante	Establece el valor predeterminado del elemento que está editando en un valor de constante que especifique.
Campo	Enlaza el valor predeterminado del elemento a un parámetro de otro elemento de la representación.
Condicional	Aplica una condición. El uso de condiciones le permite crear diversas cláusulas y expresiones, y aplicarlas a un elemento.
Externo	Seleccione una acción de script de vRealize Orchestrator para definir el valor.

- 12** Aplique restricciones al elemento en la pestaña **Restricciones**.

Opción	Descripción
No establecido	Obtiene el valor del elemento que está editando de la presentación de flujos de trabajo de vRealize Orchestrator.
Constante	Establece el valor predeterminado del elemento que está editando en un valor de constante que especifique.
Campo	Enlaza el valor predeterminado del elemento a un parámetro de otro elemento de la representación.
Condicional	Aplica una condición. El uso de condiciones le permite crear diversas cláusulas y expresiones, y aplicarlas a un elemento.
Externo	Seleccione una acción de script de vRealize Orchestrator para definir el valor.

- 13** Añada uno o varios valores para el elemento en la pestaña **Valores**.

Las opciones disponibles dependen del tipo de elemento que edite.

Opción	Descripción
No establecido	Obtiene el valor del elemento que está editando de la presentación de flujos de trabajo de vRealize Orchestrator.
Valores predefinidos	<p>Seleccione valores de una lista de objetos relacionados del inventario de vRealize Orchestrator.</p> <ul style="list-style-type: none"> a Escriba un valor en el cuadro de búsqueda Valores predefinidos para buscar en el inventario de vRealize Orchestrator. b Seleccione un valor en los resultados de la búsqueda y presione Entrar.

Opción	Descripción
Valor	<p>Defina valores personalizados con etiquetas.</p> <ol style="list-style-type: none"> Escriba un valor en el cuadro de texto Valor. Especifique una etiqueta para el valor en el cuadro de texto Etiqueta. Haga clic en el icono Añadir (+).
Valores externos	<p>Seleccione una acción de script de vRealize Orchestrator para definir el valor con información que no queda expuesta directamente mediante el flujo de trabajo.</p> <ul style="list-style-type: none"> ■ Seleccione Añadir valor externo. ■ Seleccione su acción de script de vRealize Orchestrator. ■ Haga clic en Enviar.

14 Haga clic en **Enviar**.

15 Haga clic en **Finalizar**.

Añadir un nuevo elemento

Cuando edite el formulario generado de forma predeterminada de un blueprint XaaS, podrá añadir un nuevo elemento predefinido al formulario. Por ejemplo, si no desea utilizar un campo generado de forma predeterminada, puede eliminarlo y reemplazarlo por otro nuevo.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Añadir un blueprint XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Blueprints XaaS**.
- 2 Haga clic en el blueprint XaaS que desee editar.
- 3 Haga clic en la pestaña **Formulario de blueprint**.
- 4 Arrastre un elemento del panel Campos nuevos y suéltelo en el panel Página de formulario.
- 5 Escriba el identificador de un parámetro de entrada de flujo de trabajo en el cuadro de texto **ID**.
- 6 Especifique una etiqueta en el cuadro de texto **Etiqueta**.
Los consumidores ven las etiquetas en los formularios.
- 7 (opcional) Seleccione un tipo para el campo en el menú desplegable **Tipo**.

- 8 Introduzca un objeto de vRealize Orchestrator en el cuadro de texto **Tipo de entidad** y presione Entrar.

Este paso no es necesario en todos los tipos de campos.

Opción	Descripción
Tipo de resultado	Si utiliza una acción de script para definir un valor externo para el campo, introduzca el tipo de resultado de su acción de script de vRealize Orchestrator.
Parámetro de entrada	Si utiliza el campo para aceptar la entrada del consumidor y devolver parámetros a vRealize Orchestrator, introduzca el tipo del parámetro de entrada aceptado por el flujo de trabajo de vRealize Orchestrator.
Parámetro de salida	Si utiliza el campo para mostrar información a los consumidores, introduzca el tipo del parámetro de salida del flujo de trabajo de vRealize Orchestrator.

- 9 (opcional) Active la casilla **Valores múltiples** para permitir a los consumidores seleccionar más de un objeto.

Esta opción no está disponible en todos los tipos de campos.

- 10 Haga clic en **Enviar**.

- 11 Haga clic en **Actualizar**.

Pasos siguientes

Puede editar el elemento para cambiar la configuración predeterminada y aplicar diversos valores o restricciones.

Insertar un encabezado de sección en un formulario de blueprint de XaaS

Puede insertar un encabezado de sección para dividir el formulario en dos secciones.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Añadir un blueprint XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Blueprints XaaS**.
- 2 Haga clic en el blueprint XaaS que desee editar.
- 3 Haga clic en la pestaña **Formulario de blueprint**.
- 4 Arrastre el elemento **Encabezado de sección** del panel Formulario al panel Página de formulario.
- 5 Escriba un nombre para la sección.
- 6 Haga clic fuera del elemento para guardar los cambios.
- 7 Haga clic en **Actualizar**.

Añadir un elemento de texto a un formulario de blueprint XaaS

Puede insertar un cuadro de texto para añadir información descriptiva al formulario.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Añadir un blueprint XaaS](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Blueprints XaaS**.
- 2 Haga clic en el blueprint XaaS que desee editar.
- 3 Haga clic en la pestaña **Formulario de blueprint**.
- 4 Arrastre el elemento **Texto** del panel Campos nuevos al panel Página de formulario.
- 5 Escriba el texto que desee añadir.
- 6 Haga clic fuera del elemento para guardar los cambios.
- 7 Haga clic en **Actualizar**.

Diseñar un formulario de acción personalizada

Al crear una acción personalizada, puede editar el formulario de la acción incluyendo en él nuevos campos, o bien modificando, reordenando o eliminando los ya existentes. También puede crear formularios y páginas de formulario, así como arrastrar y colocar en ellos nuevos campos.

Añadir un nuevo formulario de acción personalizada

Al editar el formulario que se genera de forma predeterminada en un flujo de trabajo que desea publicar como una acción personalizada, puede añadir un nuevo formulario de acción personalizada.

Al añadir un nuevo formulario de acción personalizada, define el aspecto que tendrá la página de detalles de la acción enviados. Si no añade un formulario de detalles de la acción enviados, el consumidor verá lo que se haya definido en el formulario de acción.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Crear una acción personalizada](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Haga clic en la acción personalizada que desee editar.
- 3 Haga clic en la pestaña **Formulario**.
- 4 Haga clic en el icono **Formulario nuevo (+)**.
- 5 Especifique un nombre y, opcionalmente, una descripción.

6 Seleccione el tipo de pantalla en el menú **Tipo de pantalla**.

Opción	Descripción
Formulario de acción	El formulario de acción personalizada predeterminado que los consumidores ven cuando deciden ejecutar la acción posterior al aprovisionamiento.
Detalles de la acción enviados	Una página de detalles de la solicitud que los consumidores ven cuando solicitan la acción y deciden ver los detalles de la solicitud en la pestaña Solicitud .

7 Haga clic en **Enviar**.

Pasos siguientes

Puede añadir todos los campos que desee arrastrándolos desde el panel Campos nuevos hasta el panel Página de formulario.

Añadir un nuevo elemento a un formulario de acción personalizada

Cuando edite el formulario generado de forma predeterminada de una acción personalizada, podrá añadir un nuevo elemento predefinido al formulario. Por ejemplo, si no desea utilizar un campo generado de forma predeterminada, puede eliminarlo y reemplazarlo por otro nuevo.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Crear una acción personalizada](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Haga clic en la acción personalizada que desee editar.
- 3 Haga clic en la pestaña **Formulario**.
- 4 Arrastre un elemento del panel Campos nuevos y suéltelo en el panel Página de formulario.
- 5 Escriba el identificador de un parámetro de entrada de flujo de trabajo en el cuadro de texto **ID**.
- 6 Especifique una etiqueta en el cuadro de texto **Etiqueta**.
Los consumidores ven las etiquetas en los formularios.
- 7 (opcional) Seleccione un tipo para el campo en el menú desplegable **Tipo**.

- 8 Introduzca un objeto de vRealize Orchestrator en el cuadro de texto **Tipo de entidad** y presione Entrar.

Este paso no es necesario en todos los tipos de campos.

Opción	Descripción
Tipo de resultado	Si utiliza una acción de script para definir un valor externo para el campo, introduzca el tipo de resultado de su acción de script de vRealize Orchestrator.
Parámetro de entrada	Si utiliza el campo para aceptar la entrada del consumidor y devolver parámetros a vRealize Orchestrator, introduzca el tipo del parámetro de entrada aceptado por el flujo de trabajo de vRealize Orchestrator.
Parámetro de salida	Si utiliza el campo para mostrar información a los consumidores, introduzca el tipo del parámetro de salida del flujo de trabajo de vRealize Orchestrator.

- 9 (opcional) Active la casilla **Valores múltiples** para permitir a los consumidores seleccionar más de un objeto.

Esta opción no está disponible en todos los tipos de campos.

- 10 Haga clic en **Enviar**.

- 11 Haga clic en **Finalizar**.

Pasos siguientes

Puede editar el elemento para cambiar la configuración predeterminada y aplicar diversos valores o restricciones.

Editar un elemento de acción personalizada

Algunas de las características de un elemento se pueden editar en la página Formulario de la acción personalizada. Puede modificar el tipo de un elemento y sus valores predeterminados, así como aplicar diversas restricciones y valores.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Crear una acción personalizada](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Haga clic en la acción personalizada que desee editar.
- 3 Haga clic en la pestaña **Formulario**.
- 4 Busque el elemento que desee editar.
- 5 Haga clic en el icono **Editar** (✎).
- 6 Escriba un nombre para el campo en el cuadro de texto **Etiqueta** para cambiar la etiqueta que ven los consumidores.

7 Edite la descripción en el cuadro de texto **Descripción**.

8 Seleccione una opción del menú desplegable **Tipo** para cambiar el tipo de visualización del elemento.

Las opciones varían en función del tipo de elemento que edite.

9 Seleccione una opción del menú desplegable **Tamaño** para cambiar el tamaño del elemento.

10 Seleccione una opción del menú desplegable **Tamaño de etiqueta** para cambiar el tamaño de la etiqueta.

11 Edite el valor predeterminado del elemento.

Opción	Descripción
No establecido	Obtiene el valor del elemento que está editando de la presentación de flujos de trabajo de vRealize Orchestrator.
Constante	Establece el valor predeterminado del elemento que está editando en un valor de constante que especifique.
Campo	Enlaza el valor predeterminado del elemento a un parámetro de otro elemento de la representación.
Condicional	Aplica una condición. El uso de condiciones le permite crear diversas cláusulas y expresiones, y aplicarlas a un elemento.
Externo	Seleccione una acción de script de vRealize Orchestrator para definir el valor.

12 Aplique restricciones al elemento en la pestaña **Restricciones**.

Opción	Descripción
No establecido	Obtiene el valor del elemento que está editando de la presentación de flujos de trabajo de vRealize Orchestrator.
Constante	Establece el valor predeterminado del elemento que está editando en un valor de constante que especifique.
Campo	Enlaza el valor predeterminado del elemento a un parámetro de otro elemento de la representación.
Condicional	Aplica una condición. El uso de condiciones le permite crear diversas cláusulas y expresiones, y aplicarlas a un elemento.
Externo	Seleccione una acción de script de vRealize Orchestrator para definir el valor.

13 Añada uno o varios valores para el elemento en la pestaña **Valores**.

Las opciones disponibles dependen del tipo de elemento que edite.

Opción	Descripción
No establecido	Obtiene el valor del elemento que está editando de la presentación de flujos de trabajo de vRealize Orchestrator.
Valores predefinidos	<p>Seleccione valores de una lista de objetos relacionados del inventario de vRealize Orchestrator.</p> <ul style="list-style-type: none"> a Escriba un valor en el cuadro de búsqueda Valores predefinidos para buscar en el inventario de vRealize Orchestrator. b Seleccione un valor en los resultados de la búsqueda y presione Entrar.
Valor	<p>Defina valores personalizados con etiquetas.</p> <ul style="list-style-type: none"> a Escriba un valor en el cuadro de texto Valor. b Especifique una etiqueta para el valor en el cuadro de texto Etiqueta. c Haga clic en el icono Añadir (+).
Valores externos	<p>Seleccione una acción de script de vRealize Orchestrator para definir el valor con información que no queda expuesta directamente mediante el flujo de trabajo.</p> <ul style="list-style-type: none"> ■ Seleccione Añadir valor externo. ■ Seleccione su acción de script de vRealize Orchestrator. ■ Haga clic en Enviar.

14 Haga clic en **Enviar**.**15** Haga clic en **Actualizar**.

Insertar un encabezado de sección en un formulario de acción personalizada

Puede insertar un encabezado de sección para dividir el formulario en dos secciones.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Crear una acción personalizada](#).

Procedimiento

- 1** Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2** Haga clic en la acción personalizada que desee editar.
- 3** Haga clic en la pestaña **Formulario**.
- 4** Arrastre el elemento **Encabezado de sección** del panel Formulario al panel Página de formulario.
- 5** Escriba un nombre para la sección.
- 6** Haga clic fuera del elemento para guardar los cambios.
- 7** Haga clic en **Finalizar**.

Añadir un elemento de texto a un formulario de acción personalizada

Puede insertar un cuadro de texto para añadir información descriptiva al formulario.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [Crear una acción personalizada](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Haga clic en la acción personalizada que desee editar.
- 3 Haga clic en la pestaña **Formulario**.
- 4 Arrastre el elemento **Texto** del panel Campos nuevos al panel Página de formulario.
- 5 Escriba el texto que desee añadir.
- 6 Haga clic fuera del elemento para guardar los cambios.
- 7 Haga clic en **Finalizar**.

Ejemplos y escenarios de XaaS

Con los ejemplos y escenarios, se ofrecen formas en que puede usar vRealize Automation para llevar a cabo tareas habituales con blueprints y acciones personalizadas XaaS.

Crear un blueprint y acción de XaaS para crear y modificar un usuario

Mediante el uso de XaaS, puede crear y publicar un elemento del catálogo para el aprovisionamiento de un usuario en un grupo. También puede asociar una nueva operación posaprovisionamiento al usuario aprovisionado. Por ejemplo, una operación que permita a los usuarios del catálogo de servicios cambiar la contraseña de usuario.

Como arquitecto XaaS, crea un recurso personalizado y un blueprint XaaS, y publica un elemento del catálogo para crear un usuario. También crea una acción personalizada para cambiar la contraseña del usuario.

Como administrador del catálogo, crea un servicio e incluye en este el elemento de catálogo de blueprint. Además, edita la presentación del flujo de trabajo del elemento del catálogo mediante la utilización del diseñador de formularios y cambia el modo en que los consumidores ven el formulario de solicitud.

Como administrador de grupo empresarial o administrador de tenants, autoriza el recién creado servicio, elemento del catálogo y acción personalizada a un consumidor.

Requisitos previos

Compruebe que el complemento Active Directory está correctamente configurado y que tiene los derechos para crear usuarios en Active Directory.

Procedimiento

1 Crear un usuario de prueba como un recurso personalizado

Puede crear un recurso personalizado y asignarlo al tipo de objeto AD:User de vRealize Orchestrator.

2 Crear un blueprint XaaS para crear un usuario

Puede crear el blueprint XaaS Crear un usuario en un grupo para poder ejecutar el flujo de trabajo que añade un usuario de Active Directory y lo asigna a un grupo de Active Directory. Puede crear el blueprint como blueprint XaaS independiente o como componente de blueprint. En este ejemplo, se crea un blueprint independiente.

3 Crear una acción personalizada para cambiar una contraseña de usuario

Se puede crear una acción personalizada para permitir que los consumidores de XaaS puedan crear un blueprint de usuario para cambiar la contraseña del consumidor después de aprovisionar a ese usuario.

4 Crear un servicio y añadirle un blueprint Crear un usuario de prueba

Puede crear un servicio para mostrar el elemento de catálogo Crear un usuario en el catálogo de servicios.

5 Autorizar el servicio y la acción personalizada a un consumidor

Los administradores de grupo empresarial y los administradores de tenant pueden autorizar el servicio y la acción personalizada a un usuario o un grupo de usuarios. Una vez autorizados, pueden ver el servicio en su catálogo y solicitar el elemento del catálogo Crear un usuario de prueba que se incluye en el servicio. Después de que los consumidores aprovisionen el elemento, pueden pedir que se cambie la contraseña de usuario.

Crear un usuario de prueba como un recurso personalizado

Puede crear un recurso personalizado y asignarlo al tipo de objeto AD:User de vRealize Orchestrator.

Requisitos previos

Inicie sesión en vRealize Automation como **arquitecto XaaS**.

Procedimiento

1 Seleccione **Diseño > XaaS > Recursos personalizados**.

2 Haga clic en el icono **Nuevo** (+).

3 En el cuadro de texto **Tipo de orquestador**, escriba **AD:User** y pulse Entrar.

4 Seleccione **AD:User** en la lista.

- 5 Escriba un nombre para el recurso.

Por ejemplo, **Usuario de prueba**.

- 6 Escriba una descripción para el recurso.

Por ejemplo,

Este es un recurso personalizado de prueba que utilizaré en mi elemento de catálogo para crear un usuario en un grupo.

- 7 Haga clic en **Siguiente**.

- 8 No modifique los valores predeterminados del formulario.

- 9 Haga clic en **Finalizar**.

Resultados

Ha creado un recurso personalizado llamado Usuario de prueba, recurso que ahora aparece recogido en la página Recursos personalizados.

Pasos siguientes

Cree un blueprint de XaaS.

Crear un blueprint XaaS para crear un usuario

Puede crear el blueprint XaaS Crear un usuario en un grupo para poder ejecutar el flujo de trabajo que añade un usuario de Active Directory y lo asigna a un grupo de Active Directory. Puede crear el blueprint como blueprint XaaS independiente o como componente de blueprint. En este ejemplo, se crea un blueprint independiente.

Requisitos previos

- Verifique que crea una acción personalizada que sea compatible con el aprovisionamiento de usuarios de Active Directory. Consulte [Crear un usuario de prueba como un recurso personalizado](#).
- Inicie sesión en vRealize Automation como **arquitecto XaaS**.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Blueprints XaaS**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 En el panel Seleccione un flujo de trabajo, desplácese hasta **Orchestrator > Biblioteca > Microsoft > Active Directory > Usuario** y seleccione el flujo de trabajo **Crear un usuario en un grupo**.
- 4 Haga clic en **Siguiente**.

5 Configure las opciones de la pestaña **General**.

- a Cambie el nombre del blueprint a **Crear un usuario de prueba** y deje la descripción tal cual.
- b Desactive la casilla de verificación **Facilitar como un componente en el lienzo de diseño**.

Este blueprint se publicará directamente en el catálogo de servicios en vez de usarlo como componente de blueprint en el lienzo de diseño. No es necesario que configure ningún flujo de trabajo de escalado vertical u horizontal.

La pestaña **Ciclo de vida del componente** se quita de la interfaz de usuario.

6 Haga clic en **Siguiente**.**7** Edite el formulario del blueprint.

- a Haga clic en **El nombre de dominio en el formulario de Win2000**.
- b Haga clic en la pestaña **Restricciones**.
- c Haga clic en la flecha desplegable **Valor**, seleccione **Constante** en el menú desplegable y escriba **test.domain**.
- d Haga clic en la flecha desplegable **Visible**, seleccione **Constante** del menú desplegable y, a continuación, seleccione **No** del menú desplegable.

De este modo, el nombre de dominio no estará visible para el consumidor del elemento de catálogo.

- e Haga clic en **Aplicar** para guardar los cambios.

8 Haga clic en **Siguiente**.**9** Seleccione **newUser [Usuario de prueba]** como parámetro de salida que se va a aprovisionar.**10** Haga clic en **Siguiente**.**11** Haga clic en **Finalizar**.**12** En la página **Blueprints XaaS**, seleccione la fila **Crear un usuario de prueba** y haga clic en **Publicar**.**Resultados**

Ha generado un blueprint que permite crear un usuario de prueba y ha hecho que el blueprint se pueda añadir a un servicio.

Pasos siguientes

Cree una acción para ejecutarla en la cuenta de usuario aprovisionada. Consulte [Crear una acción personalizada para cambiar una contraseña de usuario](#).

Crear una acción personalizada para cambiar una contraseña de usuario

Se puede crear una acción personalizada para permitir que los consumidores de XaaS puedan crear un blueprint de usuario para cambiar la contraseña del consumidor después de aprovisionar a ese usuario.

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto XaaS**.
- Verifique que crea una acción personalizada que sea compatible con el aprovisionamiento de usuarios de Active Directory. Consulte [Crear un usuario de prueba como un recurso personalizado](#).

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Vaya a **Orchestrator > Biblioteca > Microsoft > Active Directory > Usuario** en la biblioteca de flujos de trabajo de vRealize Orchestrator y seleccione el flujo de trabajo **Cambiar una contraseña de usuario**.
- 4 Haga clic en **Siguiente**.
- 5 Seleccione **Usuario de prueba** en el menú desplegable **Tipo de recurso**.
Esta selección es el recurso personalizado que se creó anteriormente.
- 6 Seleccione **usuario** en el menú desplegable **Parámetro de entrada**.
- 7 Haga clic en **Siguiente**.
- 8 Cambie el nombre de la acción personalizada a **Cambiar la contraseña del usuario de prueba** y deje la descripción tal cual aparece en la pestaña **Detalles**.
- 9 Haga clic en **Siguiente**.
- 10 (opcional) Deje el formulario tal cual.
- 11 Haga clic en **Finalizar**.
- 12 En la página Acciones personalizadas, seleccione la fila **Cambiar la contraseña del usuario de prueba** y haga clic en **Publicar**.

Resultados

Ha creado una acción personalizada para cambiar la contraseña de un usuario y ha hecho que se pueda añadir a una autorización.

Pasos siguientes

Añada a un servicio el blueprint Crear un usuario de prueba. Consulte [Crear un servicio y añadirle un blueprint Crear un usuario de prueba](#).

Crear un servicio y añadirle un blueprint Crear un usuario de prueba

Puede crear un servicio para mostrar el elemento de catálogo Crear un usuario en el catálogo de servicios.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador del catálogo**.
- Compruebe que ha creado un blueprint XaaS. Consulte [Crear un blueprint XaaS para crear un usuario](#).

Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador del catálogo**.

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Servicios**.
- 2 Haga clic en el icono **Nuevo (+)**.
- 3 Escriba **Usuario de prueba de Active Directory** como nombre del servicio.
- 4 Seleccione **Activo** en el menú desplegable **Estado**.
- 5 Deje el resto de cuadros de texto vacíos.
- 6 Haga clic en **Aceptar**.
- 7 En la lista Servicios, seleccione la fila **Usuario de prueba de Active Directory** y haga clic en **Administrar elementos del catálogo**.
- 8 Haga clic en el icono **Nuevo (+)**.
- 9 Seleccione **Crear un usuario de prueba** y haga clic en **Aceptar**.

El blueprint XaaS Crear un usuario de prueba se añadirá a la lista de elementos del catálogo.

- 10 Haga clic en **Cerrar**.

Resultados

El servicio Usuario de prueba de Active Directory incluye ahora el blueprint Crear un usuario de prueba. No es necesario que añada acciones a los servicios.

Pasos siguientes

Puede autorizar a los usuarios a solicitar el blueprint y, a continuación, a ejecutar la acción. Consulte [Autorizar el servicio y la acción personalizada a un consumidor](#).

Autorizar el servicio y la acción personalizada a un consumidor

Los administradores de grupo empresarial y los administradores de tenant pueden autorizar el servicio y la acción personalizada a un usuario o un grupo de usuarios. Una vez autorizados, pueden ver el servicio en su catálogo y solicitar el elemento del catálogo Crear un usuario de

prueba que se incluye en el servicio. Después de que los consumidores aprovisionen el elemento, pueden pedir que se cambie la contraseña de usuario.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador de grupo empresarial**.
- Compruebe que el blueprint Crear un usuario se añada a un servicio. Consulte [Crear un servicio y añadirle un blueprint Crear un usuario de prueba](#).
- Compruebe que exista la acción personalizada Cambiar una contraseña de usuario. Consulte [Crear una acción personalizada para cambiar una contraseña de usuario](#).

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Autorizaciones**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Escriba **Crear un usuario de Active Directory** en el cuadro de texto **Nombre**.
- 4 Deje vacíos los cuadros de texto **Descripción** y **Fecha de caducidad**.
- 5 Seleccione **Activo** en el menú desplegable **Estado**.
- 6 Seleccione el grupo empresarial de destino en el menú desplegable **Grupo empresarial**.
Por ejemplo, administradores de cuentas de TI.
- 7 Seleccione **Todos los usuarios y grupos** para autorizar a todos los miembros del grupo empresarial (por ejemplo, administradores de cuentas de TI) para crear una cuenta de usuario.

En el catálogo, los usuarios seleccionados podrán ver el servicio y los elementos del catálogo incluidos en el servicio. Pueden ejecutar la acción de cambio de contraseña en la cuenta del usuario después de crearla.
- 8 Haga clic en **Siguiente**.
- 9 En el cuadro de texto **Servicios autorizados**, escriba **Usuario de prueba de Active Directory** y pulse Entrar.
- 10 En el cuadro de texto **Acciones autorizadas**, escriba **Cambiar la contraseña del usuario de prueba** y pulse Entrar.
- 11 Haga clic en **Finalizar**.

Resultados

Ha creado una autorización activa, de manera que los usuarios que sean miembros del grupo empresarial de administradores de cuentas de TI pueden crear usuarios. Una vez que se aprovisiona al usuario, pueden ejecutar la acción personalizada de cambio de contraseña en la cuenta del usuario aprovisionado.

Pasos siguientes

Inicie sesión como usuario autorizado para crear un usuario de Active Directory. En la pestaña **Catálogo**, verifique que el blueprint XaaS crea el usuario como se espera. Una vez creado el usuario, ejecute la acción de cambio contraseña de la pestaña **Elementos**.

Crear y publicar una acción de XaaS para migrar una máquina virtual

Puede crear y publicar una acción personalizada de XaaS para ampliar las operaciones que los consumidores pueden realizar en máquinas virtuales de vSphere aprovisionadas por IaaS.

En este escenario, crea una acción personalizada para migrar rápidamente una máquina virtual de vSphere.

Requisitos previos

Inicie sesión en vRealize Automation como **arquitecto XaaS**.

Procedimiento

1 Crear una acción personalizada para migrar una máquina virtual de vSphere

Cree una acción personalizada para permitir que los consumidores puedan migrar máquinas virtuales de vSphere después de aprovisionar las máquinas virtuales vSphere con IaaS.

2 Publicar la acción para migrar una máquina virtual de vSphere

Para usar la acción personalizada Migración rápida de una máquina virtual como una operación posterior al aprovisionamiento, debe publicarla.

Crear una acción personalizada para migrar una máquina virtual de vSphere

Cree una acción personalizada para permitir que los consumidores puedan migrar máquinas virtuales de vSphere después de aprovisionar las máquinas virtuales vSphere con IaaS.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Haga clic en **Añadir** (+).
- 3 Vaya a **Orchestrator > Biblioteca > vCenter > Gestión de máquinas virtuales > Mover y migrar** en la biblioteca de flujos de trabajo de vRealize Orchestrator y seleccione el flujo de trabajo **Migración rápida de máquina virtual**.
- 4 Haga clic en **Siguiente**.
- 5 Seleccione **IaaS VC VirtualMachine** en el menú desplegable **Tipo de recurso**.
- 6 Seleccione **vm** en el menú desplegable **Parámetro de entrada**.
- 7 Haga clic en **Siguiente**.
- 8 Deje el nombre y la descripción de la acción personalizada tal cual aparecen en la pestaña **Detalles**.
- 9 Haga clic en **Siguiente**.

10 Deje el formulario tal cual.

11 Haga clic en **Finalizar**.

Resultados

Ha creado una acción personalizada para migrar una máquina virtual, acción que ahora aparece recogida en la página Acciones personalizadas.

Pasos siguientes

[Publicar la acción para migrar una máquina virtual de vSphere](#)

Publicar la acción para migrar una máquina virtual de vSphere

Para usar la acción personalizada Migración rápida de una máquina virtual como una operación posterior al aprovisionamiento, debe publicarla.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Seleccione la fila de la acción Migración rápida de una máquina virtual y haga clic en el botón **Publicar**.

Resultados

Ha creado y publicado un flujo de trabajo de vRealize Orchestrator como una acción personalizada. Puede ir a **Administración > Administración de catálogos > Acciones** y ver la acción personalizada Migración rápida de máquina virtual en la lista de acciones. Puede asignar un icono a la acción personalizada. Consulte [Asignar un icono a una acción de recursos de XaaS](#).

Pasos siguientes

Añada la acción a las autorizaciones que contienen las máquinas virtuales de vSphere aprovisionadas por IaaS. Consulte [Autorizar usuarios a servicios, elementos de catálogo y acciones](#).

Crear una acción de XaaS para migrar una máquina virtual con vMotion

Mediante el uso de XaaS, puede crear y publicar una acción personalizada para migrar una máquina virtual aprovisionada por IaaS con vMotion.

En este escenario, crea una acción personalizada para migrar una máquina virtual de vSphere con vMotion. Además, edita la presentación del flujo de trabajo mediante la utilización del diseñador de formularios y cambia el modo en que los consumidores ven la acción cuando la solicitan.

Requisitos previos

Inicie sesión en vRealize Automation como **arquitecto XaaS**.

Procedimiento

1 Crear una acción para migrar una máquina virtual de vSphere con vMotion

Se puede crear una acción personalizada para permitir que los usuarios del catálogo de servicios puedan migrar una máquina virtual de vSphere con vMotion después de aprovisionar la máquina con IaaS.

2 Editar el formulario de acción personalizada

El formulario de acción personalizada asigna la presentación del flujo de trabajo de vRealize Orchestrator. Puede editar el formulario y definir lo que los consumidores de la acción personalizada van a ver cuando decidan realizar la operación posterior al aprovisionamiento.

3 Añadir un formulario de detalles de la acción enviados y guardar la acción

Puede añadir un nuevo formulario a la acción personalizada Migrar una máquina virtual con vMotion para definir lo que los consumidores ven después de solicitar la ejecución de la operación posterior al aprovisionamiento.

4 Publicar la acción para migrar una máquina virtual con vMotion

Para usar la acción personalizada Migrar una máquina virtual con vMotion como una operación posterior al aprovisionamiento, debe publicarla.

Crear una acción para migrar una máquina virtual de vSphere con vMotion

Se puede crear una acción personalizada para permitir que los usuarios del catálogo de servicios puedan migrar una máquina virtual de vSphere con vMotion después de aprovisionar la máquina con IaaS.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Haga clic en **Añadir** (+).
- 3 Vaya a **Orchestrator > Biblioteca > vCenter > Gestión de máquinas virtuales > Mover y migrar** en la biblioteca de flujos de trabajo de vRealize Orchestrator y seleccione el flujo de trabajo **Migrar máquina virtual con vMotion**.
- 4 Haga clic en **Siguiente**.
- 5 Seleccione **IaaS VC VirtualMachine** en el menú desplegable **Tipo de recurso**.
- 6 Seleccione **vm** en el menú desplegable **Parámetro de entrada**.
- 7 Haga clic en **Siguiente**.
- 8 Deje el nombre y la descripción de la acción personalizada tal cual aparecen en la pestaña **Detalles**.
- 9 Haga clic en **Siguiente**.

Pasos siguientes

Editar el formulario de acción personalizada.

Editar el formulario de acción personalizada


El formulario de acción personalizada asigna la presentación del flujo de trabajo de vRealize Orchestrator. Puede editar el formulario y definir lo que los consumidores de la acción personalizada van a ver cuando decidan realizar la operación posterior al aprovisionamiento.

Procedimiento

- 1 Haga clic en el icono **Eliminar** (✖) para eliminar el elemento **grupo**.
- 2 Edite el elemento **host**.
 - a Haga clic en el icono **Editar** (✎) junto al campo **host**.
 - b Escriba **Host de destino** en el cuadro de texto **Etiqueta**.
 - c Seleccione **Búsqueda** en el menú desplegable **Tipo**.
 - d Haga clic en la pestaña **Restricciones**.
 - e Seleccione **Constante** del menú desplegable **Obligatorio** y seleccione **Sí**.
De este modo, el campo de host siempre será obligatorio.
 - f Haga clic en **Enviar**.
- 3 Edite el elemento **prioridad**.
 - a Haga clic en el icono **Editar** (✎) junto al campo **prioridad**.
 - b Escriba **Prioridad de la tarea** en el cuadro de texto **Etiqueta**.
 - c Seleccione **Grupo de botones de opción** del menú desplegable **Tipo**.
 - d Haga clic en la pestaña **Valores** y desactive la casilla **No establecido**.
 - e Escriba **prioridadBaja** en el cuadro de texto de búsqueda **Valores predefinidos** y presione Entrar.
 - f Escriba **prioridadPredeterminada** en el cuadro de texto de búsqueda **Valores predefinidos** y presione Entrar.
 - g Escriba **prioridadAlta** en el cuadro de texto de búsqueda **Valores predefinidos** y presione Entrar.
 - h Haga clic en **Enviar**.

Cuando los consumidores soliciten la acción personalizada, verán un grupo de botones de opción con tres botones de opción: **prioridadBaja**, **prioridadPredeterminada** y **prioridadAlta**.

4 Edite el elemento **estado**.

- a Haga clic en el icono **Editar** () junto al campo **estado**.
- b Escriba **Estado de máquina virtual** en el cuadro de texto **Etiqueta**.
- c Seleccione **Lista desplegable** en el menú desplegable **Tipo**.
- d Haga clic en la pestaña **Valores** y desactive la casilla **No establecido**.
- e Escriba **apagado** en el cuadro de texto de búsqueda **Valores predefinidos** y presione Entrar.
- f Escriba **encendido** en el cuadro de texto de búsqueda **Valores predefinidos** y presione Entrar.
- g Escriba **suspendido** en el cuadro de texto de búsqueda **Valores predefinidos** y presione Entrar.
- h Haga clic en **Enviar**.

Quando los consumidores soliciten la acción personalizada, verán un menú desplegable con tres opciones: **apagado**, **encendido** y **suspendido**.

Resultados

Ha editado la presentación del flujo de trabajo Migrar una máquina virtual con vMotion.



Pasos siguientes

[Añadir un formulario de detalles de la acción enviados y guardar la acción.](#)

Añadir un formulario de detalles de la acción enviados y guardar la acción

Puede añadir un nuevo formulario a la acción personalizada Migrar una máquina virtual con vMotion para definir lo que los consumidores ven después de solicitar la ejecución de la operación posterior al aprovisionamiento.

Procedimiento

- 1 Haga clic en el icono **Formulario nuevo** () junto al menú desplegable **Formulario**.
- 2 Escriba **Acción enviada** en el cuadro de texto **Nombre**.
- 3 Deje el campo **Descripción** vacío.
- 4 Seleccione **Detalles de la acción enviados** en el menú **Tipo de pantalla**.
- 5 Haga clic en **Enviar**.
- 6 Haga clic en el icono **Editar** () junto al menú desplegable **Página de formulario**.
- 7 Escriba **Detalles** en el cuadro de texto **Encabezado**.
- 8 Haga clic en **Enviar**.
- 9 Arrastre el elemento **Texto** del panel Formulario y suéltelo en la página **Formulario**.

10 Escriba

Envíó una solicitud para migrar su máquina con vMotion. Espere hasta que el proceso se haya completado correctamente.

11 Haga clic fuera del cuadro de texto para guardar los cambios.

12 Haga clic en **Enviar**.

13 Haga clic en **Agregar**.

Resultados

Ha creado una acción personalizada para migrar una máquina virtual con vMotion y puede ver que aparece en la página Acciones personalizadas.

Pasos siguientes

[Publicar la acción para migrar una máquina virtual con vMotion.](#)

Publicar la acción para migrar una máquina virtual con vMotion

Para usar la acción personalizada Migrar una máquina virtual con vMotion como una operación posterior al aprovisionamiento, debe publicarla.

Procedimiento

1 Seleccione **Diseño > XaaS > Acciones personalizadas**.

2 Seleccione la fila de la acción Migrar una máquina virtual con vMotion y haga clic en el botón **Publicar**.

Resultados

Ha creado y publicado un flujo de trabajo de vRealize Orchestrator como una acción personalizada. Puede ir a **Administración > Administración de catálogos > Acciones** y ver la acción personalizada Migrar una máquina virtual con vMotion en la lista de acciones. Puede asignar un icono a la acción personalizada. Consulte [Asignar un icono a una acción de recursos de XaaS](#).

También ha editado la presentación del flujo de trabajo y ha definido el aspecto de la acción.

Pasos siguientes

Los administradores de grupo empresarial y los administradores de tenants pueden incluir la acción personalizada Migrar una máquina virtual con vMotion en una autorización. Para obtener más información sobre cómo crear y publicar blueprints de IaaS para plataformas virtuales, consulte [Diseñar blueprints de máquinas](#).

Crear y publicar una acción de XaaS para tomar un snapshot

Mediante el uso de XaaS, puede crear y publicar una acción personalizada para tomar un snapshot de una máquina virtual de vSphere que se haya aprovisionado con IaaS.

En este escenario, crea un recurso personalizado para tomar un snapshot de la máquina virtual de vSphere aprovisionada con IaaS. Además, edita la presentación del flujo de trabajo mediante la utilización del diseñador de formularios y cambia el modo en que los consumidores ven la acción cuando la solicitan.

Requisitos previos

Inicie sesión en vRealize Automation como **arquitecto XaaS**.

Procedimiento

1 Crear una acción para tomar un snapshot de una máquina virtual de vSphere

Se puede crear una acción personalizada para permitir que los consumidores puedan tomar un snapshot de una máquina virtual de vSphere después de aprovisionarla con IaaS.

2 Publicar la acción para guardar un snapshot

Para usar la acción personalizada Crear un snapshot como una operación posterior al aprovisionamiento, debe publicarla.

Crear una acción para tomar un snapshot de una máquina virtual de vSphere

Se puede crear una acción personalizada para permitir que los consumidores puedan tomar un snapshot de una máquina virtual de vSphere después de aprovisionarla con IaaS.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Haga clic en **Añadir (+)**.
- 3 Vaya a **Orchestrator > Biblioteca > vCenter > Gestión de máquinas virtuales > Snapshot** en la biblioteca de flujos de trabajo de vRealize Orchestrator y seleccione el flujo de trabajo **Crear un snapshot**.
- 4 Haga clic en **Siguiente**.
- 5 Seleccione **IaaS VC VirtualMachine** en el menú desplegable **Tipo de recurso**.
- 6 Seleccione **vm** en el menú desplegable **Parámetro de entrada**.
- 7 Haga clic en **Siguiente**.
- 8 Deje el nombre y la descripción de la acción personalizada tal cual aparecen en la pestaña **Detalles**.
- 9 Haga clic en **Siguiente**.
- 10 Deje el formulario tal cual.
- 11 Haga clic en **Agregar**.

Resultados

Ha creado una acción personalizada para tomar un snapshot de una máquina virtual, acción que ahora aparece recogida en la página Acciones personalizadas.

Pasos siguientes

[Publicar la acción para guardar un snapshot.](#)

Publicar la acción para guardar un snapshot

Para usar la acción personalizada Crear un snapshot como una operación posterior al aprovisionamiento, debe publicarla.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Seleccione la fila de la acción Crear un snapshot y haga clic en el botón **Publicar**.

Resultados

Ha creado y publicado un flujo de trabajo de vRealize Orchestrator como una acción personalizada. Puede ir a **Administración > Administración de catálogos > Acciones** y ver la acción personalizada Crear un snapshot en la lista de acciones. Puede asignar un icono a la acción personalizada. Consulte [Asignar un icono a una acción de recursos de XaaS](#).

Pasos siguientes

Los administradores de grupo empresarial y los administradores de tenants pueden incluir la acción personalizada Crear un snapshot en una autorización. Para obtener más información sobre cómo crear y publicar blueprints de IaaS para plataformas virtuales, consulte [Diseñar blueprints de máquinas](#).

Crear y publicar una acción de XaaS para iniciar una máquina virtual de Amazon

Mediante el uso de XaaS, puede crear y publicar acciones para ampliar las operaciones que los consumidores pueden realizar en recursos aprovisionados de terceros.

En este escenario, crea y publica una acción personalizada para iniciar rápidamente máquinas virtuales de Amazon.

Requisitos previos

- Instalar el complemento de vRealize Orchestrator para Amazon Web Services en el servidor de vRealize Orchestrator predeterminado.
- Crear o importar un flujo de trabajo de vRealize Orchestrator para la asignación de recursos de instancias de Amazon.

Procedimiento

1 [Crear una asignación de recursos para instancias de Amazon](#)

Puede crear una asignación de recursos que permita asociar las instancias de Amazon aprovisionadas mediante IaaS con el tipo de vRealize Orchestrator AWS:EC2Instance expuesto por el complemento de Amazon Web Services.

2 [Crear una acción personalizada para iniciar una máquina virtual de Amazon](#)

Puede crear una acción personalizada para que los consumidores puedan iniciar máquinas virtuales de Amazon aprovisionadas.

3 [Publicar la acción para iniciar instancias de Amazon](#)

Para usar la acción personalizada Iniciar instancias recién creada para operaciones posteriores al aprovisionamiento en máquinas virtuales de Amazon, debe publicarla.

Crear una asignación de recursos para instancias de Amazon

Puede crear una asignación de recursos que permita asociar las instancias de Amazon aprovisionadas mediante IaaS con el tipo de vRealize Orchestrator AWS:EC2Instance expuesto por el complemento de Amazon Web Services.

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto XaaS**.
- Cree o importe una acción de script o un flujo de trabajo de asignación de recursos de vRealize Orchestrator.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Asignaciones de recursos**.
- 2 Haga clic en **Añadir** (+).
- 3 Especifique **Instancia de EC2** en el cuadro de texto **Nombre**.
- 4 Especifique **Máquina en la nube** en el cuadro de texto **Tipo de recurso del catálogo**.
- 5 Especifique **AWS:EC2Instance** en el cuadro de texto **Tipo de orquestador**.
- 6 Seleccione **Siempre disponible**.
- 7 Seleccione el tipo de asignación de recursos que quiera usar.
- 8 Seleccione el flujo de trabajo o la acción de script de asignación de recursos personalizada de la biblioteca de vRealize Orchestrator.
- 9 Haga clic en **Agregar**.

Resultados

Puede usar la asignación de recursos de Amazon para crear acciones personalizadas relativas a las máquinas de Amazon aprovisionadas mediante IaaS.

Pasos siguientes

[Crear una acción personalizada para iniciar una máquina virtual de Amazon.](#)

Crear una acción personalizada para iniciar una máquina virtual de Amazon

Puede crear una acción personalizada para que los consumidores puedan iniciar máquinas virtuales de Amazon aprovisionadas.

Requisitos previos

Inicie sesión en vRealize Automation como **arquitecto XaaS**.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Haga clic en **Añadir (+)**.
- 3 Seleccione **Orchestrator > Biblioteca > Amazon Web Services > Nube flexible > Instancias** y, luego, seleccione el flujo de trabajo **Iniciar instancias** en la carpeta de flujos de trabajo.
- 4 Haga clic en **Siguiente**.
- 5 Seleccione **Instancia de EC2** en el menú desplegable **Tipo de recurso**.
Este es el nombre de la asignación de recursos que creó anteriormente.
- 6 Seleccione **instancia** en el menú desplegable **Parámetro de entrada**.
Este es el parámetro de entrada del flujo de trabajo de acción personalizada que coincide con la asignación de recursos.
- 7 Haga clic en **Siguiente**.
- 8 Deje el nombre y la descripción tal cual están.
El nombre predeterminado de la acción personalizada es Iniciar instancias.
- 9 Haga clic en **Siguiente**.
- 10 Deje los campos tal cual están en la pestaña **Formulario**.
- 11 Haga clic en **Agregar**.

Resultados

Ha creado una acción personalizada para iniciar máquinas virtuales de Amazon, acción que ahora aparece recogida en la página Acciones personalizadas.

Pasos siguientes

[Publicar la acción para iniciar instancias de Amazon.](#)

Publicar la acción para iniciar instancias de Amazon

Para usar la acción personalizada Iniciar instancias recién creada para operaciones posteriores al aprovisionamiento en máquinas virtuales de Amazon, debe publicarla.

Requisitos previos

Inicie sesión en vRealize Automation como **arquitecto XaaS**.

Procedimiento

- 1 Seleccione **Diseño > XaaS > Acciones personalizadas**.
- 2 Seleccione la fila de la acción personalizada Iniciar instancias y haga clic en **Publicar**.

Resultados

El estado de la acción personalizada Iniciar instancias cambiará a Publicada.

Pasos siguientes

Añada la acción Iniciar instancias a la autorización que incluye el elemento del catálogo de Amazon. Consulte [Autorizar usuarios a servicios, elementos de catálogo y acciones](#).

Solucionar problemas de acentos incorrectos y caracteres especiales en blueprints de XaaS

Cuando cree blueprints de XaaS para idiomas que utilizan cadenas que no son ASCII, los acentos y los caracteres especiales se muestran como cadenas no utilizables.

Causa

Puede haberse habilitado una propiedad de la configuración de vRealize Orchestrator que no está establecida de forma predeterminada.

Solución

- 1 En el sistema del servidor de Orchestrator, vaya a `/etc/vco/app-server/`.
- 2 Abra el archivo de configuración `vmo.properties` en un editor de texto.
- 3 Compruebe que la siguiente propiedad se haya desactivado.

```
com.vmware.o11n.webview.htmlescaping.disabled
```

- 4 Guarde el archivo `vmo.properties`.
- 5 Reinicie el servidor de vRealize Orchestrator.

Publicar un blueprint

Los blueprints se guardan con el estado de borrador y se deben publicar de forma manual antes de configurarlos como elementos del catálogo o usarlos como componentes de blueprint en el lienzo de diseño.

Tras publicar el blueprint, puede autorizarlo para ponerlo a disposición de las solicitudes de aprovisionamiento en el catálogo de servicios.

Los blueprints solo se tienen que publicar una vez. Los cambios que realice en un blueprint publicado se reflejan automáticamente en los componentes del catálogo y del blueprint anidado.

Publicar un blueprint

Puede publicar un blueprint para usarlo en el aprovisionamiento de máquinas, o para reutilizarlo en otro blueprint. Para usar el blueprint para la solicitud de aprovisionamiento de máquinas, debe autorizar el blueprint tras publicarlo. Los blueprints que se utilizan como componentes en otros blueprints no requieren autorización.

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto de infraestructura**.
- Cree un blueprint. Consulte *Lista de comprobación para la creación de blueprints de vRealize Automation*.

Procedimiento

- 1 Haga clic en la pestaña **Diseño**.
- 2 Haga clic en **Blueprints**.
- 3 Identifique el blueprint que se publicará y haga clic en **Publicar**.
- 4 Haga clic en **Aceptar**.

Resultados

El blueprint se publicará como un elemento del catálogo, pero antes deberá autorizarlo para ponerlo a disposición de los usuarios del catálogo de servicios.

Pasos siguientes

Añada el blueprint al catálogo de servicios y autorice a los usuarios para que soliciten el elemento del catálogo de aprovisionamiento de máquinas tal como se ha definido en el blueprint.

Trabajar con blueprints de desarrollador

Además del método basado en la interfaz de usuario para la creación de blueprints de vRealize Automation, también puede trabajar con los blueprints de manera programática gracias a herramientas como vRealize CloudClient, con blueprints suministrados de forma independiente o procedentes de un origen distinto, y junto con otros desarrolladores mediante aplicaciones y flujos de trabajo de vRealize Suite y herramientas de terceros.

Para obtener información acerca de estos métodos, consulte los temas siguientes:

- [Exportar e importar blueprints y contenido](#)
- [Descargar y configurar el blueprint independiente proporcionado](#)
- [Crear blueprints y otros contenidos de IaaS en un entorno de varios desarrolladores](#)

Exportar e importar blueprints y contenido

Es posible exportar blueprints y contenido mediante programación desde un entorno de vRealize Automation a otro mediante la API de REST de vRealize Automation o mediante vRealize CloudClient.

Por ejemplo, puede crear y probar sus blueprints en un entorno de desarrollo y, a continuación, importarlos en el entorno de producción. Opcionalmente, puede importar una definición de propiedades de un foro de una comunidad en su instancia de tenant de vRealize Automation activa.

Puede importar y exportar mediante programación cualquiera de los siguientes elementos de contenido de vRealize Automation:

- Blueprints de aplicaciones y todos sus componentes
- Blueprints de máquinas de IaaS
- Componentes de Software
- Blueprints de XaaS
- Perfiles de componentes
- Grupos de propiedades

La información de grupo de propiedades es específica del tenant y solo se importa con el blueprint si el grupo de propiedades ya existe en la instancia de vRealize Automation de destino.

Cuando se exporta un blueprint de una instancia de tenant de vRealize Automation a otra, la información de grupo de propiedades definida para ese blueprint no se reconoce para el blueprint importado, a menos que el grupo de propiedades ya exista en la instancia de tenant de destino. Por ejemplo, si se importa un blueprint que contiene un grupo de propiedades denominado `mica1`, el grupo de propiedades `mica1` no aparece en el blueprint importado a menos que el grupo de propiedades `mica1` ya exista en la instancia de vRealize Automation en la que se importó el blueprint. Para evitar que se pierda la información de grupo de propiedades al exportar un blueprint de una instancia de vRealize Automation a otra, utilice vRealize CloudClient para crear un paquete de exportación en formato .zip que contenga el grupo de propiedades e importe dicho paquete en el tenant de destino antes de importar el blueprint. Para obtener más información sobre el uso de vRealize CloudClient para enumerar, empaquetar, exportar e importar grupos de propiedades, además de otros elementos de vRealize Automation, consulte el centro para desarrolladores de VMware en <https://developercenter.vmware.com/tool/cloudclient>.

Tabla 3-63. Elegir la herramienta de importación y exportación

Herramienta	Más información
vRealize CloudClient	Consulte la página de vRealize CloudClient en el sitio code.vmware.com de VMware en https://developercenter.vmware.com/tool/cloudclient .
API de REST de vRealize Automation	Consulte la documentación de la API en el explorador de API de VMware para vRealize Automation en https://code.vmware.com/apis/vrealize-automation .

Nota Cuando se exportan e importan blueprints mediante programación entre implementaciones de vRealize Automation (por ejemplo, de un entorno de prueba a uno de producción o de una organización a otra) es importante reconocer que los datos de plantilla de clonación se incluyen en el paquete. Cuando se importa el paquete de blueprints, la configuración predeterminada se rellena en función de la información del mismo. Por ejemplo, si exporta y luego importa un blueprint que se creó mediante un flujo de trabajo parecido a la clonación y la plantilla de la que proceden los datos clonados no existe en un endpoint de la implementación de vRealize Automation en la que se importa el blueprint, algunos ajustes del blueprint importado no se podrán aplicar a dicha implementación.

Escenario: importar Dukes Bank para la aplicación de muestra de vSphere y configurar el entorno

Como profesional informático que evalúa vRealize Automation o aprende cómo se utiliza, puede que desee importar una aplicación de muestra grande en la instancia de vRealize Automation para poder explorar rápidamente la funcionalidad disponible y determinar cómo crearía blueprints de vRealize Automation que satisfarían las necesidades de su organización.

Requisitos previos

- Prepare una máquina de referencia Linux CentOS 6.x, conviértala en una plantilla y cree una especificación de personalización. Consulte [Escenario: Preparar la importación del blueprint de la aplicación de muestra Dukes Bank de vSphere](#).
- Cree un perfil de red externa para proporcionar una puerta de enlace y un intervalo de direcciones IP. Consulte [Crear un perfil de red externa mediante un proveedor de IPAM de terceros](#).
- Asigne el perfil de red externa a la reserva de vSphere. Consulte [Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer](#). La aplicación de muestra no puede aprovisionar correctamente sin un perfil de red externa.

- Compruebe que dispone de privilegios tanto de **arquitecto de infraestructura** como de **arquitecto de software**. Se necesitan estas dos funciones para importar la aplicación de muestra Dukes Bank y para interactuar con los blueprints y los componentes de software de Dukes Bank.

Procedimiento

1 Escenario: Importar Dukes Bank para la aplicación de muestra de vSphere

Descargue Dukes Bank para la aplicación de vSphere desde el dispositivo de vRealize Automation. Importa la aplicación de muestra en el tenant de vRealize Automation para ver una muestra funcional de un blueprint de vRealize Automation de varios niveles que incluya varios componentes de máquina con componentes de redes y software.

2 Escenario: Configurar los componentes de muestra de Dukes Bank de vSphere en su entorno

Con sus privilegios de arquitecto de infraestructura, debe configurar los componentes de máquina de Dukes Bank para que usen la especificación de personalización, la plantilla y los prefijos de máquina que ha creado para el entorno.

Resultados

Ha configurado la aplicación de muestra de Dukes Bank para vSphere del entorno para usarla como punto de partida en el desarrollo de sus propios blueprints, como una herramienta para evaluar vRealize Automation, o como recurso de aprendizaje para ayudarle a comprender la funcionalidad y los componentes de vRealize Automation.

Escenario: Importar Dukes Bank para la aplicación de muestra de vSphere

Descargue Dukes Bank para la aplicación de vSphere desde el dispositivo de vRealize Automation. Importa la aplicación de muestra en el tenant de vRealize Automation para ver una muestra funcional de un blueprint de vRealize Automation de varios niveles que incluya varios componentes de máquina con componentes de redes y software.

Procedimiento

- 1 Inicie sesión como raíz, y mediante SSH, en el dispositivo de vRealize Automation.
- 2 Descargue Dukes Bank para la aplicación de muestra de vSphere desde el dispositivo de vRealize Automation en /tmp.

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn:5480/blueprints/
DukesBankAppForvSphere.zip
```

No descomprima el paquete.

- 3 Descargue vRealize CloudClient desde <http://developercenter.vmware.com/tool/cloudclient> en /tmp.
- 4 Descomprima el paquete cloudclient-4x-dist.zip.

- 5 Ejecute vRealize CloudClient en el directorio /bin.

```
$> ./bin/cloudclient.sh
```

- 6 Si se le solicita, acepte el contrato de licencia.
- 7 Con vRealize CloudClient, inicie sesión en el dispositivo de vRealize Automation como un usuario con privilegios de **arquitecto de software** y de **arquitecto de infraestructura**.

```
CloudClient> vra login userpass --server https://vRealize_VA_Hostname_fqdn --user  
<user@domain.com> --tenant <TenantName>
```

- 8 Cuando se le solicite, escriba su contraseña de inicio de sesión.
- 9 Valide que el contenido de DukesBankAppForvSphere.zip esté disponible.

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run true --resolution OVERWRITE
```

Tenga en cuenta que la entrada OVERWRITE distingue entre mayúsculas y minúsculas, y requiere mayúscula.

Si configura la resolución para reescribir en vez de *skip*, permitirá que vRealize Automation solucione los conflictos cuando sea posible.

- 10 Importe la aplicación de muestra Dukes Bank.

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run false --resolution  
OVERWRITE
```

Tenga en cuenta que la entrada OVERWRITE distingue entre mayúsculas y minúsculas, y requiere mayúscula.

Resultados

Cuando inicia sesión en la consola de vRealize Automation como usuario con privilegios de arquitecto de software y arquitecto de infraestructura, puede ver los blueprints y los componentes de software de Dukes Bank en la pestaña **Diseño > Blueprints** y en la pestaña **Diseño > Componentes de software**.

Escenario: Configurar los componentes de muestra de Dukes Bank de vSphere en su entorno

Con sus privilegios de arquitecto de infraestructura, debe configurar los componentes de máquina de Dukes Bank para que usen la especificación de personalización, la plantilla y los prefijos de máquina que ha creado para el entorno.

En este escenario se configuran los componentes de máquina para clonar las máquinas a partir de la plantilla que ha creado en vSphere Web Client. Si desea crear copias de una máquina virtual que usen el espacio de manera eficiente a partir de un snapshot, la aplicación de muestra también es compatible con los clones vinculados. Los clones vinculados usan una cadena de discos delta para realizar un seguimiento de las diferencias con respecto a una máquina principal, se aprovisionan rápidamente, reducen el coste de almacenamiento y su uso es ideal cuando el rendimiento no es una prioridad importante.

Procedimiento

- 1 Inicie sesión en la consola de vRealize Automation como **arquitecto de infraestructura**.

Puede configurar la aplicación de ejemplo de Dukes Bank para trabajar en su entorno solo con la función de **arquitecto de infraestructura**, pero si desea ver o editar los componentes del software de muestra, también necesitará la función de **arquitecto de software**.

- 2 Seleccione **Diseño > Blueprints**.

- 3 Seleccione el blueprint **DukesBankApplication** y haga clic en el icono **Editar**.

- 4 Edite el appserver-node para que vRealize Automation pueda aprovisionar el componente de máquina en el entorno.

Configure el blueprint para aprovisionar varias instancias del componente de máquina, de modo que pueda comprobar la funcionalidad del modo del equilibrador de carga.

- a Haga clic en el componente **appserver-node** en el lienzo de diseño.

La información de configuración aparece en el panel inferior.

- b Seleccione un prefijo de máquina del menú desplegable **Prefijo de máquina**.

- c Configure el blueprint para que aprovisione al menos dos instancias de dicho nodo (y hasta un máximo de diez) mediante la selección de un mínimo de 2 instancias y un máximo de 10.

En el formulario de solicitud, los usuarios pueden aprovisionar al menos dos nodos appserver, hasta un máximo de diez. Si los usuarios están autorizados para realizar las acciones de escalado vertical y escalado horizontal, pueden cambiar la escala de sus implementaciones para adaptarlas a las necesidades cambiantes.

- d Haga clic en la pestaña **Información de creación**.

- e Seleccione **Cloneworkflow** en el menú desplegable **Flujo de trabajo de aprovisionamiento**.

- f Seleccione la **dukes_bank_template** en el cuadro de diálogo **Clonar de**.

- g Especifique la **Customspecs_sample** en el cuadro de texto **Especificación de personalización**.

Este campo distingue mayúsculas y minúsculas.

- h Haga clic en la pestaña **Recursos de máquinas**.

- i Compruebe que la configuración de la memoria es de al menos 2048 MB.

- 5 Edite el loadbalancer-node para que vRealize Automation pueda aprovisionar el componente de máquina en el entorno.

- a Haga clic en el componente **loadbalancer-node** en el lienzo de diseño.

- b Seleccione un prefijo de máquina del menú desplegable **Prefijo de máquina**.

- c Haga clic en la pestaña **Información de creación**.

- d Seleccione **Cloneworkflow** en el menú desplegable **Flujo de trabajo de aprovisionamiento**.
- e Seleccione la **dukes_bank_template** en el cuadro de diálogo **Clonar de**.
- f Especifique la **Customspecs_sample** en el cuadro de texto **Especificación de personalización**.

Este campo distingue mayúsculas y minúsculas.

- g Haga clic en la pestaña **Recursos de máquinas**.
- h Compruebe que la configuración de la memoria es de al menos 2048 MB.

6 Repita los pasos para el componente de máquina **database-node**.

7 Haga clic en **Guardar y finalizar**.

Los cambios se guardarán y volverá a la pestaña **Blueprints**.

8 Seleccione el blueprint **DukesBankApplication** y haga clic en **Publicar**.

Resultados

Ha configurado el blueprint de aplicación de prueba de Dukes Bank para el entorno y ha publicado el blueprint completado.

Pasos siguientes

Los usuarios no podrán ver los blueprints publicados en el catálogo hasta que configure un servicio del catálogo, añada el blueprint a un servicio y autorice a los usuarios para que soliciten el blueprint. Consulte [Lista de comprobación para configurar el catálogo de servicios](#).

Tras configurar el blueprint de Dukes Bank para que se muestre en el catálogo, podrá solicitar el aprovisionamiento de la aplicación de muestra. Consulte [Escenario: Probar la aplicación de muestra Dukes Bank](#).

Escenario: Probar la aplicación de muestra Dukes Bank

Solicita el elemento del catálogo Dukes Bank e inicie sesión en la aplicación de muestra para comprobar su trabajo y ver la funcionalidad del blueprint de vRealize Automation.

Requisitos previos

- Importe la aplicación de muestra Dukes Bank y configure los componentes de blueprint para trabajar en su entorno. Consulte [Escenario: importar Dukes Bank para la aplicación de muestra de vSphere y configurar el entorno](#).
- Configure el catálogo de servicios y ponga el blueprint de Dukes Bank a disposición de los usuarios para que lo soliciten. Consulte [Lista de comprobación para configurar el catálogo de servicios](#).
- Compruebe que las máquinas virtuales aprovisionadas tengan acceso al repositorio yum.

Procedimiento

- 1** Inicie sesión en la consola de vRealize Automation como usuario autorizado en el elemento del catálogo Dukes Bank.
- 2** Haga clic en la pestaña **Catálogo**.
- 3** Ubique el elemento del catálogo de la aplicación de muestra Dukes Bank y haga clic en **Solicitar**.
- 4** Rellene la información de solicitud necesaria para cada componente que tenga un asterisco rojo.
 - a Vaya al componente JBossAppServer para rellenar la información de solicitud necesaria.
 - b Escriba el nombre de dominio completo del dispositivo de vRealize Automation en el cuadro de texto **app_content_server_ip**.
 - c Vaya a los componentes de software Dukes_Bank_App para rellenar la información de solicitud necesaria.
 - d Escriba el nombre de dominio completo del dispositivo de vRealize Automation en los cuadros de texto **app_content_server_ip**.
- 5** Haga clic en **Enviar**.

En función de la red y de la instancia de vCenter Server, el aprovisionamiento completo de la aplicación de muestra Dukes Bank puede tardar entre 15 y 20 minutos. Puede supervisar el estado en la pestaña **Solicitudes** y, cuando finalice el aprovisionamiento de la aplicación, puede ver los detalles de los elementos del catálogo en la pestaña **Elementos**.

- 6** Cuando finalice el aprovisionamiento de la aplicación, busque la dirección IP del servidor del equilibrador de carga para poder acceder a la aplicación de muestra Dukes Bank.
 - a Seleccione **Elementos > Implementaciones**.
 - b Expanda la implementación de la aplicación de muestra Dukes Bank y seleccione el servidor del equilibrador de carga Apache.
 - c Haga clic en **Ver detalles**.
 - d Seleccione la pestaña **Red**.
 - e Anote la dirección IP.
- 7** Inicie sesión en la aplicación de muestra Dukes Bank.
 - a Vaya al servidor del equilibrador de carga en `http://IP_Apache_Load_Balancer:8081/bank/main.faces`.

Si desea acceder a los servidores de aplicaciones directamente, vaya a `http://IP_AppServer:8080/bank/main.faces`.
 - b Escriba **200** en el cuadro de texto **Nombre de usuario**.
 - c Escriba **foobar** en el cuadro de texto **Contraseña**.

Resultados

La aplicación de muestra Dukes Bank funciona y puede usarla como punto de partida en el desarrollo de sus propios blueprints, como una herramienta para evaluar vRealize Automation, o como un recurso de aprendizaje para ayudarle a comprender la funcionalidad y los componentes de vRealize Automation.

Descargar y configurar el blueprint independiente proporcionado

Puede descargar un blueprint independiente proporcionado y sus componentes de software asociados del dispositivo de vRealize Automation.

El documento [Descargar y configurar el blueprint independiente de vRealize Automation](#) le guiará por el proceso de descarga de un blueprint independiente de vRealize Automation desde el dispositivo de vRealize Automation, así como por los procesos posteriores de importación, configuración y uso del blueprint en vRealize Automation junto con varios flujos de trabajo de vRealize Orchestrator.

Crear blueprints y otros contenidos de IaaS en un entorno de varios desarrolladores

Varios desarrolladores pueden utilizar los flujos de trabajo de vRealize Orchestrator junto con vRealize Suite y herramientas para desarrolladores de terceros a fin de trabajar simultáneamente en los diferentes artefactos de blueprint de vRealize Automation para los mismos blueprints de vRealize Automation u otros distintos.

Puede utilizar herramientas como vRealize Suite Lifecycle Manager para facilitar un entorno de varios desarrolladores de vRealize Automation y otras herramientas de vRealize Suite y archivos OVA, además de herramientas de terceros como GitLab/GitHub, Houdini y otros artefactos de aplicaciones desde [VMware Solutions Exchange](#).

Consulte los siguientes recursos para conocer más sobre la creación de blueprints de vRealize Automation y otros contenidos de IaaS como propiedades, suscripciones de agentes de eventos, componentes de software y flujos de trabajo de vRealize Orchestrator en un entorno de varios desarrolladores:

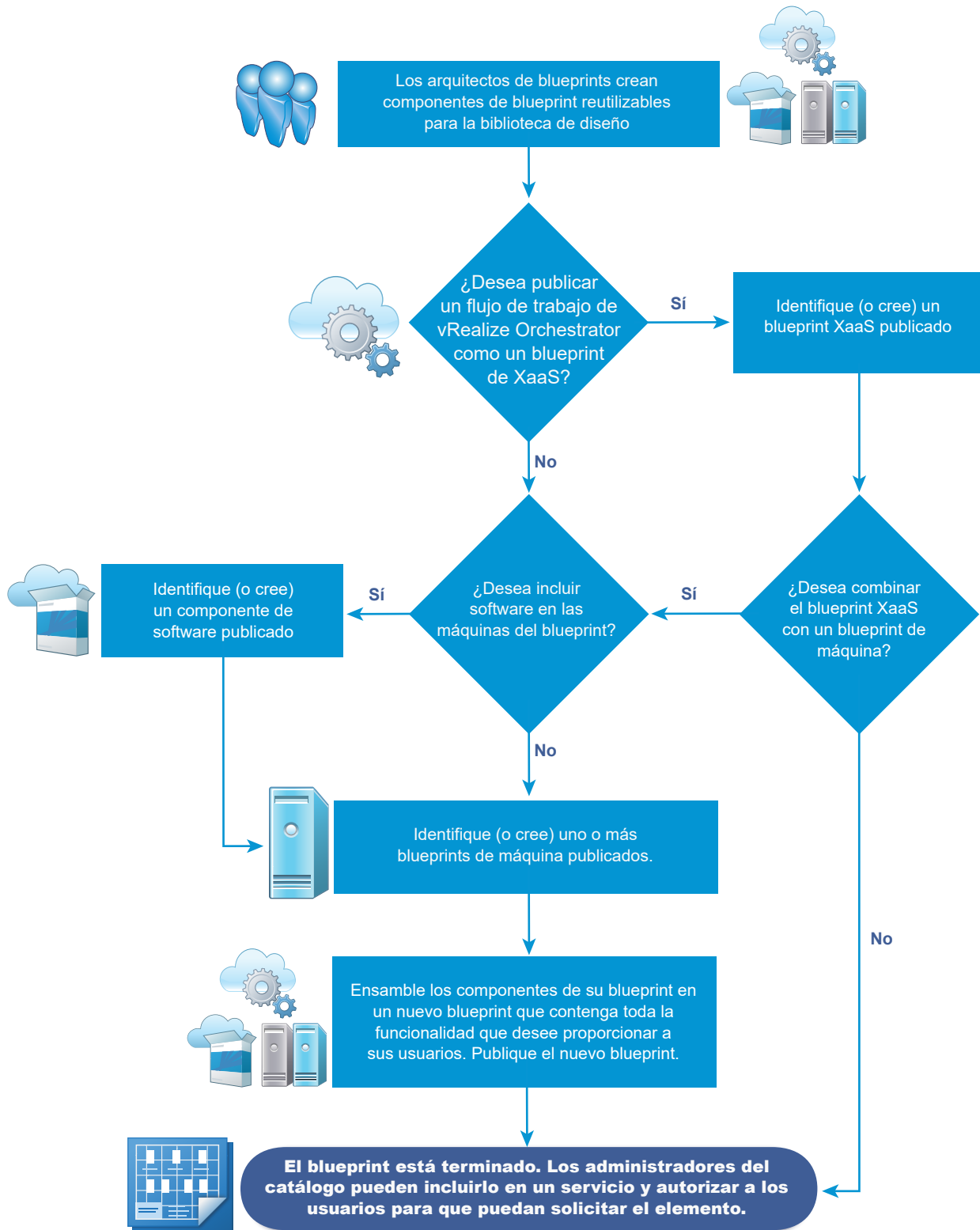
- [Vídeo: What's New en Lifecycle Manager](#)
- [Entrada de blog: vRealize Automation con blueprint de infraestructura - Configuración del entorno de varios desarrolladores](#)
- Documento: [Descargar y configurar el blueprint independiente proporcionado](#)
- [Entrada de blog: Lifecycle Manager con la integración de GitLab](#)
- [Entrada de blog: Descripción general de LifeCycle Manager](#)

Ensamblar blueprints compuestos

Puede reutilizar blueprints y componentes de blueprints publicados combinándolos de nuevas formas para crear paquetes de servicios de TI que les proporcionen funciones complejas a los usuarios.

Si los blueprints de componentes disponen de formularios personalizados, los formularios de solicitud personalizados no se aplicarán en el nuevo blueprint. Deberá crear nuevos formularios para el nuevo blueprint. Para obtener más información acerca de los formularios de solicitud personalizados, consulte [Personalizar formularios de solicitud de blueprint](#).

Figura 3-5. Flujo de trabajo para ensamblar blueprints compuestos



■ Información sobre el comportamiento de blueprint anidado

Si desea reutilizar los blueprints, puede anidarlos en otro blueprint como un componente. Los blueprints se anidan para poder reutilizarlos y para controlar la modularidad en el aprovisionamiento de máquinas, pero hay reglas y consideraciones específicas que debe tener en cuenta a la hora de trabajar con blueprints anidados.

- **Usar componentes de máquina y componentes de Software al ensamblar un blueprint**

Para proporcionar componentes de Software, deben colocarse sobre componentes de máquina compatibles durante el ensamblado de los blueprints.

- **Crear enlaces de propiedad entre componentes de blueprint**

En varios escenarios de implementación, un componente necesita el valor de propiedad de otro componente para personalizarse a sí mismo. Es posible enlazar propiedades de XaaS, máquinas, Software y propiedades personalizadas a otras propiedades en un blueprint.

- **Crear dependencias y controlar el orden de aprovisionamiento**

Si necesita información de uno de los componentes de blueprint para completar el aprovisionamiento de otro componente, puede dibujar una dependencia explícita en el lienzo de diseño para escalar el aprovisionamiento. De este modo, evitará que el componente dependiente sea aprovisionado antes de tiempo. Las dependencias explícitas controlan el orden de compilación de una implementación y desencadenan actualizaciones dependientes durante una operación de escalado horizontal o vertical. Los componentes de software se deben ordenar en un blueprint.

Información sobre el comportamiento de blueprint anidado

Si desea reutilizar los blueprints, puede anidarlos en otro blueprint como un componente. Los blueprints se anidan para poder reutilizarlos y para controlar la modularidad en el aprovisionamiento de máquinas, pero hay reglas y consideraciones específicas que debe tener en cuenta a la hora de trabajar con blueprints anidados.

Un blueprint que contiene uno o más blueprints anidados se denomina blueprint externo. Cuando añade un componente de blueprint al lienzo de diseño mientras crea o edita otro blueprint, el componente de blueprint se conoce como blueprint anidado y el blueprint contenedor al que se añade se denomina blueprint externo.

El uso de blueprints anidados plantea cuestiones que no siempre son obvias. Es importante comprender las siguientes consideraciones y reglas para aprovechar al máximo las capacidades de aprovisionamiento de su máquina.

Consideraciones y reglas generales para blueprints anidados

- Como práctica recomendada para minimizar la complejidad de los blueprints, limite la profundidad de estos a tres niveles, con el blueprint de nivel superior como uno de los tres niveles.
- Si un usuario está autorizado para utilizar el blueprint externo, dicho usuario tiene autorización para utilizar los blueprints anidados.

- Puede aplicar una política de aprobación a un blueprint. Cuando se aprueba, el elemento de catálogo del blueprint y todos sus componentes, incluidos los blueprints anidados, se aprovisionan. También puede aplicar diferentes políticas de aprobación a diferentes componentes. Todas las políticas de aprobación se deben aprobar antes de que se aprovisionen el blueprint solicitado.
- Cuando se edita un blueprint publicado, no se cambian las implementaciones que ya se han aprovisionado mediante este blueprint. En el momento del aprovisionamiento, la implementación resultante lee los valores actuales del blueprint, incluidos los de sus blueprints anidados. Los únicos cambios que pueden trasladarse a las implementaciones aprovisionadas son las modificaciones en los componentes de software (por ejemplo, en los scripts de actualización o de desinstalación).
- La configuración que se define en el blueprint externo reemplaza la configuración de los blueprints anidados, excepto en los siguientes casos:
 - Puede cambiar el nombre de un blueprint anidado, pero no puede cambiar el nombre de un componente de máquina o cualquier otro componente dentro de un blueprint anidado.
 - No puede añadir o eliminar propiedades personalizadas para un componente de máquina en un blueprint anidado. No obstante, podrá editar esas propiedades personalizadas. No es posible añadir, editar o eliminar grupos de propiedades de un componente de máquina que está en un blueprint anidado.
- Los cambios que usted u otro arquitecto realice en la configuración del blueprint anidado aparecen en los blueprints externos, a menos que haya reemplazado esa configuración en el blueprint externo.
- Limite el tiempo de concesión máximo del blueprint externo al valor de concesión máximo más bajo de un blueprint de componentes.

Puede establecerse cualquier valor para el tiempo de concesión de un blueprint anidado y del blueprint externo; no obstante, el tiempo de concesión máximo del blueprint externo debe limitarse al valor de concesión máximo más bajo de un blueprint anidado. De esta forma, el arquitecto de aplicaciones puede diseñar un blueprint compuesto con valores de concesión tanto uniformes como variables que estén dentro de las limitaciones que identifique el arquitecto de infraestructuras. Si el valor de concesión máximo que se define en un blueprint anidado es inferior al que se define en el blueprint externo, se produce un error en la solicitud de aprovisionamiento.

- Cuando trabaje en un blueprint externo, podrá sobrescribir la configuración de Recursos de máquinas que se establece para un componente de la máquina en un blueprint anidado.
- Cuando trabaje en un blueprint externo, podrá arrastrar un componente de software a un componente de máquina en un blueprint anidado.
- Si abre un blueprint en el cual un componente de máquina en un blueprint anidado se ha quitado o se ha cambiado su identificador, y el componente de máquina estaba asociado con componentes del blueprint actual, se quitan los componentes asociados y se muestra el siguiente mensaje (o uno similar):

Se ha quitado un componente de máquina en un blueprint anidado al que hacen referencia algunos componentes del blueprint actual o se ha cambiado su identificador del componente de máquina. Se han quitado todos los componentes del blueprint actual que estaban asociados con el identificador del componente de máquina faltante o cambiado. Haga clic en Cancelar para conservar el historial de asociaciones entre el identificador del componente de máquina faltante o cambiado del blueprint anidado y los componentes del blueprint actual, y corrija el problema del blueprint anidado. Abra el blueprint anidado y vuelva a añadir el componente de máquina faltante con el identificador original, o cambie el identificador del componente de máquina por su identificador original. Haga clic en Guardar para quitar todo el historial de asociaciones entre el identificador del componente de máquina faltante o cambiado del blueprint anidado y los componentes del blueprint actual.

- Al publicar un blueprint, los datos de componentes de software se tratan como un snapshot. Si luego modifica las propiedades del componente de software, el blueprint en el que existe el componente de software solo reconocerá nuevas propiedades. Las actualizaciones de las propiedades que ya existían en el componente de software en el momento de publicarse el blueprint no se actualizan en el blueprint. El blueprint solo hereda las propiedades que se añaden después de publicar el blueprint. Sin embargo, se pueden realizar cambios en las instancias del componente de software de los blueprints en los que reside el componente de software para cambiar ese blueprint en concreto.

Consideraciones y reglas relativas a redes y seguridad para blueprints anidados

- Los componentes de red y seguridad en los blueprints externos se pueden asociar a máquinas que se definen en blueprints anidados.
- Los componentes de red, seguridad y equilibrador de carga de NSX y su configuración no se admiten en los blueprints anidados.
- Cuando se aplica el aislamiento de aplicaciones en el blueprint externo, reemplaza la configuración de aislamiento de aplicaciones especificada en los blueprints anidados.
- La configuración de zona de transporte que se define en el blueprint externo reemplaza la configuración de zona de transporte especificada en los blueprints anidados.
- Cuando trabaje en un blueprint externo, podrá ajustar la configuración del equilibrador de carga relacionada con la configuración del componente de red y la configuración del componente de la máquina que se han configurado en un blueprint interno o anidado.
- Para un blueprint anidado que contiene un componente de red NAT bajo demanda, los rangos de IP especificados en el componente de red NAT bajo demanda no se pueden editar en el blueprint externo.
- El blueprint exterior no puede contener un blueprint interior que incluya configuración de redes a petición ni configuración del equilibrador de carga a petición. No se permite usar un blueprint interior que contenga un componente de red a petición de NSX ni un componente de equilibrador de carga NSX.

- Para un blueprint anidado que contiene componentes de red o de seguridad de NSX, no puede cambiar el perfil de red o la información de política de seguridad que se especifica en el blueprint anidado. No obstante, puede reutilizar esa configuración para otros componentes de la máquina de vSphere que añada al blueprint externo.
- Para garantizar que los componentes de red y seguridad de NSX de los blueprints anidados tengan un nombre exclusivo en un blueprint compuesto, vRealize Automation utiliza como prefijo el identificador de blueprint anidado en nombres de componentes de red y seguridad que aún no son únicos. Por ejemplo, si añade un blueprint con el nombre de identificador xbp_1 a un blueprint externo y ambos blueprints contienen un componente de grupo de seguridad bajo demanda con el nombre OD_Security_Group_1, el componente del blueprint anidado cambia de nombre a xbp_1_OD_Security_Group_1 en el lienzo de diseño del blueprint. Los nombres de componentes de red y seguridad del blueprint externo no tienen prefijo.
- La configuración del componente puede cambiar según la ubicación del blueprint. Por ejemplo, si incluye grupos de seguridad, etiquetas de seguridad o redes a petición tanto a nivel de blueprint interior como exterior, la configuración del blueprint exterior reemplazará la del blueprint interior. Los componentes de redes y seguridad solo son compatibles con el nivel de blueprint exterior, a excepción de las redes existentes que funcionan a nivel de blueprint interior. Para evitar problemas, añada todos los grupos de seguridad, las etiquetas de seguridad y las redes a petición solo al blueprint exterior.

Consideraciones relativas a componentes de software para blueprints anidados

En los blueprints que puedan escalarse, lo recomendable es crear blueprints de una sola capa que no reutilicen otros blueprints. Normalmente, los procesos de actualización durante las operaciones de escalado se desencadenan mediante dependencias implícitas que se crean cuando se enlaza una propiedad de software a una propiedad de máquina. Sin embargo, las dependencias implícitas en un blueprint anidado no siempre desencadenan procesos de actualización. Si necesita usar blueprints anidados en un blueprint escalable, puede dibujar manualmente dependencias entre componentes del blueprint anidado con el fin de crear dependencias explícitas que desencadenen siempre una actualización.

Usar componentes de máquina y componentes de Software al ensamblar un blueprint

Para proporcionar componentes de Software, deben colocarse sobre componentes de máquina compatibles durante el ensamblado de los blueprints.

Para ofrecer compatibilidad con componentes de Software, el blueprint de la máquina que seleccione debe contener un componente de máquina basado en una plantilla, snapshot o imagen de máquina de Amazon que contenga el agente invitado y el agente de arranque de Software y se debe usar como método de aprovisionamiento compatible.

Debido a que los agentes de Software no son compatibles con el protocolo de Internet versión 6 (IPv6), utilice la configuración de IPv4.

Nota Los componentes de software deben tener una dependencia de orden en el blueprint. Si no se ordenan los componentes de software, no se podrá aprovisionar el blueprint. Si no hay ninguna dependencia de orden real para los componentes de software, puede satisfacer los requisitos de orden del blueprint agregando una falsa dependencia entre los componentes de software.

Si diseña blueprints que puedan escalarse, lo recomendable es crear blueprints de una sola capa que no reutilicen otros blueprints. Normalmente, los procesos de actualización que se usan durante las operaciones de escalado se desencadenan por dependencias implícitas, como enlaces de propiedades. Sin embargo, las dependencias implícitas en un blueprint anidado no siempre desencadenan procesos de actualización.

Aunque los arquitectos de IaaS, los arquitectos de aplicaciones y los arquitectos de software pueden ensamblar blueprints, solo los arquitectos de IaaS pueden configurar componentes de máquinas. Si usted no es un arquitecto de IaaS, no puede configurar los componentes de su propia máquina, pero puede reutilizar blueprints de máquina que su arquitecto de IaaS haya creado y publicado.

Para añadir componentes de software correctamente al lienzo de diseño, también debe ser miembro del grupo empresarial, ser administrador del grupo empresarial, o bien tener acceso de función de administrador de tenant en el catálogo de destino.

Si necesita usar blueprints anidados en un blueprint escalable, puede dibujar manualmente dependencias entre componentes del blueprint anidado con el fin de crear dependencias explícitas que desencadenen siempre una actualización.

Nota Al publicar un blueprint, los datos de componentes de software se tratan como un snapshot. Si luego modifica las propiedades del componente de software, el blueprint en el que existe el componente de software solo reconocerá nuevas propiedades. Las actualizaciones de las propiedades que ya existían en el componente de software en el momento de publicarse el blueprint no se actualizan en el blueprint. El blueprint solo hereda las propiedades que se añaden después de publicar el blueprint. Sin embargo, se pueden realizar cambios en las instancias del componente de software de los blueprints en los que reside el componente de software para cambiar ese blueprint en concreto.

Tabla 3-64. Métodos de aprovisionamiento compatibles con Software

Tipo de máquina	Método de aprovisionamiento
vSphere	Clonar
vSphere	Clon vinculado
vCloud Director	Clonar
vCloud Air	Clonar
Amazon AWS	Imagen de máquina de Amazon

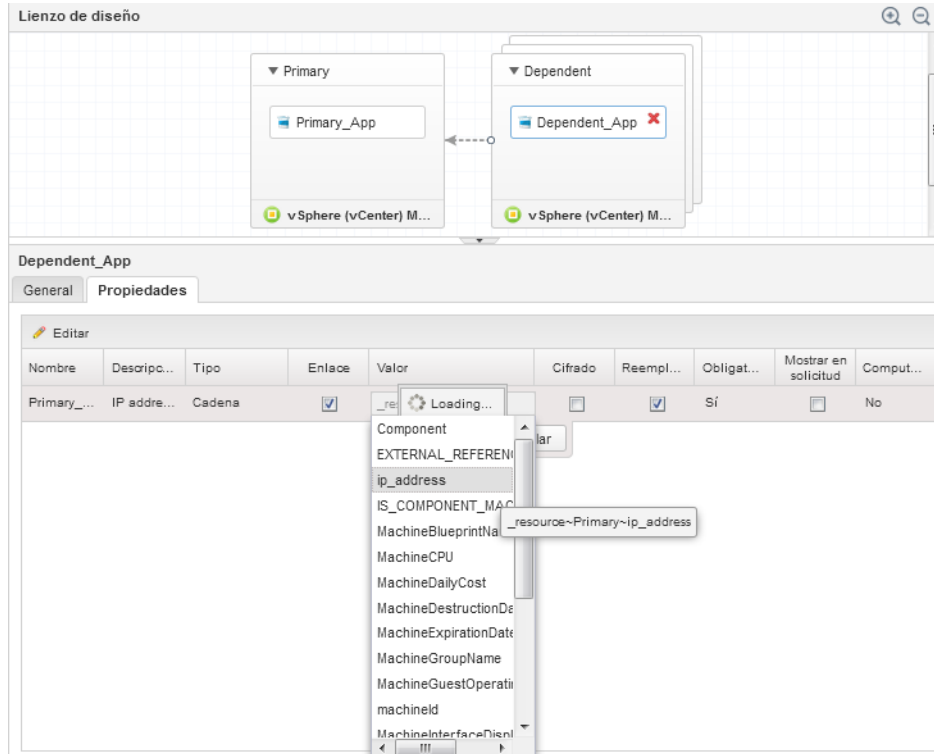
Crear enlaces de propiedad entre componentes de blueprint

En varios escenarios de implementación, un componente necesita el valor de propiedad de otro componente para personalizarse a sí mismo. Es posible enlazar propiedades de XaaS, máquinas, Software y propiedades personalizadas a otras propiedades en un blueprint.

Por ejemplo, el arquitecto de software podría modificar definiciones de propiedad en los scripts de ciclo de vida de un componente WAR. Un componente WAR puede necesitar la ubicación de instalación del componente del servidor Apache Tomcat, de modo que el arquitecto de software configura el componente WAR para establecer el valor de propiedad `server_home` en el valor de propiedad `install_path` del servidor Apache Tomcat. Como arquitecto que ensambla el blueprint, debe enlazar la propiedad `server_home` a la propiedad `install_path` del servidor Apache Tomcat para que el componente de Software aprovisiona correctamente.

Establece enlaces de propiedad al configurar componentes en un blueprint. En la página **Blueprint**, arrastre el componente al lienzo y haga clic en la pestaña **Propiedades**. Para enlazar una propiedad a otra propiedad en un blueprint, seleccione la casilla **Enlazar**. Puede escribir *ComponentName~PropertyName* en el cuadro de texto de valor, o bien utilizar la flecha hacia abajo para generar una lista de opciones de enlace disponibles. Utilice un carácter de ~ como separador entre componentes y propiedades. Por ejemplo, para enlazar a la propiedad `dp_port`, en el componente MySQL, podría escribir `mysql~db_port`. Para enlazar las propiedades que se configuran durante el aprovisionamiento, como la dirección IP de una máquina o el nombre del host de un componente de Software, escriba *_resource~ComponentName~PropertyName*. Por ejemplo, para enlazar al nombre de reserva de una máquina, puede escribir `_resource~vSphere_Machine_1~MachineReservationName`.

Figura 3-6. Enlazar una propiedad de software a la dirección IP de una máquina



Crear dependencias y controlar el orden de aprovisionamiento

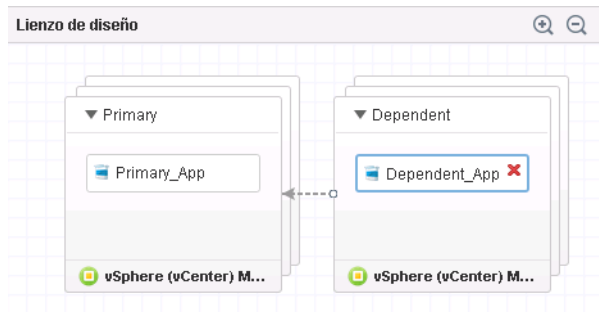
Si necesita información de uno de los componentes de blueprint para completar el aprovisionamiento de otro componente, puede dibujar una dependencia explícita en el lienzo de diseño para escalar el aprovisionamiento. De este modo, evitará que el componente dependiente sea aprovisionado antes de tiempo. Las dependencias explícitas controlan el orden de compilación de una implementación y desencadenan actualizaciones dependientes durante una operación de escalado horizontal o vertical. Los componentes de software se deben ordenar en un blueprint.

Cuando diseña blueprints con varias máquinas y aplicaciones, puede que necesite propiedades de una de las máquinas para completar la instalación de una aplicación en otra. Por ejemplo, si está compilando un servidor web, puede que necesite el nombre del host del servidor de la base de datos para poder instalar la aplicación y crear instancias de tablas de la base de datos. Si asigna una dependencia explícita, el servidor de la base de datos inicia el aprovisionamiento cuando el servidor web finaliza el aprovisionamiento.

Nota Los componentes de software deben tener una dependencia de orden en el blueprint. Si no se ordenan los componentes de software, no se podrá aprovisionar el blueprint. Si no hay ninguna dependencia de orden real para los componentes de software, puede satisfacer los requisitos de orden del blueprint agregando una falsa dependencia entre los componentes de software.

Para asignar una dependencia en un lienzo de diseño, trace una línea desde el componente dependiente hasta el componente del que depende. Al finalizar, el componente que desea compilar en segundo lugar tiene una flecha que señala el componente que desea compilar primero. Por ejemplo, en la figura Controlar el orden de compilación con la asignación de dependencias, la máquina dependiente solo se aprovisiona cuando se compila la máquina principal. También puede configurar las dos máquinas para que se aprovisionen en simultáneo, pero traza una dependencia entre los componentes de software.

Figura 3-7. Controlar el orden de compilación con la asignación de dependencias



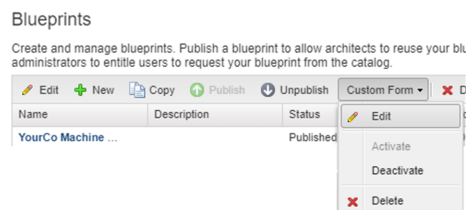
Si diseña blueprints que puedan escalarse, lo recomendable es crear blueprints de una sola capa que no reutilicen otros blueprints. Normalmente, los procesos de actualización durante las operaciones de escalado se desencadenan mediante dependencias implícitas que se crean cuando se enlaza una propiedad de software a una propiedad de máquina. Sin embargo, las dependencias implícitas en un blueprint anidado no siempre desencadenan procesos de actualización. Si necesita usar blueprints anidados en un blueprint escalable, puede dibujar manualmente dependencias entre componentes del blueprint anidado con el fin de crear dependencias explícitas que desencadenen siempre una actualización.

Personalizar formularios de solicitud de blueprint

Cada blueprint que se crea y publica muestra un formulario cuando los usuarios solicitan el blueprint del catálogo. Puede utilizar el formulario predeterminado o puede personalizar los formularios de solicitud de blueprint al crear o editar un blueprint. Un formulario se personaliza cuando la información proporcionada o solicitada en el formulario predeterminado no es lo que desea presentar a los usuarios.

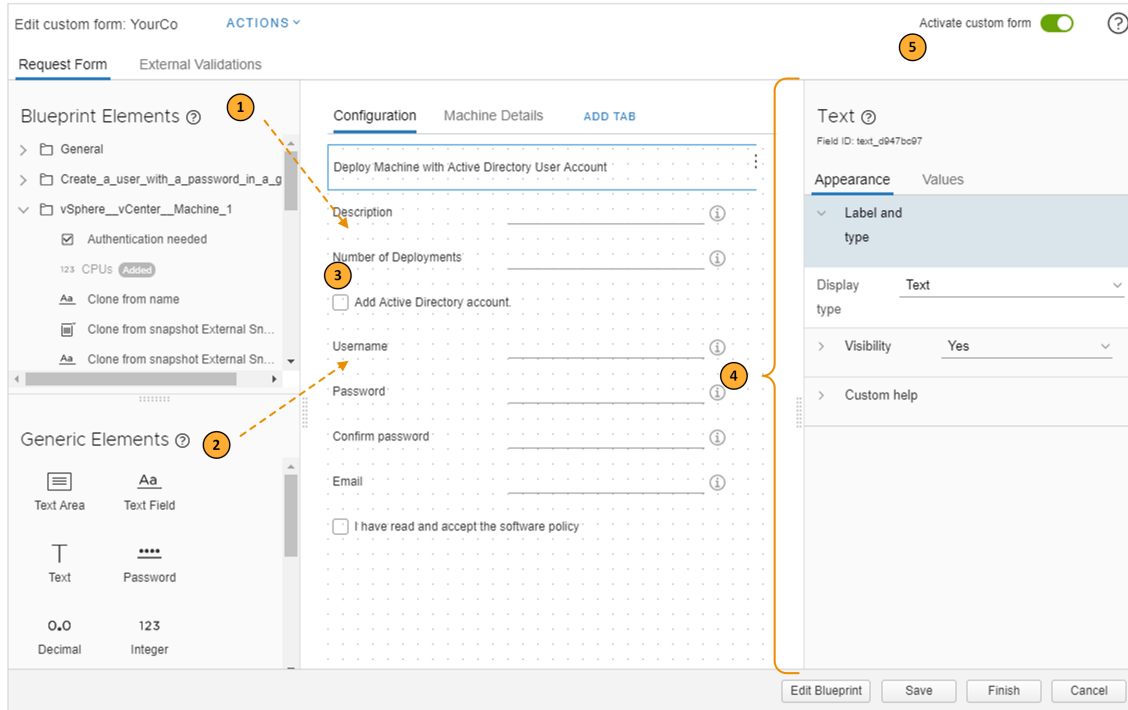
Personalizar formularios de solicitud

Se accede al diseñador de formularios de solicitud personalizados desde la cuadrícula de datos del blueprint o desde el lienzo del blueprint.



Diseñador de formularios de solicitud personalizados

El diseñador de formularios se emplea para crear el formulario personalizado.



Para crear un formulario personalizado:

- 1 Arrastre elementos (1 y 2) al lienzo de diseño (3).
- 2 Configure cada elemento mediante el panel de propiedades (4).
- 3 Active el formulario (5).

El diseñador de formularios personalizados admite la validación de datos. Para ello, añada restricciones a un campo o a través de un origen de validación externo. Para obtener opciones de restricciones que se apliquen al crear un formulario, consulte [Propiedades de campos del diseñador de formularios personalizados](#). Para obtener un ejemplo de restricción, consulte [Crear un formulario de solicitud personalizado con opciones de Active Directory](#). Para obtener información sobre la validación externa, consulte [Uso de la validación externa en el diseñador de formularios personalizados](#).

La lista de elementos de blueprint incluye propiedades personalizadas a menos que una propiedad se configure para que no se permita la sobrescritura. Si la opción Reemplazable en la propiedad se establece como No, el campo no se puede personalizar.

Acciones de formularios de solicitud personalizados

Los elementos del menú Acción se utilizan para rellenar los formularios y compartirlos con otros sistemas.

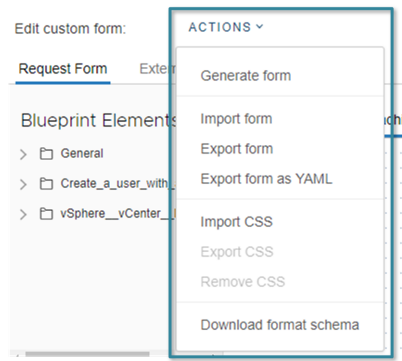


Tabla 3-65. Elementos del menú Acción del formulario de solicitud personalizado

Elemento del menú Acción	Descripción
Generar formulario	<p>Añade todos los campos asociados con cada componente de blueprint al diseñador de formularios. Cada componente se agrega a una pestaña. Si utiliza este elemento de menú después de haber creado o modificado un formulario, el formulario generado sobrescribe el formulario actual.</p> <p>Si utiliza este elemento de menú, puede ocultar o quitar los campos que no desea presentar a los usuarios en el catálogo. Si no genera el formulario, aún así puede añadir y configurar los cuadros de texto que desea que los usuarios vean.</p>
Importar formulario	<p>Importa un archivo JSON o YAML de formulario personalizado.</p>
Exportar formulario	<p>Exporta el formulario personalizado actual como un archivo JSON.</p> <p>Exporte el archivo cuando desee utilizar la parte de él que coincide con un componente que utilice en otro blueprint.</p>
Exportar formulario como YAML	<p>Exporta el formulario personalizado actual como YAML.</p> <p>Exporte el archivo como YAML cuando desee mover un formulario personalizado de una instancia de vRealize Automation a otra. Por ejemplo, moverlo del entorno de prueba al entorno de producción. Si prefiere editar el formulario como YAML, puede exportar el formulario, editarlo y luego volver a importarlo en el blueprint.</p>

Tabla 3-65. Elementos del menú Acción del formulario de solicitud personalizado (continuación)

Elemento del menú Acción	Descripción
Importar CSS	<p>Importa un archivo CSS que mejora el formulario de solicitud de catálogo.</p> <p>El archivo puede ser similar al siguiente ejemplo. En este ejemplo se cambia el tamaño de fuente y se cambia el texto a negrita. El campo al que se hace referencia es el campo de texto Implementar máquina con la cuenta de usuario de Active Directory, el cual aparece en la imagen ubicada en la sección Diseñador de formularios de solicitud personalizados que se muestra anteriormente.</p> <pre>#<field-ID> .grid-item { font-size: 16px; font-weight: bold; width: 600px; }</pre> <p>En este ejemplo, <field-ID> es el identificador del campo en el lienzo. Para localizar el valor, seleccione el campo en el lienzo. El valor se encuentra en el panel derecho, debajo del nombre. En la imagen anterior, el valor es text_d947bc97.</p> <p>Para importar el archivo, guárdelo como <nombre_de_archivo>.css.</p>
Exportar CSS	Exporta el CSS importado.
Quitar CSS	<p>Descarta el CSS personalizado.</p> <p>El CSS descartado no se puede recuperar.</p>
Descargar esquema de formato	<p>Descarga un archivo JSON que contiene la estructura y la descripción de los controles y los estados utilizados en un formulario personalizado.</p> <p>Puede utilizar este esquema para crear un formulario o modificar uno existente. Puede importar el archivo JSON modificado como el formulario personalizado.</p>

Crear un formulario de solicitud personalizado con opciones de Active Directory

Los formularios personalizados se crean cuando el formulario predeterminado proporciona al usuario solicitante demasiada información o información insuficiente. Puede añadir más campos al formulario y ocultar campos de un formulario, así como rellenar campos previamente, y mostrarlos u ocultarlos.

Este caso de uso se basa en un blueprint que contiene un tipo de máquina virtual de vSphere y un blueprint de XaaS que configura una cuenta de administrador de Active Directory en la máquina virtual. El blueprint de XaaS está basado en el flujo de trabajo Crear un usuario con contraseña en un grupo.

El objetivo de este caso de uso es el siguiente:

- Ofrecer al usuario la opción de configurar la contraseña de administrador.
- Preconfigurar los detalles de la máquina de modo que los valores de CPU y memoria se basen en GB.

¿Qué ventajas ofrece este caso de uso? El caso de uso incluye ejemplos de las siguientes personalizaciones de formulario:

- Agregar campos específicos a un formulario en blanco.
- Configurar una casilla para mostrar u ocultar elementos.
- Ocultar campos hasta que el usuario solicitante active una casilla.
- Agregar validación a los campos.
- Mostrar un campo de memoria en GB aunque el campo del blueprint se calcule en MB.
- Usar expresiones regulares.

Requisitos previos

- Inicie sesión en vRealize Automation como **arquitecto de aplicaciones, arquitecto de software o arquitecto de infraestructura**.
- Cree una máquina YourCo y un blueprint Usuario que incluya un blueprint de vSphere y otro de XaaS para crear una cuenta de usuario de Active Directory con una contraseña en un grupo. Para ver un ejemplo, consulte [Crear un blueprint XaaS para crear un usuario](#).

Procedimiento

- 1 Seleccione **Diseño > Blueprints**.
- 2 Resalte la fila que contenga la máquina YourCo y el blueprint Usuario, y haga clic en **Formulario personalizado > Editar**.
- 3 Cambie el nombre de la pestaña General.
 - a Haga clic en la pestaña.
 - b En la propiedad **Título** del panel de propiedad de la derecha, escriba **Configuración**.

- 4 En la nueva pestaña Configuración, añada y configure los siguientes campos con los valores proporcionados.

The screenshot shows the 'Edit custom form' interface in vRealize Automation. The 'Request Form' tab is selected, and the 'Configuration' sub-tab is active. The form contains the following fields:

- Deploy Machine with Active Directory User Account**: A text field with a value of 'Deploy Machine with Active Directory User Account'.
- Description**: A text field with a value of 'Description'.
- Number of Deployments**: A text field with a value of 'Number of Deployments'.
- Add Active Directory account**: A checkbox labeled 'Add Active Directory account'.
- Username**: A text field with a value of 'Username'.
- Password**: A text field with a value of 'Password'.
- Confirm password**: A text field with a value of 'Confirm password'.
- Email**: A text field with a value of 'Email'.
- I have read and accept the software policy**: A checkbox labeled 'I have read and accept the software policy'.

The 'Configuration' tab is also visible on the right side of the form, showing a 'Field ID: general' and a 'Title' field with the value 'Configuration'.

Utilice los valores proporcionados para Apariencia, Valores y Restricciones.

Resuelve los errores durante la compilación del formulario.

Campo en la captura de pantalla	Origen de los elementos de blueprint	Apariencia	Valores	Restricciones
Implementar máquina con la cuenta de usuario de Active Directory	Elementos genéricos > Texto	Etiqueta y tipo <ul style="list-style-type: none"> ■ Tipo de visualización: texto Visibilidad <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Visible: sí 	Valor predeterminado <ul style="list-style-type: none"> ■ Valor predeterminado: Implementar máquina con la cuenta de usuario de Active Directory ■ Origen del valor: constante 	
Motivo de la solicitud	Elementos del blueprint > vSphere_vCenter_Machine > Descripción	Etiqueta y tipo <ul style="list-style-type: none"> ■ Etiqueta: Motivo de la solicitud ■ Tipo de visualización: campo de texto Visibilidad <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Visible: sí Solo lectura <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Solo lectura: no Ayuda personalizada <ul style="list-style-type: none"> ■ Ayuda de poste indicador: Escriba el motivo de la solicitud. 		Obligatoria <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Obligatorio: sí

Campo en la captura de pantalla	Origen de los elementos de blueprint	Apariencia	Valores	Restricciones
Número de implementaciones	Elementos del blueprint > General > Número de implementaciones	Etiqueta y tipo <ul style="list-style-type: none"> ■ Etiqueta: Número de implementaciones ■ Tipo de visualización: entero Visibilidad <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Visible: sí Solo lectura <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Solo lectura: no Ayuda personalizada <ul style="list-style-type: none"> ■ Ayuda de poste indicador: Seleccione el número de instancias del blueprint que se implementarán. 	Valor predeterminado <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Valor predeterminado: 1 	Obligatoria <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Obligatorio: sí ■ Valor mínimo: 1
Casilla "Añadir cuenta de Active Directory"	Elementos genéricos > Casilla	Etiqueta y tipo <ul style="list-style-type: none"> ■ Etiqueta: Añadir cuenta de Active Directory ■ Tipo de visualización: casilla Visibilidad <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Visible: sí 		

Campo en la captura de pantalla	Origen de los elementos de blueprint	Apariencia	Valores	Restricciones
Nombre de usuario	Elementos del blueprint > Crear un usuario con contraseña en un grupo > El nombre de cuenta del usuario	<p>Etiqueta y tipo</p> <ul style="list-style-type: none"> ■ Etiqueta: Nombre de usuario ■ Tipo de visualización: campo de texto <p>Visibilidad</p> <p>Nota Esta propiedad de visibilidad, que se configura del mismo modo en los campos subsiguientes, oculta el campo a menos que se active la casilla Añadir cuenta de Active Directory.</p> <ul style="list-style-type: none"> ■ Origen del valor: valor condicional ■ Expresión: <ul style="list-style-type: none"> Establecer valor: sí Si Añadir cuenta de Active Directory es igual a Sí <p>Ayuda personalizada</p> <ul style="list-style-type: none"> ■ Ayuda de poste indicador: Escriba el nombre de usuario del administrador. 	<p>Valor predeterminado</p> <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Valor predeterminado: admin 	<p>Obligatoria</p> <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Obligatorio: sí <p>Expresión regular</p> <p>Nota Las expresiones regulares deben seguir la sintaxis de JavaScript.</p> <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Expresión regular: "^[a-z]*\$" ■ Mensaje de error de validación: El nombre de usuario no puede contener caracteres especiales ni números.

Campo en la captura de pantalla	Origen de los elementos de blueprint	Apariencia	Valores	Restricciones
Contraseña	Elementos del blueprint > Crear un usuario con contraseña en un grupo > La contraseña que se establecerá para la cuenta recién creada	<p>Etiqueta y tipo</p> <ul style="list-style-type: none"> ■ Etiqueta: Contraseña ■ Tipo de visualización: contraseña <p>Visibilidad</p> <ul style="list-style-type: none"> ■ Origen del valor: valor condicional ■ Expresión: Establecer valor: sí <p>Si Añadir cuenta de Active Directory es igual a Sí</p> <p>Ayuda personalizada</p> <ul style="list-style-type: none"> ■ Ayuda de poste indicador: Proporcione la contraseña de la cuenta del administrador. 		<p>Obligatoria</p> <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Obligatorio: sí <p>Expresión regular</p> <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Expresión regular: "^(?=.*[A-Z])(?=.*[O-9])(?=.*[a-z]).{8,}\$" ■ Mensaje: La contraseña de administrador debe tener al menos ocho caracteres y puede incluir caracteres alfanuméricos y especiales.

Campo en la captura de pantalla	Origen de los elementos de blueprint	Apariencia	Valores	Restricciones
Confirmar contraseña	Elementos del blueprint > Crear un usuario con contraseña en un grupo > Confirmación de la contraseña	Etiqueta y tipo ■ Etiqueta: Confirmar contraseña Tipo de visualización: contraseña Visibilidad ■ Origen del valor: valor condicional ■ Expresión: Establecer el valor como Sí Si Añadir cuenta de Active Directory es igual a Sí Ayuda personalizada ■ Ayuda de poste indicador: Vuelva a escribir la contraseña de la cuenta del administrador.		Obligatoria ■ Origen del valor: constante ■ Obligatorio: sí Campo de coincidencia ■ Campo de coincidencia: Contraseña

Campo en la captura de pantalla	Origen de los elementos de blueprint	Apariencia	Valores	Restricciones
Correo electrónico	Elementos genéricos > Campo de texto	Etiqueta y tipo <ul style="list-style-type: none"> ■ Etiqueta: Correo electrónico ■ Tipo de visualización: campo de texto Visibilidad <ul style="list-style-type: none"> ■ Origen del valor: valor condicional ■ Expresión: <div> Establecer valor: sí Si Añadir cuenta de Active Directory es igual a Sí </div> Ayuda personalizada <ul style="list-style-type: none"> ■ Ayuda de poste indicador: Escriba la dirección de correo electrónico del administrador. 	Valor predeterminado <ul style="list-style-type: none"> ■ Origen del valor: valor calculado ■ Operador: concatenación ■ Añadir valor: campo; seleccione el nombre de usuario ■ Añadir valor: constante; escriba @yourco.com 	Expresión regular <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Expresión regular: "^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\$" ■ Mensaje de error de validación: Proporcione una dirección de correo electrónico válida.
Casilla "He leído y acepto la política del software".	Elementos genéricos > Casilla	Etiqueta y tipo <ul style="list-style-type: none"> ■ Etiqueta de elemento: He leído y acepto la política del software ■ Tipo de visualización: casilla Visibilidad <ul style="list-style-type: none"> ■ Origen del valor: valor condicional ■ Expresión: <div> Establecer valor: sí Si Añadir cuenta de Active Directory es igual a Sí </div> 		

- 5 Haga clic en **Añadir pestaña** y escriba **Detalles de máquina** en la propiedad **Título** de la derecha.

6 Configure los siguientes campos en la pestaña Detalles de máquina.

Edit custom form: **ACTIONS** Activate custom form ☒ ?

Request Form External Validations

Blueprint Elements ?

- General
- Create_a_user_with_a_pas...
- vsphere_vCenter_Machi
 - ☒ Authentication nee...
 - 123 CPUs Added
 - Clone from name
 - Clone from snapsh...

Generic Elements ?

- Text Area
- Text Field
- Text
- Password
- O.O
- 123

Configuration **Machine Details** ADD TAB

Machine Details ?
 Field ID: page_beda904

Title Machine Details

Visibility y

Edit Blueprint Save Finish Cancel

Utilice los valores proporcionados para Apariencia, Valores y Restricciones.

Campo en la captura de pantalla	Origen de los elementos de blueprint	Apariencia	Valores	Restricciones
Almacenamiento (GB)	Elementos del blueprint > vSphere_vCenter_Machine > Almacenamiento (GB)	Etiqueta y tipo <ul style="list-style-type: none"> ■ Etiqueta: Almacenamiento (GB) ■ Tipo de visualización: entero Visibilidad <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Visibilidad: sí Solo lectura <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Solo lectura: no 	Valor predeterminado <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Valor predeterminado: 4 	Valor mínimo <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Valor mínimo: 2
Número de CPU	Elementos del blueprint > vSphere_vCenter_Machine > CPU	Etiqueta y tipo <ul style="list-style-type: none"> ■ Etiqueta: Número de CPU ■ Tipo de visualización: entero Visibilidad <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Visibilidad: sí 	Valor predeterminado <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Valor predeterminado: 1 	Valor mínimo <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Valor mínimo: 1
Memoria (GB)	Elementos genéricos > Entero	Etiqueta y tipo <ul style="list-style-type: none"> ■ Etiqueta: Memoria (GB) ■ Tipo de visualización: entero Visibilidad <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Visibilidad: sí 	Valor predeterminado <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Valor predeterminado: 1 	Valor mínimo <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Valor mínimo: 1
Memoria (MB)	Elementos del blueprint > vSphere_vCenter_Machine > Memoria (MB)	Etiqueta y tipo <ul style="list-style-type: none"> ■ Etiqueta: Memoria (MB) ■ Tipo de visualización: entero Visibilidad <ul style="list-style-type: none"> ■ Origen del valor: constante ■ Visibilidad: no 	Valor predeterminado <ul style="list-style-type: none"> ■ Origen del valor: valor calculado ■ Operador: multiplicación ■ Añadir valor: campo; seleccione la memoria (GB) ■ Añadir valor: constante; escriba 1024 	

- 7 Resuelva los errores. Puede guardar el formulario, pero este no se activará hasta que no haya errores.
- 8 Para guardar el formulario y cerrar el diseñador de formularios, haga clic en **Finalizar**.
- 9 Seleccione el blueprint y haga clic en **Publicar**.
- 10 Para que el formulario personalizado esté disponible cuando los usuarios lo soliciten en el catálogo de servicios, seleccione **Formulario personalizado > Activar** en la barra de herramientas de la página Blueprints.

Pasos siguientes

- Asegúrese de que el blueprint esté disponible en el catálogo de servicios. Consulte [Administrar el catálogo de servicios](#).
- En el catálogo, compruebe que el formulario de solicitud sea similar al siguiente ejemplo.

The image displays two overlapping screenshots of the vRealize Automation 'New Request' form. The top screenshot shows the 'Machine Details' tab, which includes fields for 'Storage (GB)' (4), 'Number of CPUs' (1), and 'Memory (GB)' (1). The bottom screenshot shows the 'Configuration' tab, which includes a section titled 'Deploy Machine with Active Directory User Account'. This section contains fields for 'Reason for Request', 'Number of Deployments' (1), 'Add Active Directory account' (checked), 'Username' (admin), 'Password', 'Confirm password', and 'Email' (admin@yourco.com). There is also a checkbox for 'I have read and accept the software policy'. Both screenshots show a navigation bar at the top with links to Home, Catalog, Items, Requests, Inbox, Design, Administration, Infrastructure, and Containers. The bottom screenshot also shows 'Save', 'Submit', and 'Cancel' buttons at the bottom right.

Propiedades de campos del diseñador de formularios personalizados

Las propiedades de los campos determinan el aspecto que tiene el campo seleccionado y los valores predeterminados que se presentan al usuario. También determinan las reglas que desea

aplicar al campo para garantizar que el usuario proporcione una entrada válida en el formulario de solicitud de catálogo en vRealize Automation.

Configure cada campo de forma individual. Seleccione el campo y edite sus propiedades.

Origen de valor

Para muchas de las propiedades, puede seleccionar de entre diversas opciones de origen de valor. No todas las opciones de origen están disponibles para todos los tipos de campos o propiedades.

- **Constante.** El valor no cambia. En función de la propiedad, el valor puede ser una cadena, un entero o una expresión regular, o bien se puede seleccionar de una lista limitada (por ejemplo, Sí o No). Por ejemplo, puede proporcionar 1 como un entero de valor predeterminado, seleccionar No para la propiedad Solo lectura o proporcionar la expresión regular para validar una entrada de campo.
- **Valor condicional** El valor se basa en una o varias condiciones. Las condiciones se procesan en el orden indicado. Si más de una condición tiene el valor true, la última condición que tiene dicho valor determina el comportamiento del campo para esa propiedad. Por ejemplo, puede crear una condición que determina si se muestra un campo en función del valor de otro campo.
- **Origen externo.** El valor se basa en los resultados de una acción de vRealize Orchestrator. Por ejemplo, el cálculo de los costes en función de una acción de vRealize Orchestrator generada por script. Para ver un ejemplo, consulte [Usar acciones de vRealize Orchestrator en el diseñador de formularios personalizados](#).
- **Enlazar campo.** El valor es el mismo que el campo al que está enlazado. Los campos disponibles están limitados al mismo tipo de campo. Por ejemplo, se enlaza el valor predeterminado de un campo de casilla de verificación de autenticación necesaria a otro campo de casilla de verificación. Cuando se activa una casilla de verificación del campo de destino en el formulario de solicitud, se activa la casilla de verificación en el campo actual.
- **Valor computado.** El valor se determina en función de cómo el operador procesa los campos y los valores seleccionados. Los campos de texto usan el operador de concatenación. Los campos de enteros utilizan las operaciones de suma, resta, multiplicación o división seleccionadas. Por ejemplo, puede configurar un campo de entero para convertir megabytes en gigabytes utilizando la operación de multiplicación.

Apariencia del campo

Las propiedades de apariencia se utilizan para determinar si el campo aparece en el formulario, así como la etiqueta y la ayuda personalizada que desea proporcionar a los usuarios del catálogo.

Tabla 3-66. Opciones de la pestaña Apariencia

Opción	Descripción
Etiqueta y tipo	<p>Proporciona una etiqueta y selecciona un tipo de visualización.</p> <p>Los tipos de visualización disponibles dependen del campo. Algunos campos admiten varios tipos de texto y otros solo admiten enteros. Valores posibles:</p> <ul style="list-style-type: none"> ■ Decimal ■ Menú desplegable ■ Imagen ■ Entero ■ Selección múltiple ■ Contraseña ■ Grupo de botones de opción ■ Texto ■ Área de texto ■ Campos de texto <p>Los campos de menú desplegable y cuadrícula de datos incluyen una opción Marcador de posición. El valor introducido aparece como una etiqueta interna o como instrucciones en el menú desplegable, o como instrucciones o etiqueta general en la cuadrícula de datos.</p>
Visibilidad	<p>Muestra u oculta un campo del formulario de solicitud.</p> <ul style="list-style-type: none"> ■ Constante. Seleccione Sí para mostrar el campo en el formulario. Seleccione No para ocultar el campo. ■ Valor condicional La visibilidad está determinada por la primera expresión que tiene el valor true. Por ejemplo, un campo se puede ver si se activa una casilla de verificación en un formulario. ■ Origen externo. La visibilidad se define en función de los resultados de la acción de vRealize Orchestrator seleccionada.
Solo lectura	<p>Impide que los usuarios cambien los valores del campo.</p> <ul style="list-style-type: none"> ■ Constante. Seleccione Sí para mostrar el valor sin permitir que se realicen cambios o No para permitirlo. ■ Valor condicional El estado se establece en función de la primera expresión que tiene el valor true. Por ejemplo, un campo es de solo lectura si el valor de un campo de almacenamiento es superior a 2 GB. ■ Origen externo. El estado se establece según los resultados de la acción de vRealize Orchestrator seleccionada.

Tabla 3-66. Opciones de la pestaña Apariencia (continuación)

Opción	Descripción
Filas por página	Solamente para los elementos de cuadrícula de datos. Introduzca el número de filas.
Ayuda personalizada	Proporciona información acerca del campo a los usuarios. Esta información aparece en la ayuda de poste indicador del campo. Puede utilizar texto simple o HTML, incluidos vínculos HREF. Por ejemplo, <code>vRealize Automation documentation</code> .

Valores de campos

Las propiedades de los valores se utilizan para proporcionar valores predeterminados.

Tabla 3-67. Opciones de la pestaña Valores

Opción	Descripción
Columnas	Solamente para el elemento de cuadrícula de datos. Proporciona la etiqueta, el identificador y el tipo de valor de cada columna de la tabla. El valor predeterminado de la cuadrícula de datos debe incluir los datos del encabezado que coincidan con las columnas definidas. Por ejemplo, si dispone de un identificador user_name para una columna y un identificador user_role para otra, la primera fila es user_name,user_role. Para ver ejemplos de configuración, consulte Usar el elemento de cuadrícula de datos en el diseñador de formularios personalizados .
Valor predeterminado	Rellena el campo con un valor predeterminado en función del origen de valor. Los posibles orígenes de valor dependen del campo. <ul style="list-style-type: none"> ■ Constante. La cadena que se ha introducido. ■ Valor condicional El valor predeterminado se establece en función de la primera expresión que tiene el valor true. Por ejemplo, el valor predeterminado de un campo de almacenamiento es 1 GB si el campo de memoria es inferior a 512 MB. ■ Origen externo. El valor se basa en los resultados de la acción de vRealize Orchestrator seleccionada. ■ Enlazar campo. El valor es igual al del campo seleccionado. ■ Valor computado. El valor se basa en los resultados de los valores de campo que se proporcionan y el operador seleccionado. Por ejemplo, el valor predeterminado de memoria en MB se basa en la memoria en GB multiplicado por 1.024.

Tabla 3-67. Opciones de la pestaña Valores (continuación)

Opción	Descripción
Opción de valor	<p>Rellena los campos de un menú desplegable, una selección múltiple, un grupo de botones de opción o un selector de valores.</p> <ul style="list-style-type: none"> ■ Constante. El formato de la lista es Valor Etiqueta,Valor Etiqueta,Valor Etiqueta. Por ejemplo, 2 Small,4 Medium,8 Large. ■ Origen externo. El valor se basa en los resultados de la acción de vRealize Orchestrator seleccionada.
Paso	<p>Para campos de enteros o decimales, define los valores que aumentan o disminuyen.</p> <p>Por ejemplo, si el valor predeterminado es 1 y establece el valor de paso en 3, los valores permitidos son 4, 7, 10 y así sucesivamente.</p>

Restricciones de campo

Las propiedades de restricción se utilizan para garantizar que el usuario solicitante proporciona valores válidos en el formulario de solicitud.

También se puede utilizar la validación externa como un método alternativo para garantizar valores válidos. Consulte [Uso de la validación externa en el diseñador de formularios personalizados](#).

Tabla 3-68. Opciones de la pestaña Restricciones

Opción	Descripción
Obligatorio	<p>El usuario solicitante debe proporcionar un valor para este campo.</p> <ul style="list-style-type: none"> ■ Constante. Seleccione Sí para exigir que el usuario que realiza la solicitud proporcione un valor o No si el campo es opcional. ■ Valor condicional Para determinar que el campo es obligatorio, la primera expresión debe tener el valor true. Por ejemplo, este campo es obligatorio si la familia del sistema operativo empieza con Darwin en otro campo. ■ Origen externo. El estado se basa en los resultados de la acción de vRealize Orchestrator seleccionada.
Expresión regular	<p>Proporciona una expresión regular que valida el valor y un mensaje que aparece cuando se produce un error en la validación.</p> <p>Las expresiones regulares deben seguir la sintaxis de JavaScript. Para obtener a una descripción general, consulte Creación de una expresión regular. Para obtener instrucciones más detalladas, consulte Sintaxis.</p> <ul style="list-style-type: none"> ■ Constante. Proporciona una expresión regular. Por ejemplo, para una dirección de correo electrónico, la expresión regular podría ser <code>^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\$</code> y el mensaje de error de validación es El formato de dirección de correo electrónico no es válido. Inténtelo de nuevo. ■ Valor condicional La expresión regular que se utiliza se establece en función de la primera expresión que tiene el valor true.
Valor mínimo	<p>Especifica un valor numérico mínimo. Por ejemplo, una contraseña debe tener al menos 8 caracteres.</p> <p>Proporciona un mensaje de error, como por ejemplo: La contraseña debe tener al menos 8 caracteres.</p> <ul style="list-style-type: none"> ■ Constante. Introduce el entero. ■ Valor condicional El valor mínimo se establece en función de la primera expresión que tiene el valor true. Por ejemplo, un valor mínimo de CPU es 4 si el sistema operativo es distinto de Linux. ■ Origen externo. El valor se basa en los resultados de la acción de vRealize Orchestrator seleccionada.

Tabla 3-68. Opciones de la pestaña Restricciones (continuación)

Opción	Descripción
Valor máximo	<p>Valor numérico máximo. Por ejemplo, un campo está limitado a 50 caracteres.</p> <p>Proporciona un mensaje de error, Por ejemplo: Esta descripción no puede superar los 50 caracteres.</p> <ul style="list-style-type: none"> ■ Constante. Introduce el entero. ■ Valor condicional El valor máximo se establece en función de la primera expresión que tiene el valor true. Por ejemplo, un valor máximo de almacenamiento es de 2 GB si la ubicación de implementación es igual a AMEA. ■ Origen externo. El valor se basa en los resultados de la acción de vRealize Orchestrator seleccionada.
Campo de coincidencia	<p>Este valor de campo debe coincidir con el valor de campo seleccionado.</p> <p>Por ejemplo, un campo de confirmación de contraseña debe coincidir con el campo de contraseña.</p>

Usar acciones de vRealize Orchestrator en el diseñador de formularios personalizados

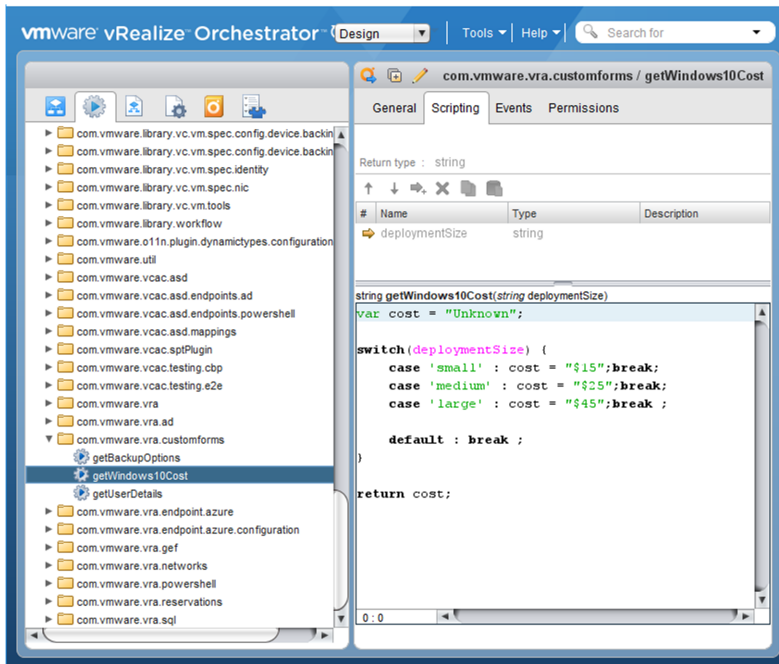
Cuando personaliza el formulario de solicitud para un blueprint de vRealize Automation, puede basar el comportamiento de algunos campos en los resultados de una acción de vRealize Orchestrator.

Existen varias formas de utilizar las acciones de vRealize Orchestrator. Puede tener una acción que extraiga los datos de un tercer origen, o bien puede usar un script que defina el tamaño y el coste. En este ejemplo se utiliza un script.

Ejemplo: Ejemplo de los campos de tamaño y coste

En este caso de uso, se desea que el usuario del catálogo seleccione un tamaño de la máquina virtual y, a continuación, muestre el coste de esa máquina por día. Para llevar a cabo este ejemplo, tiene una instancia de vRealize Orchestrator que correlaciona el tamaño y el coste, y añade un campo de tamaño y un campo de coste al formulario personalizado del blueprint. El campo del tamaño determina el valor que aparece en el campo del coste.

- 1 En vRealize Orchestrator, configure una acción (getWindows10Cost) con un script deploymentSize similar al siguiente ejemplo.



Utilice lo que se indica a continuación como un ejemplo de script.

```
var cost = "Unknown";

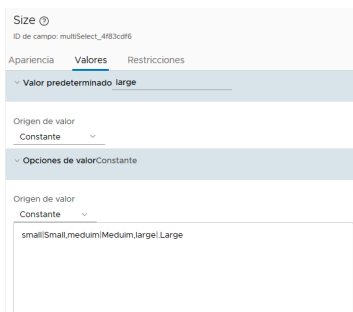
switch(deploymentSize) {
    case 'small' : cost = "$15";break;
    case 'medium' : cost = "$25";break;
    case 'large' : cost = "$45";break ;

    default : break ;
}

return cost;
```

- 2 En vRealize Automation, añada un campo de tamaño y un campo de coste a un formulario personalizado de blueprint, y configúrelos.

Configure el campo de tamaño para que sea de selección múltiple con los valores Pequeño, Mediano y Grande.



En vRealize Automation, añada un campo de tamaño y un campo de coste a un formulario personalizado de blueprint, y configúrelos.

En la pestaña Valores, configure los siguientes valores de propiedad.

- Valor predeterminado: **Grande**
- Opciones de valor
 - Origen del valor: **constante**
 - Definición de valor: **pequeño | Pequeño, mediano | Mediano, grande | Grande**

- 3 Configure el campo de coste para que muestre el coste según se define en la acción de vRealize Orchestrator en función del valor seleccionado en el campo de tamaño.

Cost ⓘ
Field ID: cost

Appearance **Values** Constraints

▼ Default value External source

Value source External source ▼

Select action com.vmware.vra.customforms/getWindows10Cost

Action inputs

deploymentSize Field ▼ Size ▼

En la pestaña Valores, configure los siguientes valores de propiedad.

- Valor predeterminado: Origen externo
- Seleccionar acción: <carpeta de acciones de vRealize Orchestrator>/getWindows10Cost
- Entradas de acción
 - deploymentSize. Este valor se configuró en la acción.
 - Campo
 - Tamaño

Usar el elemento de cuadrícula de datos en el diseñador de formularios personalizados

Cuando se personaliza el formulario de solicitud para un blueprint, la información se añade como una de tabla. Los datos que se presentan en la tabla se pueden proporcionar manualmente o basados en un origen externo.

Ejemplo: Ejemplo de datos de CSV proporcionados

En este caso de uso, tiene una tabla de valores que se proporcionan en el formulario de solicitud personalizado. La información se ofrece en la tabla como un origen de valor constante. El origen se basa en una estructura de datos de CSV, en la que la primera fila es el encabezado. Los encabezados son los identificadores de columna separados por comas. Cada fila adicional está formada por los datos que aparecen en cada fila de la tabla.

- 1 Añada el elemento genérico Cuadrícula de datos al lienzo de diseño.
- 2 Seleccione la cuadrícula de datos y defina los valores en el panel de propiedades.

Data Grid ⓘ
Field ID: datagrid_0a3999da

Appearance

Values

Columns

ADD COLUMN

Label

Username

Id

username

Type

String

Label

Employee ID

Id

employeeId

Type

Integer

Label

Manager

Id

manager

Type

String

Default value

Constant

Value source

Constant

CSV

username,employeeId,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai

Etiqueta	ID	Tipo
Nombre de usuario	username	Cadena
Identificador de empleado	employeeId	Entero
Administrador	manager	Cadena

Defina los valores de CSV.

```
username,employeeId,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

3 Compruebe que la cuadrícula de datos muestre los datos previstos en el formulario de solicitud del blueprint.

+

−

<input type="checkbox"/>	Username	Employee ID	Manager
<input checked="" type="checkbox"/>	leonardo	95621	Farah
<input type="checkbox"/>	vindhya	15496	Farah
<input type="checkbox"/>	martina	52648	Nikolai
<div><div><input checked="" type="checkbox"/> 1</div><div></div></div> <div>1 - 3 de 3</div>			

VMware, Inc.

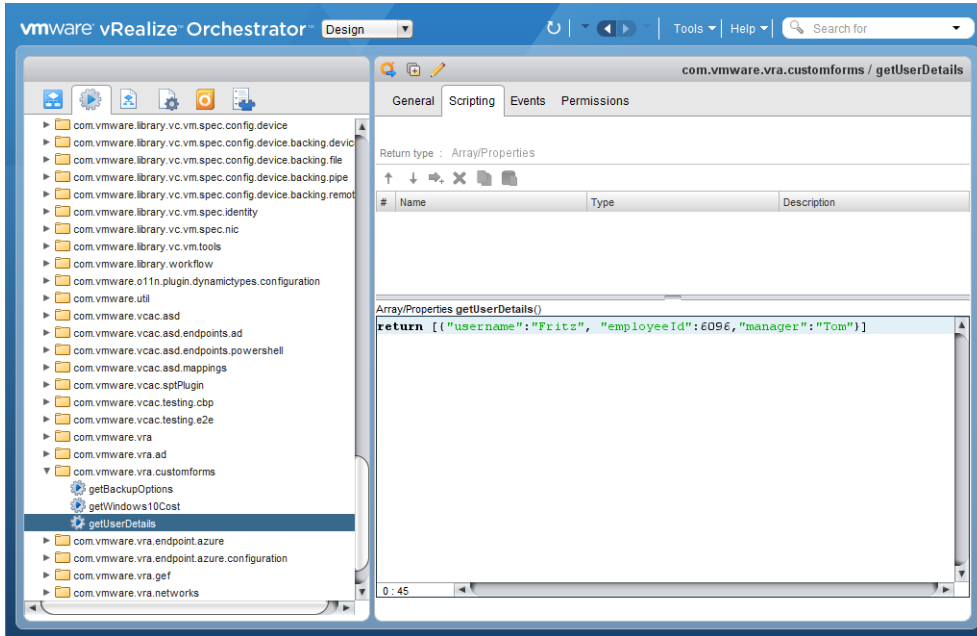
631

Ejemplo: Ejemplo de un origen externo

Este ejemplo utiliza el ejemplo anterior, pero los valores se basan en una acción de vRealize Orchestrator. A pesar de que se trata de un ejemplo de acción simple, puede usar una acción más compleja que recupere esta información de un sistema o una base de datos locales.

La acción que se utiliza como validación debe tener un parámetro de entrada Matriz/Propiedades.

- 1 En vRealize Orchestrator, configure una acción (getUserDetails) con una matriz similar a la del siguiente ejemplo.



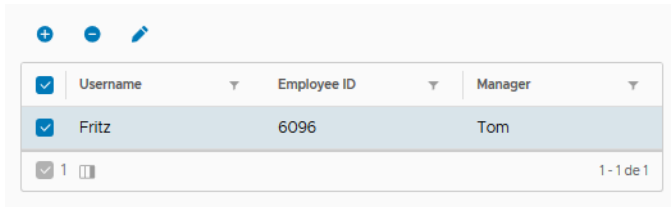
Utilice el siguiente script de ejemplo.

```
return [{"username": "Fritz", "employeeId": 6096, "manager": "Tom"}]
```

- 2 En vRealize Automation, añada la cuadrícula de datos y configure las columnas de la cuadrícula de datos con los siguientes valores.

Etiqueta	ID	Tipo
Nombre de usuario	username	Cadena
Identificador de empleado	employeeId	Entero
Administrador	manager	Cadena

- 3 En la lista Origen de valor, seleccione **Origen externo**.
- 4 En Seleccionar acción, introduzca getUserDetails y seleccione la acción que creó en vRealize Orchestrator.
- 5 Guarde la tabla y compruébela en el formulario de solicitud.



<input checked="" type="checkbox"/>	Username	Employee ID	Manager
<input checked="" type="checkbox"/>	Fritz	6096	Tom

1 1-1 de 1

Uso de la validación externa en el diseñador de formularios personalizados

Los formularios de solicitud se pueden personalizar para garantizar que los usuarios proporcionen valores válidos en el momento de la solicitud añadiendo restricciones a los campos o empleando un origen de validación externo.

Algunas propiedades de campos (como los mínimos, los máximos, las expresiones regulares, los campos de coincidencia o la obligatoriedad de rellenar un campo), se pueden configurar con restricciones para garantizar que los valores sean válidos. Consulte [Propiedades de campos del diseñador de formularios personalizados](#).

En la validación externa se comprueban los valores válidos de un origen externo mediante acciones de vRealize Orchestrator.

Si planea validar un valor de cuadrícula de datos, la acción que utilice como validación debe tener un parámetro de entrada Matriz/Propiedades.

Algunos posibles ejemplos de uso de la validación externa son:

- Los valores válidos se definen en un origen externo. Por ejemplo, vRealize Orchestrator.
- La validación debe afectar a varios campos. Por ejemplo, una acción de vRealize Orchestrator recopila el tamaño de disco y la capacidad del grupo de almacenamiento, y valida los valores de tamaño proporcionados en función del espacio disponible.

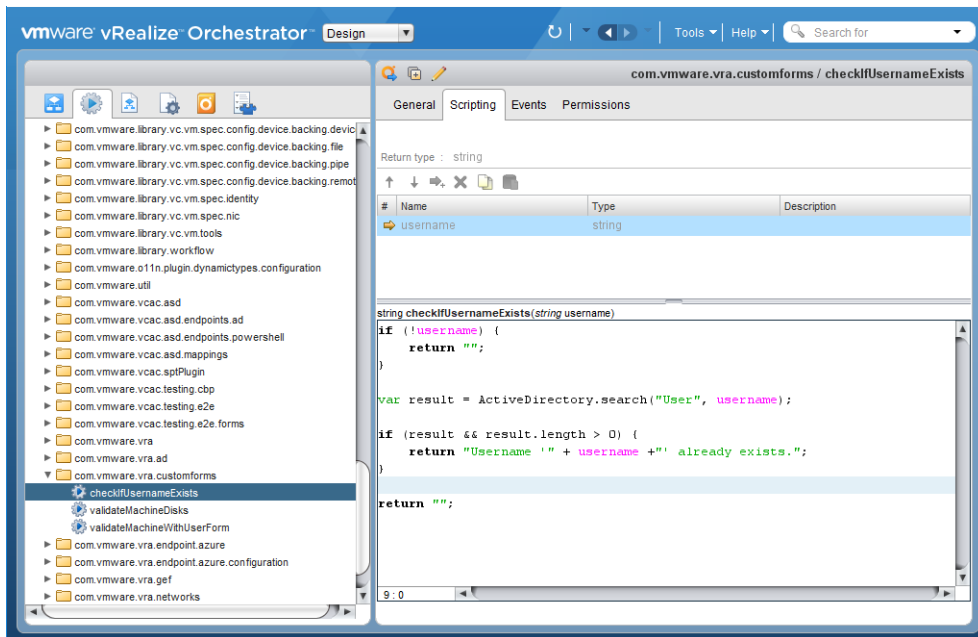
¿Cómo se solicitan varias validaciones externas en un blueprint? Las validaciones se procesan en el orden en el que aparecen en el lienzo de validación externa. Si hay dos validaciones que validan el mismo campo, los resultados de la segunda validación reemplazarán a los de la primera. Para reorganizar las validaciones, puede hacer clic en las tarjetas y arrastrarlas en el lienzo.

Ejemplo: Ejemplo de usuario de vRealize Orchestrator

En este caso de uso, se desea que el usuario del catálogo proporcione únicamente un nombre de usuario nuevo. Para llevar a cabo este ejemplo, tiene una acción de vRealize Orchestrator que comprueba si el nombre de usuario proporcionado en el formulario existe en la base de datos de Active Directory. Si el nombre existe, aparece un mensaje de error en el formulario de solicitud.

Este caso de uso se aplica al ejemplo de [Crear un formulario de solicitud personalizado con opciones de Active Directory](#).

- 1 En vRealize Orchestrator, configure una acción (checkIfUsernameExists) con un script similar al siguiente ejemplo.



Utilice lo que se indica a continuación como un ejemplo de script. En este ejemplo, return es el mensaje que aparece si se produce un error en la validación.

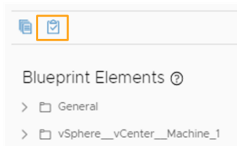
```
if (!username) {
    return "";
}

var result = ActiveDirectory.search("User", username);

if (result && result.length > 0) {
    return "Username '" + username + "' already exists.";
}

return "";
```

- 2 En vRealize Automation, abra el diseñador de formularios personalizados del blueprint, haga clic en **Validación externa** y arrastre el tipo **Validación de Orchestrator** al lienzo.



- 3 Configure las opciones de validación externa.

- Etiqueta de validación: comprueba si el nombre de usuario existe.
- Seleccionar acción: <carpeta de acciones de vRealize Orchestrator>/checkIfUsernameExists
- Entradas de acción
 - Nombre de usuario: Campo y Nombre de usuario
- Campos resaltados
 - Haga clic en **Añadir campo** y seleccione Nombre de usuario.

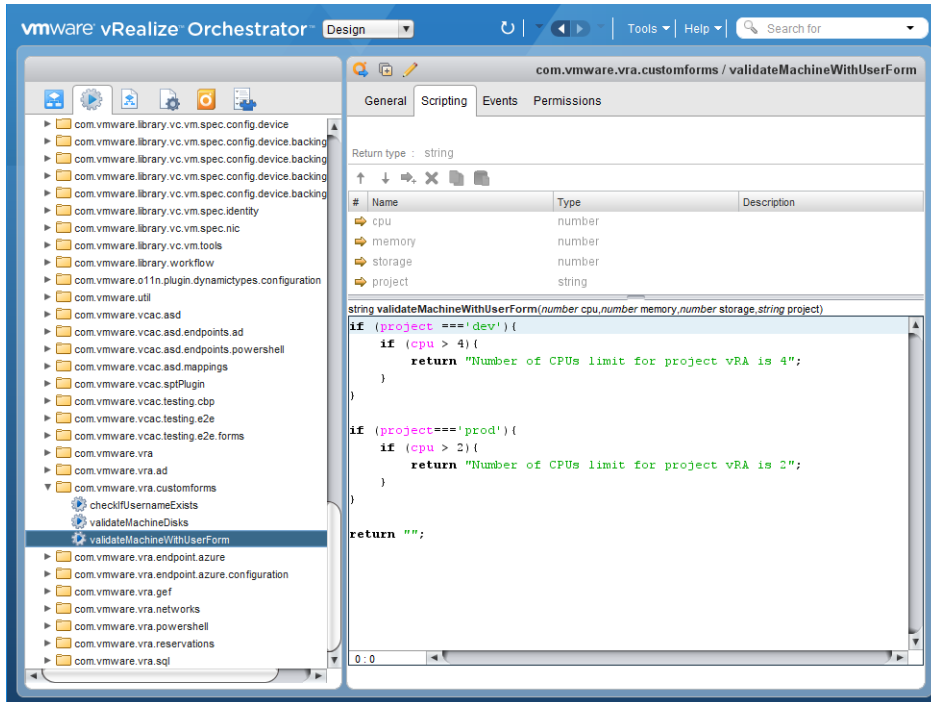
Si el valor introducido no supera la validación, aparece un error de validación de nivel de campo en el formulario de solicitud de catálogo. Si desea un error global, no configure el campo resaltado.

Ejemplo: Ejemplo de varios campos de vRealize Orchestrator

En este caso de uso, se desea basar la validación de los valores de CPU, memoria y almacenamiento en el valor del proyecto. Por ejemplo, si los usuarios seleccionan el proyecto de desarrollo, el número máximo de CPU sería 4. Si seleccionan el de producción, el valor máximo sería 2.

Para este caso de uso, añada un campo de proyecto al ejemplo de [Crear un formulario de solicitud personalizado con opciones de Active Directory](#). Configure el proyecto como un menú desplegable con desarrollo y producción.

- 1 En vRealize Orchestrator, configure una acción (validateMachineWithUserForm) con un script similar al siguiente ejemplo.



Utilice lo siguiente como un ejemplo de script para la comprobación de la CPU. Siga añadiendo los valores de memoria y almacenamiento al script según sea necesario. En este ejemplo, return es el mensaje que aparece si se produce un error en la validación.

```

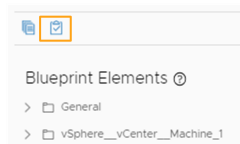
if (project === 'dev'){
    if (cpu > 4){
        return "Number of CPUs limit for project vRA is 4";
    }
}

if (project==='prod'){
    if (cpu > 2){
        return "Number of CPUs limit for project vRA is 2";
    }
}

return "";

```

- En vRealize Automation, abra el diseñador de formularios personalizados del blueprint, haga clic en **Validación externa** y arrastre el tipo **Validación de Orchestrator** al lienzo.



- Configure las opciones de validación externa.

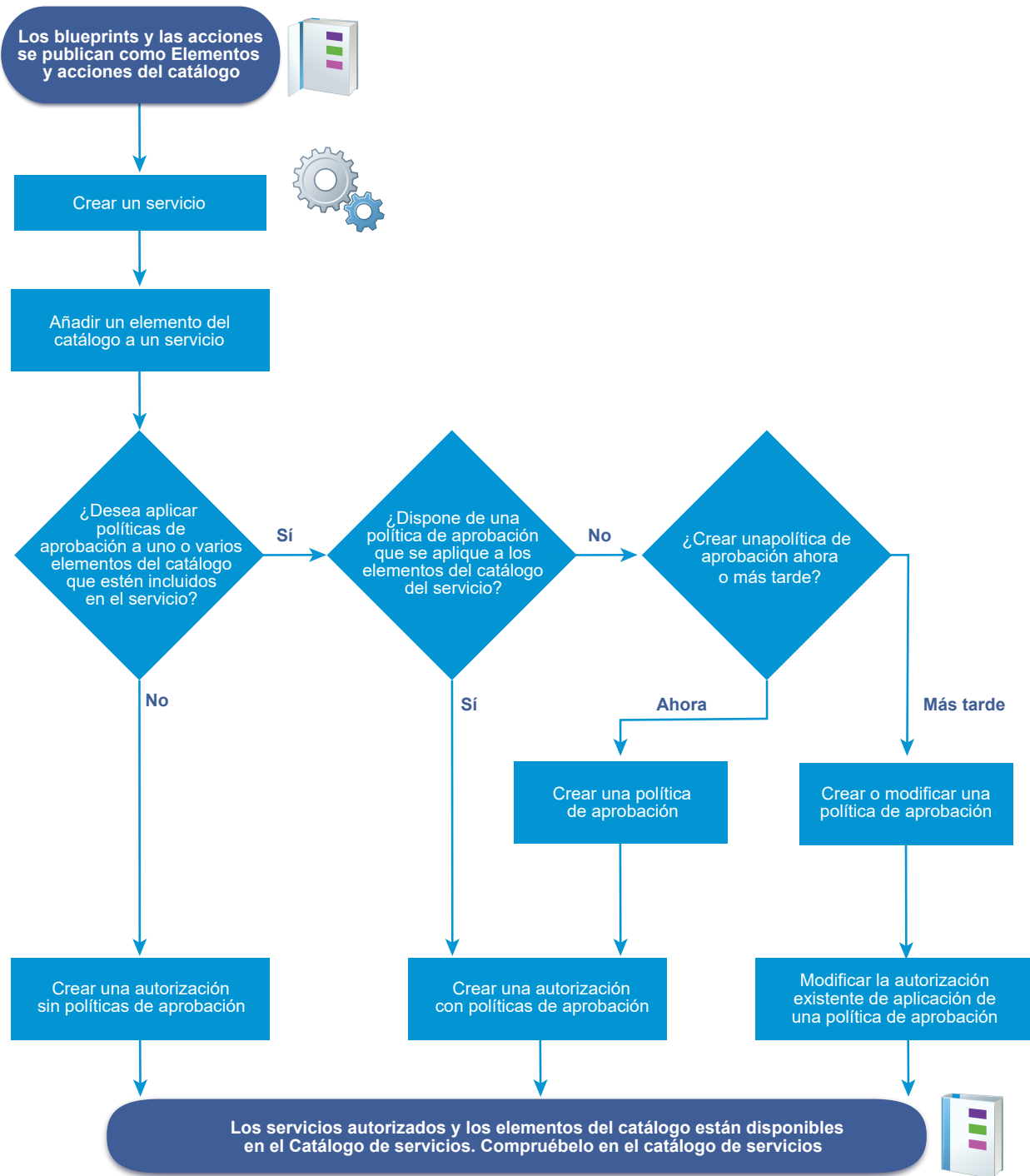
- Etiqueta de validación: Validar detalles de la máquina
- Seleccionar acción: <carpeta de acciones de vRealize Orchestrator>/validateMachineWithUserForm
- Entradas de acción
 - CPU: Campo y Número de CPU
 - Memoria: Campo y Memoria (GB)
 - Almacenamiento: Campo y Almacenamiento (GB)
 - Proyecto: Campo y Proyecto
- Campos resaltados
 - Haga clic en **Añadir campo** y seleccione **Proyecto**.

En el catálogo, el usuario del catálogo podría ver un error de validación similar al del siguiente ejemplo.

Administrar el catálogo de servicios

El catálogo de servicios es donde los clientes solicitan el aprovisionamiento de máquinas y otros elementos para utilizarlos. El acceso de los usuarios a los elementos del catálogo de servicios se administra en función del modo en que se hayan creado los servicios, se haya autorizado a los usuarios para uno o varios elementos, y se haya aplicado gobierno.

El flujo de trabajo para añadir elementos al catálogo de servicios varía en función de si se crean y aplican políticas de aprobación.



Lista de comprobación para configurar el catálogo de servicios

Después de crear y publicar blueprints y acciones, puede crear un servicio de vRealize Automation, configurar elementos del catálogo y asignar autorizaciones y aprobaciones.

La lista de comprobación para configurar el catálogo de servicios proporciona una descripción general de los pasos que debe realizar para configurar el catálogo e incluye vínculos a puntos de decisión o instrucciones detalladas de cada paso.

Tabla 3-69. Lista de comprobación para la configuración del catálogo de servicios

Tarea	Función necesaria	Detalles
<input type="checkbox"/> Añadir un servicio.	Administrador de tenants o administrador del catálogo	Consulte Añadir un servicio .
<input type="checkbox"/> Añadir un elemento del catálogo a un servicio.	Administrador de tenants o administrador del catálogo	Consulte Añadir elementos del catálogo a un servicio .
<input type="checkbox"/> Configurar el elemento del catálogo en el servicio.	Administrador de tenants o administrador del catálogo	Consulte Configurar un elemento del catálogo .
<input type="checkbox"/> Crear y aplicar autorizaciones al elemento del catálogo.	Administrador de tenants o administrador de grupo empresarial	Consulte Autorizar usuarios a servicios, elementos de catálogo y acciones .
<input type="checkbox"/> Crear y aplicar políticas de aprobación al elemento del catálogo.	Administrador de tenants o administrador de aprobaciones; pueden crear políticas de aprobación Administrador de tenants o administrador de grupo empresarial; pueden aplicar políticas de aprobación	Consulte Crear una política de aprobación .

Crear un servicio

Un servicio es un grupo de elementos de catálogo que quiere que se incluya en el catálogo de servicios. Puede autorizar el servicio, de modo que los usuarios de un grupo empresarial estén autorizados a usar todos los elementos del catálogo asociados. Además, puede aplicar una política de aprobación para el servicio.

Un servicio funciona como un grupo dinámico de elementos de catálogo. Si autoriza un servicio, todos los elementos del catálogo asociados a dicho servicio estarán disponibles en el catálogo de servicios para los usuarios especificados y, de igual modo, los elementos de catálogo que añada a un servicio o quite de este influirán en el catálogo de servicios.

Cuando cree el servicio, puede usarlo como una categoría de servicio y, así, acumular ofertas de servicio para los usuarios del catálogo de servicios. Por ejemplo, un servicio de escritorio de Windows que englobe elementos de catálogo de los sistemas operativos Windows 7, 8 y 10, o un servicio de Linux que incluya elementos de los sistemas operativos CentOS y RHEL.

Añadir un servicio

Añada un servicio para poner los elementos del catálogo a disposición de los usuarios del catálogo de servicios. Todos los elementos del catálogo deben estar asociados a un servicio para que sea posible autorizar los elementos a los usuarios.

Cuando se autoriza el servicio a los usuarios, los elementos del catálogo aparecen juntos en el catálogo de servicios. También es posible autorizar a los usuarios los elementos del catálogo de individuales.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador del catálogo**.

Procedimiento

1 Seleccione **Administración > Administración de catálogos > Servicios**.

2 Haga clic en el icono **Nuevo** (+).

3 Escriba un nombre y una descripción.

Estos valores aparecen en el catálogo de servicios para los usuarios del catálogo.

4 Para añadir un icono específico para el servicio en el catálogo de servicios, haga clic en **Examinar** y seleccione una imagen.

Los tipos de archivo de imagen admitidos son GIF, JPG y PNG. La imagen mostrada es de 40 x 40 píxeles. Si no selecciona una imagen personalizada, aparece el icono predeterminado en el catálogo de servicios.

5 Seleccione un estado en el menú desplegable **Estado**.

Opción	Descripción
Inactivo	El servicio no está disponible en el catálogo de servicios. Cuando un servicio tiene este estado, puede asociar elementos del catálogo al servicio, pero no puede autorizar el servicio a los usuarios. Si selecciona Inactivo para un servicio que esté activo y autorizado, este se elimina del catálogo de servicios hasta que lo reactive.
Activo	(Predeterminado) El servicio y los elementos del catálogo asociados están disponibles para autorizarlos a los usuarios y, si están autorizados, pasan a estar disponibles en el catálogo de servicios de dichos usuarios.
Eliminado	Quita el servicio de vRealize Automation. Todos los elementos del catálogo asociados siguen estando presentes, pero los elementos asociados al servicio en el catálogo de servicios ya no están disponibles para los usuarios del catálogo.

6 Configuración del servicio.

Las siguientes opciones de configuración ofrecen información a los usuarios del catálogo de servicios. Estas opciones de configuración no afectan la disponibilidad del servicio.

Opción	Descripción
Horas	Configure la hora coincidente con la disponibilidad del equipo de soporte. La hora se basa en su hora local. Las horas de servicio no pueden abarcar horas de días distintos. Por ejemplo, no es posible establecer un período de horas de servicio desde las 16:00 hasta las 04:00. Para cruzar la medianoche, cree dos autorizaciones. Una autorización de las 16:00 a las 24:00 h, y otra de las 24:00 a las 4:00 h.
Propietario	Especifique el usuario o el grupo de usuarios que es el propietario principal del servicio y de los elementos del catálogo asociados.
Equipo de soporte	Especifique el usuario o el grupo de usuarios personalizado que está disponible para dar soporte a los problemas que encuentren los usuarios del catálogo de servicios durante el aprovisionamiento de elementos asociados al servicio.
Cambiar período	Seleccione una fecha y una hora en las que prevé realizar cambios en el servicio. La fecha y la hora especificadas son meramente informativas y no afectan a la disponibilidad del servicio.

7 Haga clic en **Agregar**.

Pasos siguientes

Asocie elementos del catálogo con un servicio, para que se puedan autorizar usuarios en los elementos. Consulte [Añadir elementos del catálogo a un servicio](#).

Añadir elementos del catálogo a un servicio

Añada elementos del catálogo a servicios para que pueda autorizar a los usuarios a solicitar los elementos del catálogo de servicios. Un elemento del catálogo solo puede estar asociado a un único servicio.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador del catálogo**.
- Compruebe que haya un servicio. Consulte [Añadir un servicio](#).
- Compruebe haya uno o varios elementos del catálogo publicados. Consulte [Configurar un elemento del catálogo](#).

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Servicios**.
- 2 Seleccione el servicio al que desea añadir elementos del catálogo y haga clic en **Administrar elementos del catálogo**.
- 3 Haga clic en el icono **Elementos del catálogo** (+).
 - a Seleccione los elementos del catálogo que se vayan a incluir en este servicio.

El cuadro de diálogo Seleccionar elementos del catálogo solo muestra los elementos que ya no están asociados a un servicio.
 - b Haga clic en **Agregar**.
- 4 Haga clic en **Cerrar**.

Pasos siguientes

- Puede añadir un icono personalizado al elemento del catálogo que aparecerá con el elemento en el catálogo de servicios. Consulte [Configurar un elemento del catálogo](#).
- Autorice a los usuarios a los servicios o elementos del catálogo para que puedan solicitarlos en el catálogo de servicios. Consulte [Crear autorizaciones](#).

Trabajar con elementos del catálogo y acciones

Los elementos del catálogo son blueprints publicados para máquinas, componentes de software y otros objetos. Las acciones del área de administración de catálogos son acciones publicadas que se pueden ejecutar en los elementos del catálogo aprovisionados. Puede usar las listas para determinar cuáles son los blueprints y las acciones que se publican, para ponerlos a disposición de los usuarios del catálogo de servicios.

Elemento del catálogo publicados

Un elemento del catálogo es un blueprint publicado. Los blueprints publicados también se pueden utilizar en otros blueprints. La reutilización de los blueprints en otros blueprints no se muestra en la lista de elementos del catálogo.

Los elementos del catálogo publicados también pueden incluir elementos que solo son componentes de blueprints. Por ejemplo, los componentes de software publicados aparecen como elementos del catálogo, pero solo están disponibles como parte de una implementación.

Los elementos del catálogo de implementación debe estar asociados a un servicio para que puedan ponerse a disposición de los usuarios autorizados en el catálogo de servicios. Solo los elementos activos aparecen en el catálogo de servicios. Puede configurar elementos del catálogo en un servicio diferente, desactivarlo si desea quitarlo temporalmente del catálogo de servicios y agregar un icono personalizado que aparezca en el catálogo.

Acciones publicadas

Las acciones son cambios que pueden realizarse en los elementos del catálogo aprovisionados. Por ejemplo, el reinicio de una máquina virtual.

Las acciones pueden ser acciones integradas o acciones creadas mediante XaaS. Las acciones integradas se añaden cuando se añade una máquina u otro blueprint proporcionado. Las acciones de XaaS deben crearse y publicarse.

Las acciones no están asociadas con servicios. Debe incluir una acción en la autorización que contiene el elemento del catálogo sobre el que se ejecute la acción. Las acciones que se autorizan a los usuarios no aparecen en el catálogo de servicios. Las acciones disponibles para el elemento aprovisionado en la pestaña **Implementaciones** del usuario del catálogo de servicios dependen de si son aplicables al elemento y al estado actual del elemento.

Puede añadir un icono personalizado a la acción que se muestra en la pestaña **Implementaciones**.

Configurar un elemento del catálogo

Un elemento del catálogo es un blueprint publicado que puede autorizar a los usuarios. Las opciones de los elementos del catálogo se utilizan para cambiar el servicio asociado o el estado. También puede ver la autorizaciones que incluyen el elemento del catálogo seleccionado.

Solo aparecen en el catálogo de servicios los elementos del catálogo asociados a un servicio y autorizados a usuarios. Los elementos del catálogo pueden asociarse con solo un servicio.

Puede desactivar un elemento del catálogo si no desea que aparezca en el catálogo de servicios; no es necesario quitarlo de una autorización ni de la lista de elementos del catálogo publicada. El estado de un elemento del catálogo desactivado es "retirado" en la cuadrícula e "inactivo" en los detalles de configuración. Puede activarlo en otro momento.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador del catálogo**.
- Verificar que tiene al menos un blueprint publicado como elemento del catálogo. Consulte [Publicar un blueprint](#).

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Elementos del catálogo**.
- 2 Seleccionar el elemento del catálogo y hacer clic en **Configurar**.
- 3 Configurar la configuración del elemento del catálogo.

Opción	Descripción
Icono	Busque una imagen. Los tipos de archivo de imagen admitidos son GIF, JPG y PNG. La imagen mostrada es de 40 x 40 píxeles. Si no selecciona una imagen personalizada, aparece el icono del catálogo predeterminado en el catálogo de servicios.
Estado	<p>Entre los posibles valores se incluyen Activo, Inactivo, y Almacenamiento provisional.</p> <ul style="list-style-type: none"> ■ Activo. El elemento del catálogo aparece en el catálogo de servicios y los usuarios autorizados pueden utilizarlo para aprovisionar recursos. El elemento aparece en la lista de elementos del catálogo como publicado. ■ Inactivo. El elemento del catálogo no está disponible en el catálogo de servicios. El elemento aparece en la lista de elementos del catálogo como retirado. ■ Almacenamiento provisional. El elemento del catálogo no está disponible en el catálogo de servicios. Seleccione este elemento del menú si el elemento anteriormente estaba inactivo y está utilizando el almacenamiento provisional para indicar que se está planteando reactivarlo. Aparece en la lista de elementos del catálogo como en almacenamiento provisional.
Cuota	<p>Establezca el número de instancias de este elemento de catálogo que un usuario puede implementar.</p> <p>Si el usuario supera este número, aparece una notificación en la solicitud del catálogo y esta no se envía.</p>
Servicio	Seleccionar un servicio. Todos los elementos del catálogo deben asociarse con un servicio si desea que aparezca en el catálogo de servicios para usuarios autorizados. La lista incluye servicios activos e inactivos.

- 4 Para ver las autorizaciones en las que el elemento del catálogo queda disponible para los usuarios, haga clic en la pestaña **Autorizaciones**.
- 5 Haga clic en **Actualizar**.

Pasos siguientes

- Para que el elemento del catálogo esté disponible en el catálogo de servicios, debe autorizar a los usuarios al servicio asociado con el elemento o al elemento individual. Consulte [Crear autorizaciones](#).
- Para especificar el orden de procesamiento de autorizaciones para que las políticas de aprobación de usuarios individuales se apliquen correctamente, establezca el orden de prioridad de varias autorizaciones para el mismo grupo empresarial. Consulte [Priorizar autorizaciones](#).

Configurar una acción del catálogo de servicios

Una acción es un cambio o un flujo de trabajo que puede ejecutarse en elementos aprovisionados. Es posible agregar un icono o ver las autorizaciones que incluyen la acción seleccionada.

Una acción es una acción integrada de una máquina aprovisionada, una red u otros componentes de blueprint, o bien es una acción de XaaS publicada.

Los tipos de archivo de imagen admitidos en el icono son GIF, JPG y PNG. La imagen mostrada es de 40 x 40 píxeles. Si no selecciona una imagen personalizada, aparece el icono de la acción predeterminada en la pestaña **Elementos**.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador del catálogo**.
- Compruebe que tiene al menos una acción publicada. Consulte [Publicar un blueprint](#) y [Publicar una acción personalizada](#).

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Acciones**.
- 2 Seleccione la acción compartida y haga clic en **Ver detalles**.
- 3 Busque una imagen.
- 4 Para ver las autorizaciones en las que la acción está disponible para los usuarios, haga clic en el pestaña **Autorizaciones**.
- 5 Haga clic en **Actualizar**.

Pasos siguientes

[Autorizar usuarios a servicios, elementos de catálogo y acciones](#).

Crear autorizaciones

Las autorizaciones rigen los elementos y las acciones que los miembros del grupo empresarial seleccionados van a tener disponibles en el catálogo de servicios. Debe haber una autorización activa para que los elementos se muestren en el catálogo de servicios. Si tiene elementos que

precisan de gobierno, puede recurrir a las autorizaciones para aplicar políticas a distintos elementos.

Para configurar la autorización, los elementos de catálogo deben estar incluidos en un servicio. Las autorizaciones pueden incluir varios servicios, elementos de catálogo de los servicios incluidos en otras autorizaciones y las acciones que se pueden ejecutar en los elementos de catálogo implementados.

Descripción de las interacciones de las autorizaciones

La configuración de una autorización determina lo que aparece en el catálogo de servicios. La interacción de los servicios, elementos de catálogo y componentes, acciones y políticas de aprobación afecta a las solicitudes que puede realizar el usuario del catálogo de servicios y al modo en que se aplican las políticas de aprobación.

Al crear una autorización, hay que tener en cuenta las interacciones de los servicios, los elementos de catálogo, las acciones y las aprobaciones.

■ Servicios de las autorizaciones

Un servicio autorizado funciona como un grupo dinámico de elementos de catálogo. Si un elemento de catálogo se añade a un servicio después de que se haya autorizado, ese nuevo elemento de catálogo estará disponible para los usuarios especificados sin necesidad de configuración adicional.

■ Elementos de catálogo y componentes de las autorizaciones

Los elementos de catálogo autorizados son blueprints que puede solicitar en el catálogo de servicios. Los componentes autorizados forman parte de los blueprints, pero no se pueden solicitar específicamente en el catálogo de servicios.

■ Acciones de las autorizaciones

Las acciones se ejecutan en los elementos de catálogo implementados. En la pestaña Elementos, se muestran los elementos de catálogo aprovisionados y las acciones que está autorizado a ejecutar en ellos. Para ejecutar una acción en un elemento implementado, la acción debe estar incluida en la misma autorización que el elemento del catálogo que aprovisionó el elemento desde el catálogo de servicios.

■ Políticas de aprobación de las autorizaciones

Las políticas de aprobación se aplican en las autorizaciones para que pueda administrar los recursos de su entorno.

Servicios de las autorizaciones

Un servicio autorizado funciona como un grupo dinámico de elementos de catálogo. Si un elemento de catálogo se añade a un servicio después de que se haya autorizado, ese nuevo elemento de catálogo estará disponible para los usuarios especificados sin necesidad de configuración adicional.

Si aplica una política de aprobación a un servicio, todos los elementos se someterán a la misma política de aprobación cuando se soliciten.

Elementos de catálogo y componentes de las autorizaciones

Los elementos de catálogo autorizados son blueprints que puede solicitar en el catálogo de servicios. Los componentes autorizados forman parte de los blueprints, pero no se pueden solicitar específicamente en el catálogo de servicios.

Los elementos de catálogo y los componentes autorizados pueden ser cualquiera de los siguientes elementos:

Elementos del catálogo

- Elementos procedentes de un servicio que quiere aprovisionar a los usuarios autorizados, incluidos aquellos servicios que no están incluidos en la autorización actual.

Por ejemplo, como administrador del catálogo, ha asociado varias versiones distintas de Red Hat Enterprise Linux con un servicio de Red Hat y ha autorizado ese servicio a los ingenieros de calidad del producto A. Luego, recibe una solicitud para crear elementos del catálogo de servicios que incluye solo la versión más reciente de los sistemas operativos Linux para el equipo de formación. Así, crea una autorización para el equipo de formación que incluye las versiones más recientes de los otros sistemas operativos en un servicio. Como ya tiene la versión más reciente de RHEL asociada a otro servicio, añade RHEL como un elemento de catálogo en lugar de añadir el servicio de Red Hat entero.

- Elementos incluidos en un servicio que está incluido en la autorización actual, pero quiere aplicar a esos elementos de catálogo individual una política de aprobación distinta de la aplicada al servicio.

Por ejemplo, como administrador de grupo empresarial, autoriza a su equipo de desarrollo a usar un servicio que incluye tres elementos de catálogo de máquina virtual. Aplica una política de aprobación que requiere que las máquinas con más de cuatro CPU sean aprobadas por el administrador de la infraestructura virtual. Una de las máquinas virtuales se usa para las pruebas de rendimiento, de modo que la añade como un elemento de catálogo y le aplica una política de aprobación menos restrictiva para el mismo grupo de usuarios.

Componentes

- Los componentes no están disponibles por su nombre en el catálogo de servicios porque forman parte de un elemento del catálogo. Se autorizan de forma individual para poder aplicar una política de aprobación específica distinta del elemento de catálogo en el que se incluye.

Por ejemplo, un elemento incluye una máquina y software. La máquina está disponible como elemento aprovisionable y tiene una política de aprobación que requiere la aprobación por parte del administrador del sitio. El software no está disponible como elemento aprovisionable independiente, sino únicamente como parte de una solicitud de máquina, pero la política de aprobación de software requiere la aprobación por parte del administrador de licencias de software de la organización. Cuando la máquina se solicita en el catálogo de servicios, deberá contar con la aprobación del administrador del sitio y del administrador de licencias de software para que se pueda aprovisionar. Después de aprovisionarla, la máquina (con la entrada de software) aparecerá como parte de la máquina en la pestaña Elementos del solicitante.

Acciones de las autorizaciones

Las acciones se ejecutan en los elementos de catálogo implementados. En la pestaña Elementos, se muestran los elementos de catálogo aprovisionados y las acciones que está autorizado a ejecutar en ellos. Para ejecutar una acción en un elemento implementado, la acción debe estar incluida en la misma autorización que el elemento del catálogo que aprovisionó el elemento desde el catálogo de servicios.

Por ejemplo, la autorización 1 incluye una máquina virtual de vSphere y una acción para crear snapshots, mientras que la autorización 2 incluye únicamente una máquina virtual de vSphere. Cuando se implementa una máquina de vSphere desde la autorización 1, la acción para crear snapshots estará disponible; no obstante, si se implementa desde la autorización 2, no habrá ninguna acción disponible. Para poner la acción a disposición de los usuarios de la autorización 2, añada a ella la acción de creación de snapshots.

Si selecciona una acción que no procede para alguno de los elementos de catálogo en la autorización, no se mostrará en la pestaña Elementos. Por ejemplo, su autorización incluye una máquina de vSphere y autoriza una acción de destrucción de una máquina en la nube. Esta acción no se puede ejecutar en la máquina aprovisionada.

Puede aplicar una política de aprobación a una acción que sea distinta de la política aplicada al elemento de catálogo en la autorización.

Si el usuario del catálogo de servicios pertenece a varios grupos empresariales y un grupo sólo está autorizado a encender y apagar y el otro grupo sólo está autorizado a destruir, ese usuario tendrá las tres acciones disponibles para la máquina aprovisionada aplicable.

Procedimientos recomendados al autorizar usuarios a acciones

Los blueprints son complejos y la autorización de acciones para que se ejecuten en blueprints aprovisionados puede provocar un comportamiento inesperado. Utilice las siguientes recomendaciones cuando autorice a los usuarios del catálogo de servicios a ejecutar acciones en sus elementos aprovisionados.

- Cuando autorice a usuarios la acción de destruir una máquina, autorice también la acción de destruir la implementación. Un blueprint aprovisionado es una implementación.

Una implementación puede contener una máquina. Si el usuario del catálogo de servicios está autorizado a ejecutar la acción de destruir la máquina pero no la de destruir la implementación, cuando el usuario ejecute la acción de destruir la máquina en la última o única máquina de una implementación, aparecerá un mensaje que indica que no tiene permiso para ejecutar dicha acción. Al autorizar ambas acciones, se garantiza la eliminación de la implementación de su entorno. Para administrar el control de la acción de destruir la implementación, puede crear una política de aprobación previa y aplicarla a la acción. Esta política le permitirá al aprobador designado validar la solicitud para destruir la implementación antes de que se ejecute.

- Cuando autoriza a usuarios del catálogo de servicios las acciones Cambiar concesión, Cambiar propietario, Caducar, Reconfigurar u otras acciones que pueden aplicarse a máquinas y a implementaciones, autorícelas para realizar ambas acciones.

Políticas de aprobación de las autorizaciones

Las políticas de aprobación se aplican en las autorizaciones para que pueda administrar los recursos de su entorno.

Para poder aplicar una política de aprobación al crear la autorización, dicha política ya debe existir. Si no es así, puede seguir creando la autorización y dejarla en estado de borrador o inactivo hasta crear las políticas de aprobación necesarias para los elementos de catálogo y las acciones de esta autorización. Posteriormente, puede aplicar las políticas en cuestión.

No es necesario aplicar una política de aprobación a ningún elemento o acción. Si no se aplica una política de aprobación, los elementos y las acciones se implementan cuando se soliciten sin desencadenar una solicitud de aprobación.

Autorizar usuarios a servicios, elementos de catálogo y acciones

Cuando añade un servicio, un elemento del catálogo o una acción a una autorización, permite a los usuarios identificados en dicha autorización que soliciten los elementos que se pueden aprovisionar en el catálogo de servicios. Las acciones se asocian a elementos y aparecen en la pestaña **Elementos** del usuario solicitante.

Existen varias funciones de usuario con permiso para crear autorizaciones para grupos empresariales.

- Los administradores de tenants pueden crear autorizaciones para cualquier grupo empresarial en sus tenants.
- Los administradores de grupos empresariales pueden crear autorizaciones para los grupos que administran.
- Los administradores de catálogos pueden crear autorizaciones para cualquier grupo empresarial en sus tenants.

Cuando crea una autorización, debe seleccionar un grupo empresarial y especificar sus miembros para la autorización.

Para comprender cómo crear una autorización para usar las interacciones de servicios, elementos del catálogo y acciones sin aprobaciones, consulte [Crear autorizaciones](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador del catálogo**.
- Compruebe que los elementos de catálogo para los que autoriza a usuarios están asociados a un servicio. Consulte [Añadir elementos del catálogo a un servicio](#).
- Confirme que el grupo empresarial para el que está definiendo la autorización existe y que los usuarios miembro y los grupos de usuarios se han especificado. Consulte [Crear un grupo empresarial](#).

- Si tiene intención de añadir aprobaciones al crear esta autorización, compruebe que existen las políticas de aprobación correspondientes. Consulte [Crear una política de aprobación](#). Si desea autorizar usuarios a los elementos del catálogo de servicios sin aprobaciones, puede modificar la autorización más adelante para añadir aprobaciones.

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Autorizaciones**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Configure las opciones de **Detalles**.

Detalles determina el modo en que la autorización va a aparecer en la lista de autorizaciones, así como qué usuarios van a tener acceso a los elementos en el catálogo de servicios.

Opción	Descripción
Nombre y descripción	Información sobre la autorización que aparece recogida en la lista de autorizaciones.
Fecha de caducidad	Establezca una fecha y una hora si quiere que la autorización quede inactiva en una fecha concreta.
Estado	<p>Entre los posibles valores se incluyen Activo, Inactivo y Eliminado.</p> <ul style="list-style-type: none"> ■ Activo. Los elementos están disponibles en el catálogo de servicios. Esta opción está disponible cuando añade o edita autorizaciones. ■ Inactivo. Los elementos no están disponibles en el catálogo de servicios. El usuario ha desactivado la autorización o esta ha alcanzado la fecha de caducidad. ■ Eliminado. Elimina la autorización.
Grupo empresarial	<p>Seleccione un grupo empresarial. Se pueden crear autorizaciones para únicamente un grupo empresarial. Los usuarios autorizados deben pertenecer a ese grupo empresarial.</p> <p>Si desea que una autorización esté disponible para todos los usuarios, debe contar con un grupo empresarial Todos los usuarios, o bien debe crear autorizaciones para cada grupo empresarial.</p> <p>Si ha iniciado sesión como administrador de grupo empresarial, podrá crear autorizaciones solo para su grupo empresarial.</p>
Usuarios y grupos	<p>Seleccione Todos los usuarios y grupos para autorizar a todos los miembros del grupo empresarial para acceder a los elementos del catálogo y las acciones, o bien puede autorizar individuos o grupos individuales. Para activar una autorización, debe seleccionar al menos un grupo o un usuario de grupo empresarial.</p>

- 4 Haga clic en **Siguiente**.

- 5 Haga clic en el icono **Nuevo** (+) para permitir a los usuarios usar los servicios, elementos de catálogo o acciones con esta autorización.

Puede crear una autorización con diversas combinaciones de servicios, elementos y acciones.

Opción	Descripción
Servicios autorizados	<p>Añada un servicio cuando quiera conceder a los usuarios autorizados acceso a todos los elementos publicados del catálogo asociados al servicio.</p> <p>Un servicio autorizado es una autorización dinámica. Si un elemento se añade al servicio posteriormente, se añade al catálogo de servicios para los usuarios autorizados. Las autorizaciones pueden incluir tanto servicios como elementos del catálogo individuales.</p>
Elementos de catálogo y componentes autorizados	<p>Añada elementos individuales que estén disponibles para los usuarios autorizados.</p> <p>Las autorizaciones pueden incluir tanto servicios como elementos de catálogo individuales. Para aplicar una política de aprobación diferente a un elemento incluido en el servicio, añádala como un elemento del catálogo. La política de aprobación en un elemento prevalece sobre la política de aprobación en el servicio al que pertenece cuando ambos se encuentran en la misma autorización. Si están en distintas autorizaciones, el orden se rige según la prioridad establecida.</p> <p>Los elementos de catálogo deben estar asociados a un servicio para que puedan estar disponibles en el catálogo de servicios. Los elementos del catálogo pueden estar asociados a cualquier servicio, el cual no necesariamente tiene que ser un servicio en la autorización actual.</p> <p>Los componentes son una parte de un elemento de catálogo, pero no están disponibles por su nombre en el catálogo de servicios. Por ejemplo, el software MySQL es un componente del elemento de catálogo de máquina virtual CentOS. Los componentes se autorizan junto con el elemento de catálogo. Si desea aplicar una política de aprobación específica del software, debe autorizar el elemento de forma individual. De lo contrario, no es necesario autorizar un componente para que se implemente con el elemento principal.</p>

Opción	Descripción
Acciones autorizadas	<p>Añada acciones cuando quiera permitir que los usuarios realicen las acciones relativas a un elemento aprovisionado.</p> <p>Las acciones que quiera que se realicen en los elementos aprovisionados desde esta autorización deben estar incluidos en la misma autorización.</p> <p>Las acciones autorizadas no aparecen en el catálogo de servicios, sino en la pestaña Elementos de un elemento aprovisionado.</p>
Las acciones solo se aplican a los elementos definidos en esta autorización	<p>Determina si las acciones autorizadas tienen autorización para todos los elementos del catálogo de servicios aplicable o solo para los elementos de esta autorización.</p> <p>Si se selecciona, las acciones están autorizadas para los miembros del grupo empresarial en los elementos aplicables de esta autorización. Este método de autorización de acciones permite especificar acciones para elementos específicos.</p> <p>Si esta opción no está seleccionada, las acciones se autorizan a los usuarios especificados en la autorización para todos los elementos del catálogo aplicables, tanto si los elementos están incluidos en esta autorización como si no lo están. Cualquier política de aprobación aplicada sobre estas acciones también está activa.</p>

- 6 Use los menús desplegables de cada sección para filtrar los elementos disponibles.
- 7 Active las casillas de los elementos que quiera incluir en la autorización.
- 8 Para añadir una política de aprobación al servicio, elemento o acción seleccionados, seleccione una política de aprobación en el menú desplegable **Aplicar esta política a los elementos seleccionados**.

Si aplica una política de aprobación a un servicio, todos los elementos del servicio tendrán la misma política de aprobación. Para aplicar una política distinta a un elemento, añádala como un elemento del catálogo y aplíquela.

- 9 Haga clic en **Aceptar**.

El servicio, el elemento o la acción se añaden a la autorización.

- 10 Haga clic en **Finalizar** para guardar la autorización.

Resultados

Si el estado de la autorización es activo, el servicio y los elementos se añaden al catálogo de servicios.

Pasos siguientes

Compruebe que los elementos de catálogo y servicios autorizados figuren en el catálogo de servicios de los usuarios autorizados y que los elementos solicitados aprovisionen los objetos de destino según lo previsto. Puede solicitar el elemento en nombre de los usuarios seleccionados.

Priorizar autorizaciones

Si existen varias autorizaciones para el mismo grupo empresarial, puede dar prioridad a las autorizaciones de modo que, cuando un usuario de catálogo de servicios realice una solicitud, la autorización y la política de aprobación asociada se procesen en el orden especificado.

Si configura una política de aprobación para un grupo de usuarios y desea que un miembro del grupo tenga una política única para uno o más servicios, elementos de catálogo o acciones, dé más prioridad a la autorización del miembro que a la del grupo. Cuando el miembro solicite un elemento del catálogo de servicios, la política de aprobación que se aplicará dependerá del orden de prioridad de las autorizaciones del grupo empresarial. En cuanto se encuentra el nombre del miembro, como parte de un grupo de usuarios personalizado o como un usuario individual, se aplica la política de aprobación.

Por ejemplo, se crean dos autorizaciones para el mismo elemento de catálogo de modo que se pueda aplicar una política de aprobación al grupo de usuarios Contabilidad y otra política de aprobación a Chris, un miembro de dicho grupo.

Tabla 3-70. Autorizaciones de ejemplo

Autorización 1	Autorización 2
Grupo empresarial: Finanzas	Grupo empresarial: Finanzas
Usuarios y grupos: grupo Contabilidad	Usuarios y grupos: Chris
Elemento de catálogo 1: Política A	Elemento de catálogo 1: Política C

Chris solicita el elemento de catálogo 1 del catálogo de servicios. Según el orden de prioridad de las autorizaciones para el grupo empresarial Finanzas, se aplicará una política diferente a la solicitud de Chris.


Tabla 3-71. Resultados de ejemplo

Configuración y resultado	Orden de prioridad	Orden de prioridad
Orden de prioridad	1: Autorización 1 2: Autorización 2	1: Autorización 2 2: Autorización 1
Política aplicada	Se ha aplicado la Política A. Chris es miembro del grupo de usuarios Contabilidad. La búsqueda de Chris como usuario con autorización se detiene en la autorización 1 y se aplica la política de aprobación.	Se ha aplicado la Política C. La búsqueda de Chris como usuario con autorización se detiene en la autorización 2 y se aplica la política de aprobación.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador del catálogo**.

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Autorizaciones**.
- 2 Haga clic en el icono **Priorizar** ().
- 3 Seleccione un grupo empresarial en la lista desplegable **Grupo empresarial**.
- 4 Arrastre una autorización a otra ubicación de la lista para cambiar su prioridad.
- 5 Seleccione un método de actualización.

Opción	Descripción
Actualizar	Guarda los cambios.
Actualizar y cerrar	Guarda los cambios y cierra la venta Priorizar elementos .

Trabajar con políticas de aprobación

Las políticas de aprobación son mecanismos de gobierno que se añaden a las solicitudes del catálogo de servicios para poder administrar recursos en su entorno. Cada política es un conjunto definido de condiciones que se pueden aplicar a servicios, elementos de catálogo y acciones cuando se autoriza a los usuarios a usar esos elementos.

Proceso de políticas de aprobación

En primer lugar, un administrador de tenants o un administrador de aprobación crea las políticas de aprobación en las que se necesitan mecanismos de gobierno de aprovisionamiento.

Se crean políticas de aprobación para tipos de políticas de aprobación o elementos específicos. Si la política se basa en un tipo de política, puede aplicarla a tipos de elementos de catálogo coincidentes. Por ejemplo, si una política se basa en un tipo de política de software, puede definirla para aplicarla a cualquier elemento de software de las autorizaciones. Si la política es para un elemento específico, debe aplicarla solo a ese elemento. Por ejemplo, si el elemento es un elemento de software específico, debe aplicarla solo a ese elemento de software de base de datos específico de la autorización.

Las políticas pueden incluir requisitos previos y posteriores a la aprobación. Para la aprobación previa, la solicitud se debe aprobar antes de que se aprovisione el elemento solicitado. Las políticas posteriores a la aprobación requieren que el aprobador pueda aceptar la solicitud antes de que el elemento aprovisionado esté disponible para el usuario solicitante.

Las configuraciones previas y posteriores a la aprobación están compuestas por uno o más niveles que determinan cuándo se activa la política de aprobación o cómo se aprueba la solicitud. Puede incluir varios niveles. Por ejemplo, una política de aprobación puede tener un nivel para la aprobación del administrador, seguido de un nivel para la aprobación financiera.

A continuación, un administrador de tenants o un administrador de grupos empresariales aplica las políticas de aprobación a los servicios, a los elementos de catálogo y a las acciones según proceda.

Por último, cuando un usuario del catálogo de servicios solicita un elemento al que se le aplica una política de aprobación, los aprobadores aprueban o rechazan la solicitud en su ficha **Bandeja de entrada**, en la página **Aprobaciones**. El usuario que realiza la solicitud puede realizar un seguimiento del estado de la aprobación para una solicitud específica en su ficha **Solicitudes**.

Ejemplos de políticas de aprobación basadas en el tipo de política de máquina virtual

Puede crear una política de aprobación que se pueda aplicar al mismo tipo de elemento del catálogo, pero que produzca resultados distintos cuando se solicite un elemento en el catálogo de servicios. El efecto en el usuario del catálogo de servicios y el aprobador será distinto en función de cómo esté definida y aplicada la política de aprobación.

En la siguiente tabla se incluyen ejemplos de distintas políticas de aprobación, todas basadas en el mismo tipo de política de aprobación. En estos ejemplos se muestran algunas formas de configurar políticas de aprobación para conseguir distintos tipos de control.

Tabla 3-72. Ejemplos de políticas de aprobación y resultados

Objetivos de control	Tipo de política seleccionada	Aprobación previa o posterior	Cuándo se requiere aprobación	Quiénes son los aprobadores	Cómo se aplica la política en la autorización	Resultados cuando se solicita el elemento en el catálogo de servicios
El administrador de grupo empresarial debe aprobar cualquier solicitud de máquina virtual. La política de aprobación debe poder aplicarse a varios grupos empresariales en varias autorizaciones.	Catálogo de servicios - Solicitud de elemento del catálogo - Máquina virtual	Añadir a pestaña Aprobación previa	Seleccione Se requiere siempre.	Seleccione Determinar aprobadores a partir de la solicitud. Seleccione la condición Grupo empresarial > Administradores > Usuarios > administrador. Seleccione Cualquiera puede aprobar.	Las autorizaciones están basadas en los grupos empresariales. Esta aprobación se puede usar en cualquier autorización en la que se requiera la aprobación del administrador para la máquina virtual.	Cuando el usuario del catálogo de servicios solicita una máquina virtual a la que se aplicó esta aprobación, el administrador del grupo empresarial puede aprobar la solicitud antes de que se aprovisione la máquina.
El administrador de la infraestructura virtual debe comprobar el aprovisionamiento correcto de la máquina virtual y aprobar la solicitud antes de que la máquina virtual se libere para el usuario que la solicita.	Catálogo de servicios - Solicitud de elemento del catálogo - Máquina virtual	Añadir a pestaña Aprobación posterior	Seleccione Se requiere siempre.	Seleccione Usuarios y grupos específicos. Seleccione el grupo de usuarios personalizado de administradores de la infraestructura virtual. Seleccione Cualquiera puede aprobar.	Esta aprobación se puede usar en cualquier autorización en la que desee que el administrador de la infraestructura virtual compruebe la máquina virtual en vCenter Server después de que se haya aprovisionado.	Cuando el usuario del catálogo de servicios solicita una máquina virtual para la que se aplicó esta aprobación, entonces se aprovisiona la máquina virtual. Si cada miembro del grupo de administradores de la infraestructura virtual aprueba la solicitud, la máquina se libera para el usuario.

Tabla 3-72. Ejemplos de políticas de aprobación y resultados (continuación)

Objetivos de control	Tipo de política seleccionada	Aprobación previa o posterior	Cuándo se requiere aprobación	Quiénes son los aprobadores	Cómo se aplica la política en la autorización	Resultados cuando se solicita el elemento en el catálogo de servicios
Para administrar los recursos de la infraestructura virtual y controlar los precios, puede añadir dos tipos de niveles de aprobación previa: una aprobación es para los recursos de máquina y la otra, para el precio de la máquina por día.	Catálogo de servicios - Solicitud de elemento del catálogo - Máquina virtual	Añadir a pestaña Aprobación previa	Nivel 1 Seleccione Se requiere según condiciones . Configure las condiciones, donde CPU > 6 o memoria > 8 o almacenamiento > 100 GB.	Seleccione Determinar aprobadores a partir de la solicitud . Seleccione la condición Solicitado por > administrador. Seleccione . Haga clic en Propiedades del sistema y seleccione CPUs, Memoria y Almacenamiento para que el aprobador pueda cambiar el valor a un nivel aceptable.	Esta política de aprobación se puede usar en una autorización donde desee que el administrador del usuario que la solicita y un miembro del departamento o financiero aprueben la solicitud.	Cuando el usuario del catálogo de servicios solicita una máquina virtual, se evalúa la solicitud para determinar si los volúmenes de CPU, memoria o almacenamiento o solicitados superan los volúmenes especificados en el nivel 1. Si no los superan, entonces se evalúa la condición de nivel 2. Si las solicitudes superan al menos una de las condiciones del nivel 1, el administrador debe aprobar la solicitud. El administrador tiene la opción de reducir los volúmenes de configuración solicitados y aprobarlos, o puede rechazar la solicitud.

Tabla 3-72. Ejemplos de políticas de aprobación y resultados (continuación)

Objetivos de control	Tipo de política seleccionada	Aprobación previa o posterior	Cuándo se requiere aprobación	Quiénes son los aprobadores	Cómo se aplica la política en la autorización	Resultados cuando se solicita el elemento en el catálogo de servicios
			Nivel 2 Selecione Se requiere según condiciones. Configure la condición Precio > 15,00 al día.	Selecione Usuarios y grupos específicos. Selecione el grupo de usuarios personalizados del departamento financiero. Selecione Cualquiera puede aprobar.		
En el caso de los elementos del catálogo de blueprint con parámetros, un administrador de nube debe aprobar las solicitudes de implementación en las que el perfil de componente de una máquina de vSphere de tipo size esté establecido en large.	Catálogo de servicios - Solicitud de elemento del catálogo - Máquina virtual	Añadir a pestaña Aprobación previa	Nivel 1 Selecione Se requiere según condiciones. Nivel 2 Selecione Condición única. Selecione Perfil de componente > Tamaño de máquina de vSphere. Configure la condición size = large.	Selecione Usuarios y grupos específicos. Selecione los usuarios y grupos que van a tener capacidad para aprobar la solicitud. Selecione Cualquiera puede aprobar.	Esta política de aprobación se puede usar en una autorización donde se desee que un administrador de nube apruebe la solicitud de aprovisionamiento.	Cuando el usuario del catálogo de servicios solicite una máquina virtual que se ha sometido a esta aprobación, el administrador de la nube debe aprobar dicha solicitud para que la máquina pueda aprovisionarse.

Ejemplo de acciones con políticas de aprobación aplicadas en una implementación compuesta

Cuando se aplican políticas de aprobación a acciones que se pueden ejecutar en varios componentes en un blueprint compuesto, el proceso de aprobación varía según el modo en que esté configurada la autorización y el modo en que se apliquen las políticas.

En este ejemplo se usan detalles específicos para crear el blueprint y, después, aplicar políticas de aprobación a acciones que se pueden ejecutar desde el catálogo de servicios en el blueprint aprovisionado en distintas autorizaciones. El blueprint es un blueprint compuesto que incluye otro blueprint. Las acciones usadas son: destruir los elementos aprovisionados, destruir una implementación para los blueprints y destruir una máquina virtual para la máquina. El comportamiento resultante incluye lo que se ha destruido y cuándo inician solicitudes de aprobación las políticas de aprobación aplicadas.

Blueprint de ejemplo

En este ejemplo, se configura un blueprint que incluye un blueprint anidado con una máquina virtual.

- Blueprint 1 - Blueprint de integración continua
 - Blueprint 2 - Blueprint de preproducción
 - Máquina virtual 1 - TestAsAService vSphere VM

Políticas de aprobación para acciones de destrucción

Se configuran las dos políticas de aprobación para destruir los elementos aprovisionados. En este ejemplo, se puede ejecutar una acción de destrucción-implementación en el blueprint 1 o en el blueprint 2. Se puede ejecutar una acción de destrucción-máquina virtual en la máquina virtual 1. Se crean las políticas de aprobación para poder aplicarlas a las acciones en la autorización.

Nombre de política de aprobación	Tipo de política de aprobación
Política de aprobación A	Catálogo de servicios - Solicitud de acción personalizada - Destrucción - Implementación
Política de aprobación B	Catálogo de servicios - Solicitud de acción personalizada - Destrucción - Máquina virtual

Autorizaciones y políticas de aprobación aplicadas a acciones

Se configuran tres autorizaciones. Cada autorización incluye el blueprint compuesto. En cada autorización, se agregan las acciones de destrucción y se aplican las políticas de aprobación.

Nombre de autorización	Acción autorizada en máquina aprovisionada	Política de aprobación aplicada
Autorización 1	Destruir - Implementación	Política de aprobación A
Autorización 2	Destruir - máquina virtual	Política de aprobación B
Autorización 3	Destruir - Implementación	Política de aprobación A
	Destruir - máquina virtual	Política de aprobación B

Acciones del usuario en el catálogo de servicios

Cuando el usuario del catálogo de servicios ejecuta la acción, los blueprints o las máquinas se destruyen en función del elemento sobre el que el usuario ejecutó la acción.

Acción del usuario en el catálogo de servicios	Acción seleccionada	Máquinas o blueprints destruidos
Acción 1	La acción de destrucción-implementación se ejecuta en el blueprint 1 - blueprint de integración continua	Blueprint 1, blueprint 2 y máquina virtual 1
Acción 2	La acción de destrucción-implementación se ejecuta en el blueprint 2 anidado - blueprint de preproducción	Blueprint 2 y máquina virtual 1
Acción 3	La acción de destrucción-máquina virtual se ejecuta en la máquina situada dentro de una implementación, máquina virtual 1 - TestAsAService vSphere VM	Máquina virtual 1

Políticas de aprobación aplicadas a acciones en las autorizaciones

Una vez que aprueba las políticas de aprobación, los aprobadores reciben una solicitud de aprobación en función del blueprint o la máquina en la que el usuario del catálogo de servicios ejecutó la acción.

Nombre de autorización	Política de aprobación en acciones	Acción de usuario	Solicitud de aprobación iniciada	Si se aprueba, máquinas o blueprints destruidos
Autorización 1 - Política de aprobación de destrucción-implementación	Política A (Política de aprobación de destrucción-implementación) solo en acción de destrucción - implementación	Acción 1 (ejecutar acción de destrucción-implementación en blueprint 1)	Las solicitudes de aprobación se inician solo para blueprint 1	Blueprint 1, blueprint 2 y máquina virtual 1
		Acción 2 (ejecutar acción de destrucción-implementación en blueprint 2)	Las solicitudes de aprobación se inician solo para blueprint 2	Blueprint 2 y máquina virtual 1
		Acción 3 (la acción de destrucción-máquina virtual se ejecuta en la máquina virtual 1)	No se inicia ninguna solicitud de aprobación	Máquina virtual 1
Autorización 2	Política B (política de destrucción-máquina virtual) solo en acción de destrucción-máquina virtual	Acción 1 (ejecutar acción de destrucción-implementación en blueprint 1)	No se inicia ninguna solicitud de aprobación	Blueprint 1, blueprint 2 y máquina virtual 1
		Acción 2 (ejecutar acción de destrucción-implementación en blueprint 2)	No se inicia ninguna solicitud de aprobación	Blueprint 2 y máquina virtual 1
		Acción 3 (la acción de destrucción-máquina virtual se ejecuta en la máquina virtual 1)	Las solicitudes de aprobación se inician solo para máquina virtual 1	Máquina virtual 1

Nombre de autorización	Política de aprobación en acciones	Acción de usuario	Solicitud de aprobación iniciada	Si se aprueba, máquinas o blueprints destruidos
Autorización 3	Política A (política de aprobación de destrucción-implementación) en acción de destrucción-implementación y política B (política de destrucción-máquina virtual) en acción de destrucción-máquina virtual	Acción 1 (ejecutar acción de destrucción-implementación en blueprint 1)	Las solicitudes de aprobación se inician solo para blueprint 1	Blueprint 1, blueprint 2 y máquina virtual 1
		Acción 2 (ejecutar acción de destrucción-implementación en blueprint 2)	Las solicitudes de aprobación se inician solo para blueprint 2	Blueprint 2 y máquina virtual 1
		Acción 3 (la acción de destrucción-máquina virtual se ejecuta en la máquina virtual 1)	Las solicitudes de aprobación se inician solo para máquina virtual 1	Máquina virtual 1

Ejemplo de política de aprobación en varias autorizaciones

Si aplica una política de aprobación en un elemento que se usa en varias autorizaciones que se otorgan a los mismos usuarios en un grupo empresarial, la política de aprobación se inicia en el elemento, incluso en el servicio donde la política de aprobación no esté aplicada expresamente en la autorización.

Por ejemplo, se crean los siguientes blueprints, servicios, políticas de aprobación y autorizaciones.

Blueprints

- Máquina virtual de RHEL vSphere
- Las pruebas de calidad incluyen la máquina virtual RHEL vSphere
- La formación de calidad incluye la máquina virtual RHEL vSphere

Servicios

- El blueprint de pruebas de calidad está asociado al servicio de pruebas
- El blueprint de formación de calidad está asociado al servicio de formación

Autorizaciones

- Autorización 1
- Autorización 2

Tabla 3-73. Configuraciones de autorizaciones

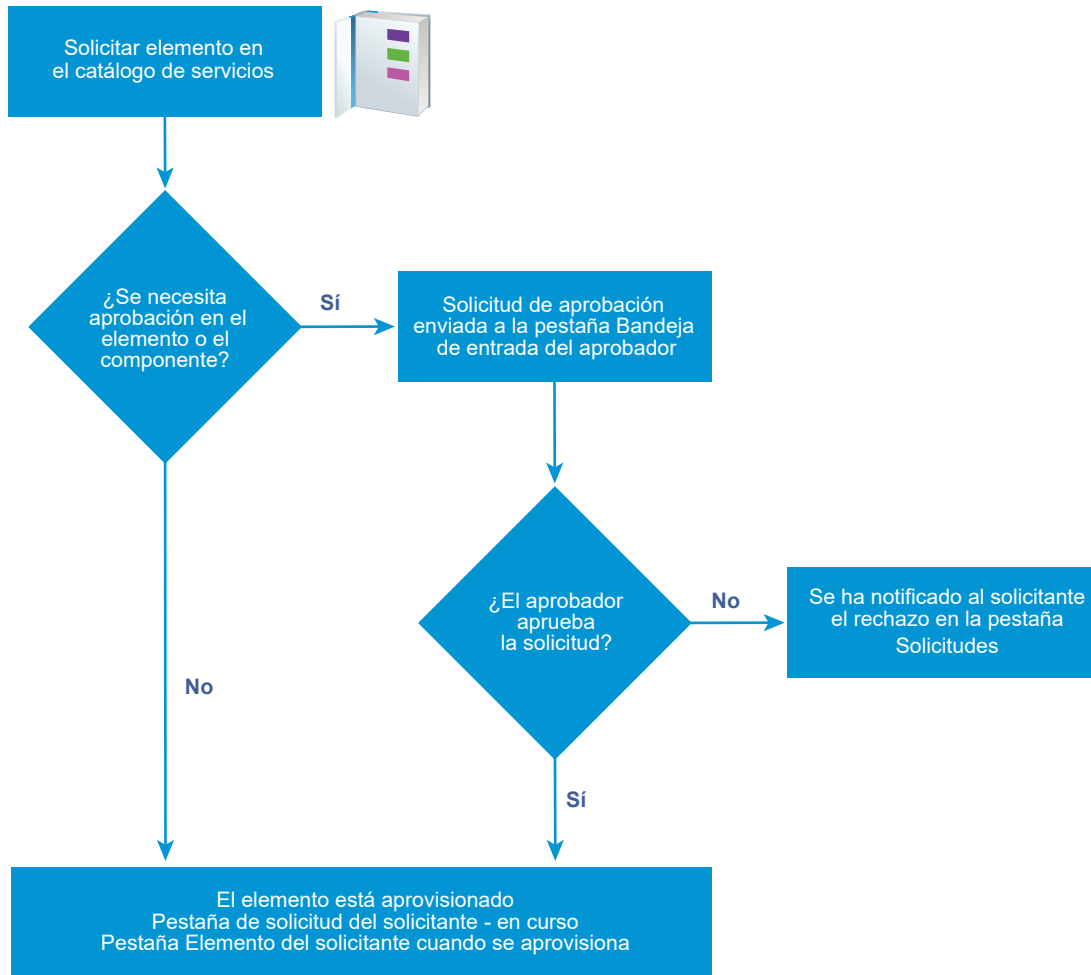
Nombre de autorización	Grupo empresarial	Servicio autorizado	Elemento autorizado
Autorización 1	Calidad	Pruebas	Solicitud de elemento del catálogo - Máquina virtual aplicada a componente de máquina virtual
Autorización 2	Calidad	Formación	

Resultados

Cuando el usuario selecciona la formación de calidad en el catálogo de servicios, se inicia la política de aprobación para la máquina virtual de RHEL vSphere porque es un blueprint basado en el componente de máquina virtual que se usa en el blueprint de formación de calidad.

Procesar políticas de aprobación en el catálogo de servicios

Cuando un usuario solicita un elemento del catálogo de servicios que tiene aplicada una política de aprobación, el aprobador y el usuario solicitante procesan la solicitud siguiendo un flujo de trabajo similar al siguiente:



Crear una política de aprobación

Los administradores de tenants y los administradores de aprobaciones pueden definir políticas de aprobación y usarlas en las autorizaciones. Se pueden configurar políticas de aprobación con varios niveles para eventos de aprobación previa y de aprobación posterior.

Si modifica una opción en un blueprint del componente de software y una política de aprobación usa esa opción para iniciar una solicitud de aprobación, es posible que la política de aprobación no funcione de la manera esperada. Si debe modificar una opción en un componente, compruebe que los cambios no afecten a una o a varias políticas de aprobación.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador de aprobaciones**.

Procedimiento

1 Especificar información sobre políticas de aprobación

Cuando cree una política de aprobación, defina el tipo de política de aprobación, el nombre, la descripción y el estado.

2 Crear un nivel de aprobación

Cuando crea una política de aprobación, puede añadir niveles de aprobación previa y de aprobación posterior.

3 Configurar el formulario de aprobación para incluir propiedades personalizadas y del sistema

Puede añadir propiedades personalizadas y del sistema para que se muestren en un formulario de aprobación. Estas propiedades se añaden para que los aprobadores puedan cambiar los valores de las propiedades personalizadas y las propiedades del sistema relacionadas con la configuración de recursos de la máquina, como la CPU o la memoria, antes de completar una solicitud de aprobación.

4 Configuración de políticas de aprobación

Cuando se crea una política de aprobación, se configuran varias opciones que determinan cuándo debe aprobarse un elemento solicitado por parte de un usuario del catálogo de servicios. La aprobación puede solicitarse antes de que la solicitud inicie el aprovisionamiento o después de aprovisionar el elemento, pero antes de que se entregue al usuario solicitante.

Especificar información sobre políticas de aprobación

Cuando cree una política de aprobación, defina el tipo de política de aprobación, el nombre, la descripción y el estado.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador de aprobaciones**.

Procedimiento

- 1 Seleccione **Administración > Políticas de aprobación**.
- 2 Haga clic en el icono **Nuevo** (+).

3 Seleccione un tipo de política o un componente de software.

Opción	Descripción
Seleccionar un tipo de política de aprobación	<p>Cree una política de aprobación en función del tipo de solicitud de aprobación.</p> <p>Seleccione esta opción para definir una política de aprobación aplicable a todos los elementos de catálogo de ese tipo. El tipo de solicitud puede ser genérica, de elemento del catálogo o de acción personalizada.</p> <p>Las opciones de configuración de condición disponibles varían según el tipo. Cuanto más específico es el tipo, más lo son los campos de configuración. Por ejemplo, Catálogo de servicios - Solicitud de elemento del catálogo solo proporciona los campos que son comunes a todas las solicitudes de elementos del catálogo, pero Catálogo de servicios - Solicitud de elemento del catálogo - Máquina virtual también incluye las opciones comunes y las específicas de las máquinas virtuales.</p> <p>El tipo de solicitud limita los elementos del catálogo o las acciones a los que puede aplicar la política de aprobación.</p>
Seleccionar un elemento	<p>Cree una política de aprobación en función de un elemento específico.</p> <p>Seleccione esta opción para definir una política de aprobación que sea aplicable a elementos específicos que no estén disponibles individualmente en el catálogo de servicios, sino solo como parte de una máquina u otra implementación: por ejemplo, los componentes de software.</p> <p>Los campos de configuración de condición disponibles son específicos del elemento y pueden ser más detallados que los criterios ofrecidos para un elemento de tipo de política.</p>
Lista	<p>Ofrece el tipo de política o los elementos del catálogo disponibles.</p> <p>Busque un tipo o elemento específicos o bien ordene las columnas para encontrarlos.</p>

4 Haga clic en **Aceptar**.

5 Especifique un nombre y, opcionalmente, una descripción.

6 Seleccione el estado de la política en el menú desplegable **Estado**.

Opción	Descripción
Borrador	Guarda la política de aprobación en un estado que se puede editar.
Activo	Guarda la política de aprobación en un estado de solo lectura que se puede usar en una autorización.
Inactivo	Guarda la política de aprobación en un estado de solo lectura que no se puede usar en una autorización hasta que se active la política.

Pasos siguientes

Cree los niveles de aprobación previa y posterior.

Crear un nivel de aprobación

Cuando crea una política de aprobación, puede añadir niveles de aprobación previa y de aprobación posterior.

Puede crear varios niveles de aprobación para una política de aprobación. Cuando un usuario del catálogo de servicios solicita un elemento al que se le aplica una política de aprobación con varios niveles, debe aceptarse cada nivel previo para poder enviar la solicitud de aprobación al siguiente aprobador. Consulte [Trabajar con políticas de aprobación](#).

Si configura una directiva de aprobación que se activa por una solicitud de duración de concesión, debe seleccionar **Se requiere siempre** como el requisito de aprobación.

Requisitos previos

[Especificar información sobre políticas de aprobación](#).

Procedimiento

- 1 En la pestaña **Aprobación previa** o **Aprobación posterior**, haga clic en el icono **Nuevo** (+).
- 2 Especifique un nombre y, opcionalmente, una descripción.
- 3 Seleccione un requisito de aprobación.

Opción	Descripción
Se requiere siempre	Se desencadena la política de aprobación para todas las solicitudes.
Se requiere según condiciones	<p>La política de aprobación se basa en una o varias cláusulas de condición. Si selecciona esta opción, debe crear las condiciones. Cuando se aplica esta política de aprobación a los servicios, los elementos del catálogo o las acciones apropiados en una autorización, se evalúan las condiciones. Si las condiciones son verdaderas, la solicitud se debe aprobar con el método de aprobador especificado antes de aprovisionarla. Si son falsas, la solicitud se aprovisiona sin requerir una aprobación. Por ejemplo, todas las solicitudes de una máquina virtual con 4 o más CPU deben ser aprobadas por el administrador de la infraestructura virtual.</p> <p>La disponibilidad de los campos en los que basar las condiciones depende del tipo de política de aprobación o del elemento del catálogo que se haya seleccionado.</p> <p>Cuando se especifica un valor para una condición, se distingue entre mayúsculas y minúsculas.</p> <p>Para configurar más de una cláusula de condición, seleccione la operación booleana para las cláusulas.</p>

- 4 Seleccione los aprobadores.

Opción	Acción
Usuarios y grupos específicos	Envía la solicitud de aprobación a los usuarios seleccionados.
Determinar aprobadores a partir de la solicitud	Envía la solicitud de aprobación a los usuarios en función de la condición definida.
Usar suscripción a un evento	<p>Procesa la solicitud de aprobación en función de suscripciones a eventos definidas.</p> <p>La suscripción de flujo de trabajo se debe definir en Administración > Eventos > Suscripciones. Las suscripciones de flujo de trabajo correspondientes son de aprobación previa y posterior.</p>

5 Indique quién debe aprobar la solicitud o la acción.

Opción	Descripción
Cualquiera puede aprobar	<p>Solo hace falta que uno de los aprobadores apruebe la solicitud para que se procese.</p> <p>Cuando se solicita el elemento en el catálogo de servicios, las solicitudes de aprobación se envían a todos los aprobadores. Si un aprobador aprueba la solicitud, la solicitud se aprueba y se elimina de la bandeja de entrada de los demás aprobadores.</p>
Todos deben aprobar	Todos los aprobadores deben aprobar la solicitud para que se procese.

6 Añada propiedades a un formulario de aprobación o guarde el nivel.

- Para añadir propiedades al formulario de aprobación, haga clic en **Propiedades del sistema** o en **Propiedades personalizadas**.
- Para guardar el nivel, haga clic en **Aceptar**.

Pasos siguientes

Para añadir propiedades al formulario de aprobación, consulte [Configurar el formulario de aprobación para incluir propiedades personalizadas y del sistema](#).

Configurar el formulario de aprobación para incluir propiedades personalizadas y del sistema

Puede añadir propiedades personalizadas y del sistema para que se muestren en un formulario de aprobación. Estas propiedades se añaden para que los aprobadores puedan cambiar los valores de las propiedades personalizadas y las propiedades del sistema relacionadas con la configuración de recursos de la máquina, como la CPU o la memoria, antes de completar una solicitud de aprobación.

Las propiedades del sistema que hay disponibles dependen del tipo de política de aprobación y de cómo esté configurado el blueprint. En el caso de algunas propiedades, el campo configurado en el blueprint debe incluir un valor mínimo y uno máximo para que la propiedad figure en la lista de propiedades del sistema.

Las propiedades personalizadas se pueden añadir cuando se añade el nivel de aprobación. Si se configura una propiedad personalizada y se incluye en un blueprint, las propiedades personalizadas que añada al formulario de aprobación sobrescribirán cualquier otra instancia de esta propiedad personalizada, como, por ejemplo, en blueprints, grupos de propiedades o endpoints.

El aprobador puede modificar las propiedades seleccionadas o configuradas en el formulario de aprobación.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador de aprobaciones**.
- [Crear un nivel de aprobación](#).

Procedimiento

- 1 En la pestaña **Aprobación previa** o **Aprobación posterior**, haga clic en el icono **Nuevo** (+).
- 2 Haga clic en la pestaña **Propiedades del sistema**.
- 3 Seleccione la casilla de verificación de cada propiedad del sistema que desee que el aprobador configure durante el proceso de aprobación.
- 4 Configure las propiedades personalizadas.

Añada una o varias propiedades personalizadas que desee que el aprobador configure durante el proceso de aprobación.

- a Haga clic en la pestaña **Propiedades personalizadas**.
- b Haga clic en el icono **Nuevo** (+).
- c Escriba los valores de las propiedades personalizadas.

Opción	Descripción
Nombre	Escriba el nombre de la propiedad.
Etiqueta	Escriba la etiqueta que se presenta al aprobador en el formulario de aprobación.
Descripción	Escriba la información ampliada para el aprobador. Esta información aparece como la información sobre herramientas del campo en el formulario.

- d Haga clic en **Guardar**.
 - e Para eliminar varias propiedades personalizadas, seleccione las filas y haga clic en **Eliminar**.
- 5 Haga clic en **Aceptar**.

Pasos siguientes

- Añada más niveles de aprobación previa o aprobación posterior.
- Guarde la política de aprobación. La política debe estar activa para aplicar los servicios, los elementos o las acciones en las **Autorizaciones**.

Configuración de políticas de aprobación

Cuando se crea una política de aprobación, se configuran varias opciones que determinan cuándo debe aprobarse un elemento solicitado por parte de un usuario del catálogo de servicios. La aprobación puede solicitarse antes de que la solicitud inicie el aprovisionamiento o después de aprovisionar el elemento, pero antes de que se entregue al usuario solicitante.

Seleccione **Administración > Políticas de aprobación**. Haga clic en **Nuevo**.

- **Configuración de tipos de políticas de aprobación**

El tipo de política de aprobación determina el modo en que se configura la política de aprobación y a qué elementos o acciones puede aplicarlo en la autorización. Cuando añade niveles de aprobación, el elemento o tipo de política afecta a los campos que están disponibles para crear las condiciones para los niveles de aprobación.

- **Añadir configuración de políticas de aprobación**

Configure la información básica acerca de la política de aprobación, incluido el estado de la política, para poder administrarla.

- **Añadir información de nivel a la configuración de políticas de aprobación**

Un nivel de aprobación incluye las condiciones que desencadenan un proceso de aprobación cuando el usuario del catálogo de servicios solicita el elemento, así como las propiedades del sistema y del cliente que desee incluir. Cuando se desencadenan, las solicitudes de aprobación se envían a los aprobadores designados.

- **Añadir propiedades del sistema a la configuración de políticas de aprobación**

Ha seleccionado propiedades del sistema que desea añadir al formulario de aprobación y que permiten al aprobador modificar el valor.

- **Añadir propiedades personalizadas a la configuración de políticas de aprobación**

Configure las propiedades personalizadas que desee añadir al formulario de aprobación para permitir al aprobador modificar el valor.

Configuración de tipos de políticas de aprobación

El tipo de política de aprobación determina el modo en que se configura la política de aprobación y a qué elementos o acciones puede aplicarlo en la autorización. Cuando añade niveles de aprobación, el elemento o tipo de política afecta a los campos que están disponibles para crear las condiciones para los niveles de aprobación.

Seleccione **Administración > Políticas de aprobación**. Haga clic en **Nuevo**.

Tabla 3-74. Opciones de tipo de política de aprobación

Opción	Descripción
Seleccionar un tipo de política de aprobación	<p>Cree una política de aprobación en función del tipo de solicitud de aprobación.</p> <p>Seleccione esta opción para definir una política de aprobación aplicable a todos los elementos de catálogo de ese tipo. El tipo de solicitud puede ser genérica, de elemento del catálogo o de acción personalizada.</p> <p>Las opciones de configuración de condición disponibles varían según el tipo. Cuanto más específico es el tipo, más lo son los campos de configuración. Por ejemplo, Catálogo de servicios - Solicitud de elemento del catálogo solo proporciona los campos que son comunes a todas las solicitudes de elementos del catálogo, pero Catálogo de servicios - Solicitud de elemento del catálogo - Máquina virtual también incluye las opciones comunes y las específicas de las máquinas virtuales.</p> <p>El tipo de solicitud limita los elementos del catálogo o las acciones a los que puede aplicar la política de aprobación.</p>
Seleccionar un elemento	<p>Cree una política de aprobación en función de un elemento específico.</p> <p>Seleccione esta opción para definir una política de aprobación que sea aplicable a elementos específicos que no estén disponibles individualmente en el catálogo de servicios, sino solo como parte de una máquina u otra implementación: por ejemplo, los componentes de software.</p> <p>Los campos de configuración de condición disponibles son específicos del elemento y pueden ser más detallados que los criterios ofrecidos para un elemento de tipo de política.</p>
Lista	<p>Ofrece el tipo de política o los elementos del catálogo disponibles.</p> <p>Busque un tipo o elemento específicos o bien ordene las columnas para encontrarlos.</p>

Añadir configuración de políticas de aprobación

Configure la información básica acerca de la política de aprobación, incluido el estado de la política, para poder administrarla.

Para definir la información básica sobre la política de aprobación, seleccione **Administración > Políticas de aprobación**. Haga clic en **Nuevo**. Seleccione el tipo de política y haga clic en **Aceptar**.

Tabla 3-75. Opciones de política de aprobación

Opción	Descripción
Nombre	Nombre que aparece cuando se aplica la política de aprobación en una autorización.
Descripción	Proporcione una descripción detallada de cómo está construida la política de aprobación. Esta información le ayudará a administrar las políticas de aprobación.

Tabla 3-75. Opciones de política de aprobación (continuación)

Opción	Descripción
Estado	<p>Entre los posibles valores, se encuentran:</p> <ul style="list-style-type: none"> ■ Borrador. La política de aprobación no está disponible para aplicarse en autorizaciones. Una vez que active la política, ya no puede volver a ser borrador. ■ Activo. La política de aprobación está disponible para aplicarse en autorizaciones. ■ Inactivo. La política de aprobación no está disponible para aplicarse en autorizaciones. Si la política no se ha aplicado a autorizaciones y la inactiva, podrá eliminarla pero no reactivarla. Si la política se ha aplicado y la inactiva, los elementos a los que se aplique deberán vincularse a otra política o se quedarán desvinculados. Las acciones y los elementos desvinculados siguen autorizados para los usuarios, pero no tienen ninguna política de aprobación aplicada.
Tipo de política	<p>Muestra el tipo de solicitud de política de aprobación.</p> <p>Si seleccionó un elemento del catálogo en el cual basar la política de aprobación, se muestra el tipo de solicitud asociado.</p>
Elemento	<p>Muestra el elemento del catálogo seleccionado.</p> <p>Si seleccionó un tipo de solicitud en la cual basar la política de aprobación, este campo está vacío.</p>
Última actualización por	Nombre del usuario que realizó cambios en la política de aprobación.
Última actualización el	Fecha de la última modificación llevada a cabo en la política de aprobación.
Nivel de aprobación previa	<p>Para requerir la aprobación antes de que se aprovisionen los elementos solicitados o se ejecuten las acciones, configure una o varias condiciones que desencadenen el proceso de aprobación cuando el usuario del catálogo de servicios solicite el elemento.</p>
Nivel de aprobación posterior	<p>Para requerir la aprobación después de que se aprovisiona el elemento pero antes de que el elemento modificado o aprovisionado se libere al usuario del catálogo de servicios que lo solicitó, configure una o varias condiciones que desencadenen un proceso de aprobación.</p> <p>Por ejemplo, el administrador de infraestructura virtual comprueba que la máquina virtual se encuentra en un estado funcional antes de liberarla al usuario del catálogo de servicios.</p>
Ver autorizaciones vinculadas	<p>Muestra todas las autorizaciones en las que la política de aprobación se haya aplicado a servicios, elementos del catálogo o acciones. Puede vincular los elementos de una autorización a una política diferente.</p> <p>Esta opción solo está disponible cuando se ve una política de aprobación activa.</p>

Añadir información de nivel a la configuración de políticas de aprobación

Un nivel de aprobación incluye las condiciones que desencadenan un proceso de aprobación cuando el usuario del catálogo de servicios solicita el elemento, así como las propiedades del sistema y del cliente que desee incluir. Cuando se desencadenan, las solicitudes de aprobación se envían a los aprobadores designados.

Para definir la información básica sobre la política de aprobación, seleccione **Administración > Políticas de aprobación**. Haga clic en **Nuevo**. Seleccione el tipo de política y haga clic en **Aceptar**. En la pestaña Aprobación previa o Aprobación posterior, haga clic en el icono **Nuevo (+)**.

Priorice los niveles en función del orden en que desee que se procesen. Cuando se desencadena la política de aprobación, si se rechaza el primer nivel de aprobación, se rechazará la solicitud.

Tabla 3-76. Opciones de información de nivel

Opción	Descripción
Nombre	<p>Escriba un nombre.</p> <p>El nombre de nivel aparece cuando se revisan solicitudes con políticas de aprobación.</p>
Descripción	<p>Escriba una descripción del nivel.</p> <p>Por ejemplo, CPU>4 a administrador de VI.</p>
¿Cuándo se requiere aprobación?	<p>Seleccione cuándo se desencadena la política de aprobación.</p>
Se requiere siempre	<p>Se desencadena la política de aprobación para todas las solicitudes.</p> <p>Si selecciona esta opción y aplica esta política de aprobación a los servicios, los elementos del catálogo o las acciones apropiados en una autorización, es necesario que la solicitud se apruebe con el método de aprobador específico antes de aprovisionarla. Por ejemplo, todas las solicitudes las debe aprobar el administrador del usuario solicitante.</p>

Tabla 3-76. Opciones de información de nivel (continuación)

Opción	Descripción
Se requiere según condiciones	<p>La política de aprobación se basa en una o varias cláusulas de condición.</p> <p>Si selecciona esta opción, debe crear las condiciones. Cuando se aplica esta política de aprobación a los servicios, los elementos del catálogo o las acciones apropiados en una autorización, se evalúan las condiciones. Si las condiciones son verdaderas, la solicitud se debe aprobar con el método de aprobador especificado antes de aprovisionarla. Si son falsas, la solicitud se aprovisiona sin requerir una aprobación. Por ejemplo, todas las solicitudes de una máquina virtual con 4 o más CPU deben ser aprobadas por el administrador de la infraestructura virtual.</p> <p>La disponibilidad de los campos en los que basar las condiciones depende del tipo de política de aprobación o del elemento del catálogo que se haya seleccionado.</p> <p>Cuando se especifica un valor para una condición, se distingue entre mayúsculas y minúsculas.</p> <p>Para configurar más de una cláusula de condición, seleccione la operación booleana para las cláusulas.</p> <ul style="list-style-type: none"> ■ Todos los siguientes. Se desencadena la aprobación cuando todas las cláusulas son verdaderas. Esto equivale a un operador booleano AND entre cada cláusula. ■ Cualesquiera de los siguientes. Se desencadena el nivel de aprobación cuando al menos una de las cláusulas es verdadera. Esto equivale a un operador booleano OR entre cada cláusula. ■ No los siguientes. Se desencadena la aprobación cuando ninguna de las cláusulas es verdadera. Esto equivale a un operador booleano NOT entre cada cláusula.
Aprobadores	Seleccione el método de aprobador.
Usuarios y grupos específicos	<p>Envía la solicitud de aprobación a los usuarios seleccionados.</p> <p>Seleccione los usuarios o grupos de usuarios que deben aprobar la solicitud de catálogo de servicios antes de que se aprovisionen o se ejecute una acción. Por ejemplo, la solicitud se dirige al grupo de administradores de infraestructura virtual con la opción Cualquiera puede aprobar seleccionada.</p>
Determinar aprobadores a partir de la solicitud	<p>Envía la solicitud de aprobación a los usuarios en función de la condición definida.</p> <p>Por ejemplo, si va a aplicar esta política de aprobación en todos los grupos empresariales y desea que el administrador de grupo empresarial la apruebe, seleccione Grupo empresarial > Consumidor > Usuarios > Administrador.</p>

Tabla 3-76. Opciones de información de nivel (continuación)

Opción	Descripción
Usar suscripción a un evento	<p>Procesa la solicitud de aprobación en función de suscripciones a eventos definidas.</p> <p>La suscripción de flujo de trabajo se debe definir en Administración > Eventos > Suscripciones. Las suscripciones de flujo de trabajo correspondientes son de aprobación previa y posterior.</p>
Cualquiera puede aprobar	<p>Solo hace falta que uno de los aprobadores apruebe la solicitud para que se procese.</p> <p>Cuando se solicita el elemento en el catálogo de servicios, las solicitudes de aprobación se envían a todos los aprobadores. Si un aprobador aprueba la solicitud, la solicitud se aprueba y se elimina de la bandeja de entrada de los demás aprobadores.</p> <p>Si el primer aprobador rechaza la solicitud, se notifica al solicitante sobre el rechazo y se elimina la solicitud de la bandeja de entrada de los aprobadores.</p> <p>Si el primer aprobador aprueba la solicitud y esta se abre en la consola del segundo aprobador, no se permite que este envíe la solicitud de aprobación. Se considera ya completada con la respuesta del primer aprobador.</p> <p>Si selecciona Usuarios y grupos específicos o Determinar aprobadores a partir de la solicitud y hay más de un aprobador, es una de las opciones adicionales. Si solo existe un aprobador, esta opción no se aplica.</p>
Todos deben aprobar	<p>Todos los aprobadores deben aprobar la solicitud para que se procese.</p> <p>Si selecciona Usuarios y grupos específicos o Determinar aprobadores a partir de la solicitud y hay más de un aprobador, es una de las opciones adicionales. Si solo existe un aprobador, esta opción no se aplica.</p>

Añadir propiedades del sistema a la configuración de políticas de aprobación

Ha seleccionado propiedades del sistema que desea añadir al formulario de aprobación y que permiten al aprobador modificar el valor.

Por ejemplo, para la aprobación de una máquina virtual, seleccione CPU si desea permitir al aprobador modificar una solicitud de 6 CPU a 4 CPU.

Para seleccionar propiedades del sistema, seleccione **Administración > Políticas de aprobación**. Haga clic en **Nuevo**. Seleccione el tipo de política y haga clic en **Aceptar**. En la pestaña Aprobación previa o Aprobación posterior, haga clic en el icono **Nuevo (+)** y haga clic en la pestaña **Propiedades del sistema**.

Tabla 3-77. Opciones de propiedades del sistema

Opción	Descripción
Propiedades	<p>La lista de propiedades del sistema disponibles depende del tipo de solicitud o elemento del catálogo que se haya seleccionado y de si existen propiedades del sistema para el elemento.</p> <p>Algunas propiedades solo están disponibles cuando el blueprint está configurado de una manera concreta, por ejemplo, en el caso de las CPU. El blueprint al que va a aplicar la política de aprobación con la propiedad del sistema CPU debe estar configurado como rango. Por ejemplo, el mínimo de CPU es 2 y el máximo, 8.</p>

Añadir propiedades personalizadas a la configuración de políticas de aprobación

Configure las propiedades personalizadas que desee añadir al formulario de aprobación para permitir al aprobador modificar el valor.

Por ejemplo, para una aprobación de máquina virtual, añada **VMware.VirtualCenter.Folder** si desea permitirle al aprobador especificar la carpeta en la que se añade la máquina en vCenter Server.

También es posible añadir una propiedad personalizada específica de este formulario de políticas de aprobación.

Para seleccionar propiedades del sistema, seleccione **Administración > Políticas de aprobación**. Haga clic en **Nuevo**. Seleccione el tipo de política y haga clic en **Aceptar**. En la pestaña Aprobación previa o Aprobación posterior, haga clic en el icono **Nuevo (+)** y haga clic en la pestaña **Propiedades personalizadas**.

Tabla 3-78. Propiedades personalizadas

Opción	Descripción
Nombre	Escriba el nombre de la propiedad.
Etiqueta	Escriba la etiqueta que se presenta al aprobador en el formulario de aprobación.
Descripción	<p>Escriba la información ampliada para el aprobador.</p> <p>Esta información aparece como la información sobre herramientas del campo en el formulario.</p>

Modificar una política de aprobación

No puede modificar una política de aprobación activa o inactiva. Debe crear una copia de la política original y sustituir la política que no logra los resultados necesarios. Las políticas de aprobación activas e inactivas son de solo lectura. Puede modificar políticas de aprobación que estén en el estado de borrador.


Cuando realice la copia de la política de aprobación, la nueva política se basará en el tipo de política original. Puede editar todos los atributos excepto el tipo de política. Debe hacerlo cuando desee modificar los niveles de aprobación para modificar, añadir o eliminar niveles o para añadir propiedades del sistema o personalizadas a los formularios.

Puede crear niveles previos y posteriores a la aprobación. Para obtener instrucciones sobre la creación de un nivel de aprobación, consulte [Crear un nivel de aprobación](#).

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador de aprobaciones**.

Procedimiento

- 1 Seleccione **Administración > Políticas de aprobación**.
- 2 Seleccione la fila de la política de aprobación que desee copiar.
- 3 Haga clic en el icono **Copiar** ().
Se creará una copia de la política de aprobación.
- 4 Seleccione la nueva política de aprobación para editarla.
- 5 Escriba un nombre en el cuadro de texto **Nombre**.
- 6 (opcional) Escriba una descripción en el cuadro de texto **Descripción**.
- 7 Seleccione el estado de la política en el menú desplegable **Estado**.

Opción	Descripción
Borrador	Guarda la política de aprobación en un estado que se puede editar.
Activo	Guarda la política de aprobación en un estado de solo lectura que se puede usar en una autorización.
Inactivo	Guarda la política de aprobación en un estado de solo lectura que no se puede usar en una autorización hasta que se active la política.

- 8 Edite los niveles anteriores y posteriores a la aprobación.
- 9 Haga clic en **Aceptar**.

Resultados

Ha creado una nueva política de aprobación basada en una política de aprobación existente.

Pasos siguientes

Aplice la nueva política de aprobación en una autorización. Consulte [Autorizar usuarios a servicios, elementos de catálogo y acciones](#).

Desactivar una política de aprobación

Cuando considere que una política de aprobación es obsoleta, puede desactivarla para que no esté disponible durante el aprovisionamiento.

Para desactivar una política de aprobación, debe asignar una nueva política a cada autorización a la que se aplica actualmente la política de aprobación.

Más adelante podrá reactivar las políticas de aprobación que haya desactivado o eliminarlas.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador de aprobaciones**.

Procedimiento

- 1 Seleccione **Administración > Políticas de aprobación**.
- 2 Haga clic en el nombre de la política de aprobación.
- 3 Haga clic en **Ver autorizaciones vinculadas**.
 - a En el menú desplegable **Reemplazar todo con**, seleccione la nueva política de aprobación.

Si la lista incluye más de una autorización, se aplica la nueva política de aprobación a todas las autorizaciones de la lista.
 - b Haga clic en **Aceptar**.
- 4 Después de comprobar que no hay ninguna autorización vinculada a la política de aprobación, seleccione **Inactivo** en el menú desplegable Estado.
- 5 Haga clic en **Aceptar**.
- 6 Para eliminar una política de aprobación, seleccione una fila que contenga la política inactiva.
 - a Haga clic en **Eliminar**.
 - b Haga clic en **Aceptar**.

Resultados

La política de aprobación se desvincula de cualquier autorización donde se esté usando y se desactiva. Más adelante podrá reactivar y volver a aplicarla a los elementos de una autorización.

Pasos siguientes

Si ya no necesita la política de aprobación, puede eliminarla. Consulte [Eliminar una política de aprobación](#).

Eliminar una política de aprobación

Si tiene políticas de aprobación que ha desactivado y ya no necesita, puede eliminarlas de vRealize Automation.

Requisitos previos

- Desvincule y desactive políticas de aprobación. Consulte [Desactivar una política de aprobación](#).
- Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador de aprobaciones**.

Procedimiento

- 1 Seleccione **Administración > Políticas de aprobación**.
- 2 Seleccione la fila que contenga la política inactiva.
- 3 Haga clic en **Eliminar**.
- 4 Haga clic en **Aceptar**.

Resultados

La política de aprobación se elimina.

Escenario: Crear y aplicar políticas de aprobación de CentOS con MySQL

Como administrador de tenants para el grupo empresarial de ingeniería de desarrollo y calidad, desea aplicar un gobierno estricto a las solicitudes de elementos del catálogo. Antes de que los usuarios puedan aprovisionar el elemento del catálogo CentOS con MySQL, desea que el administrador de infraestructura virtual de vSphere apruebe la solicitud de máquina y que el administrador de software apruebe la solicitud de software.

Cree y aplique una política de aprobación para la solicitud de catálogo de servicios vSphere CentOS con MySQL que requiera que un administrador de infraestructura virtual de vSphere apruebe la máquina según determinadas condiciones y una segunda política de aprobación para el componente de Software MySQL que requiera la aprobación de un administrador de software en cada solicitud.

Los administradores de aprobación solo pueden crear las aprobaciones y los administradores de grupo empresarial pueden aplicarlas a las autorizaciones. Como administrador de tenants, puede crear las aprobaciones y aplicarlas a las autorizaciones.

Requisitos previos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants**. Solo un administrador de tenants puede crear y aplicar políticas de aprobación.
- Asegúrese de que el elemento del catálogo de CentOS con MySQL está incluido como servicio. Consulte [Escenario: Hacer que el blueprint de aplicación CentOS con MySQL esté disponible en el catálogo de servicios](#).

Escenario: Crear una política de aprobación de la máquina virtual CentOS con MySQL

Como administrador de tenant, desea asegurarse de que el grupo de ingeniería de desarrollo y calidad recibe máquinas virtuales correctamente aprovisionadas en su entorno. Para ello, debe crear una política de aprobación que requiera la aprobación previa para determinados tipos de solicitud.

Dado que la máquina virtual CentOS con MySQL consume recursos de vCenter Server, desea que el administrador de infraestructura virtual de vSphere apruebe las solicitudes cuando se soliciten más de 2.048 MB de memoria o más de 2 CPU, con el fin de garantizar el consumo responsable de los recursos. También dota al aprobador de la capacidad de modificar los valores de CPU y memoria solicitados antes de aprobar una solicitud.

Procedimiento

- 1 Seleccione **Administración > Políticas de aprobación**.
- 2 Cree una política de aprobación para el aprovisionamiento de máquinas virtuales.
 - a Haga clic en el icono **Nuevo** (+).
 - b Seleccione **Seleccionar un tipo de política de aprobación**.
 - c En la lista, seleccione **Catálogo de servicios - Solicitud de elemento del catálogo - Máquina virtual**.
 - d Haga clic en **Aceptar**.
 - e Configure las siguientes opciones:

Opción	Configuración
Nombre	Escriba CentOS on vSphere CPU or Memory VM .
Descripción	Escriba Requires VI Admin approval for CPU>2 or Memory>2048 .
Estado	Seleccione Activo .

- 3 En la pestaña **Aprobación previa**, haga clic en el icono **Añadir** (+).
- 4 Configure la pestaña **Información de nivel** con los criterios desencadenantes y las acciones de aprobación.
 - a En el cuadro de texto **Nombre**, escriba **CPU>2 or Memory>2048 – VI Admin**.
 - b En el cuadro de texto **Descripción**, escriba **VI Admin approval for CPU and Memory**.
 - c Seleccione **Se requiere según condiciones**.
 - d En la lista desplegable **Cláusula**, seleccione **Cualesquiera de los siguientes**.
 - e En la nueva lista desplegable **Cláusula**, seleccione **CPU** y configure la cláusula con los valores **CPU > 2**.
 - f Haga clic en **Añadir expresión** y configure la cláusula con los valores **Memory (MB) > 2048**.
 - g Seleccione **Usuarios y grupos específicos**.
 - h Escriba el nombre del administrador de infraestructura virtual de vSphere o del grupo de administradores en el cuadro de búsqueda de texto y haga clic en el icono de búsqueda (🔍).

- i Seleccione el usuario o el grupo.
- j Seleccione **Cualquiera puede aprobar**.

La solicitud solo necesita un administrador de infraestructura virtual para comprobar los recursos y aprobar la solicitud.

- 5 Haga clic en la pestaña **Propiedades del sistema** y seleccione las propiedades que permiten al aprobador modificar los valores de CPU y memoria solicitados antes de aprobar una solicitud.
 - a Active las casillas **CPU** y **Memoria (MB)**.
 - b Haga clic en **Aceptar**.
- 6 Haga clic en **Aceptar**.

Resultados

Ha creado una política de aprobación para solicitudes de máquina virtual, pero desea crear una aprobación para el componente MySQL. No se desencadenará ninguna aprobación hasta que no aplique las políticas a una autorización.

Escenario: Crear una política de aprobación de un componente de Software MySQL

Como administrador de tenants, ha recibido el encargo de los administradores de software de crear y aplicar políticas de aprobación en instalaciones de MySQL, con el fin de realizar un seguimiento del uso de licencias. Cree una política para notificar al administrador de licencias de software cada vez que se solicite un componente de Software MySQL para máquinas virtuales Linux.

Es posible que necesite este tipo de aprobación en algunos entornos, ya que las claves de licencia las debe proporcionar el administrador de software. En este escenario, solo necesita que el administrador de software realice un seguimiento de la solicitud y la apruebe. Después de crear la política de aprobación, debe aplicar la política al elemento del catálogo MySQL para máquinas virtuales Linux. Esta política de aprobación es muy específica y solo se puede aplicar al componente de Software MySQL para máquinas virtuales Linux en las autorizaciones.

Procedimiento

- 1 Seleccione **Administración > Políticas de aprobación**.
- 2 Cree una política de aprobación para el componente de Software MySQL.
 - a Haga clic en el icono **Nuevo** (+).
 - b Seleccione **Seleccionar un elemento**.
 - c Seleccione **MySQL para máquinas virtuales Linux**.

- d Haga clic en **Aceptar**.
- e Configure las siguientes opciones:

Opción	Configuración
Nombre	Escriba MySQL tracking approval .
Descripción	Escriba Approval request sent to software manager .
Estado	Seleccione Activo .

- 3 En la pestaña **Aprobación previa**, haga clic en el icono **Añadir (+)**.
- 4 Configure la pestaña **Información de nivel** con los criterios desencadenantes y las acciones de aprobación.
 - a En el cuadro de texto **Nombre**, escriba **MySQL software deployment notice**.
 - b En el cuadro de texto **Descripción**, escriba **Software mgr approval of software installation**.
 - c Seleccione **Se requiere siempre**.
 - d Seleccione **Usuarios y grupos específicos**.
 - e Escriba el nombre del administrador de software en el cuadro de texto de búsqueda y haga clic en el icono de búsqueda (🔍) y seleccione el usuario.
 - f Seleccione **Cualquiera puede aprobar**.
 La solicitud solo necesita la aprobación de un administrador de software.
 Haga clic en **Aceptar**.

- 5 Haga clic en **Aceptar**.

Resultados

Ha creado políticas de aprobación para máquinas virtuales y para componentes de Software MySQL para máquinas virtuales de Linux. No se desencadenará ninguna aprobación hasta que no aplique las políticas de aprobación a una autorización.

Escenario: Aplicar políticas de aprobación a componentes de CentOS con MySQL

Como administrador de tenant, puede crear autorizaciones y políticas de aprobación. Modifique la autorización de desarrollo y calidad para aplicar las políticas de aprobación que ha creado para que las aprobaciones se activen cuando un usuario del catálogo de servicios solicite el elemento.

Si bien sería sencillo autorizar todo el servicio del catálogo a su grupo empresarial, eso no le permitiría tener el mismo control y gobierno que si creara autorizaciones individuales para los elementos del catálogo. Por ejemplo, si autoriza usuarios en un servicio, podrán solicitar cualquier elemento del catálogo de dicho servicio, así como todos los elementos que se añadan al servicio en el futuro. También significa que solo puede usar en el servicio políticas de aprobación de muy alto nivel aplicables a todos los elementos del catálogo; por ejemplo, requerir siempre la

aprobación de un administrador. Si elige autorizar los elementos del catálogo uno a uno, puede crear y aplicar políticas de aprobación muy específicas para cada elemento y llevar un control estricto de quién puede solicitar cada uno de los elementos del servicio. Incluso puede tener un mayor control si elige autorizar los componentes individuales de cada uno de los elementos del catálogo.

Si no sabe qué políticas de aprobación debe aplicar a los elementos en una autorización, puede volver más tarde y aplicarlas. En este escenario, puede aplicar políticas de aprobación diferentes a dos componentes del mismo blueprint de aplicación publicado.

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Autorizaciones**.
- 2 Haga clic en **Autorización de desarrollo y calidad**.
- 3 Haga clic en la pestaña **Elementos y aprobaciones**.
- 4 Añada la máquina CentOS con MySQL y aplique la política de aprobación.
 - a Haga clic en el icono **Añadir elementos** (+) junto al encabezado Elementos autorizados.
 - b Active la casilla **CentOS con MySQL**.
 - c Haga clic en la flecha desplegable **Aplicar esta política a los elementos seleccionados**.
La política CPU y memoria de CentOS en vSphere no aparece en la lista.
 - d Haga clic en **Mostrar todo** y en la flecha desplegable para ver todas las políticas de aprobación.
 - e Seleccione **CPU y memoria de CentOS en vSphere [Catálogo de servicios - Solicitud de elemento del catálogo - Máquina virtual]**.
La máquina CentOS de vSphere es un blueprint de máquina en un blueprint de aplicación. Revise los nombres de políticas y seleccione la más adecuada al tipo de elemento del catálogo. Si aplica una política incorrecta, la política de aprobación genera errores o desencadena solicitudes de aprobación basadas en condiciones incorrectas.
 - f Haga clic en **Aceptar**.
- 5 Añada el componente de software MySQL para máquinas virtuales de Linux como elemento y aplique una política de aprobación al elemento de MySQL.
 - a Haga clic en el icono **Añadir elementos del catálogo y componentes** (+) junto al encabezado Elementos del catálogo y componentes autorizados.
 - b En el menú desplegable **Elementos del catálogo y componentes**, seleccione **No**.
Los componentes de software siempre están asociados a una máquina. No están disponibles para solicitudes individualmente en el catálogo de servicios.
 - c Active la casilla **MySQL para máquinas virtuales de Linux**.
 - d Haga clic en la flecha desplegable **Aplicar esta política a los elementos seleccionados**.

- e Seleccione **Aprobación de seguimiento de MySQL [Catálogo de servicios - Solicitud de elemento del catálogo - Componente de software]**.

No necesita la opción avanzada porque la política de aprobación se creó para este componente de software específico, que se añade a una máquina virtual.

- f Haga clic en **Aceptar**.

6 Añada acciones que los usuarios puedan ejecutar en la máquina aprovisionada.

Las políticas de aprobación no se aplican a las acciones en este escenario.

- a Haga clic en el icono **Añadir acciones** (+) junto al encabezado Acciones autorizadas.
- b Seleccione las siguientes acciones.

Nombre / Tipo	Descripción
Crear snapshot / máquina virtual	Crea un snapshot de la máquina virtual, incluido el software instalado. Permite que los desarrolladores creen snapshots que pueden restaurar durante el desarrollo.
Destruir / Implementación	Destruye todo el blueprint aprovisionado, no solo la máquina. Use esta acción para evitar los componentes huérfanos.
Apagar / máquina	Apaga la máquina virtual.
Encender / máquina	Enciende la máquina virtual.
Restaurar snapshot / máquina virtual	Restaura un snapshot creado previamente.

- c Haga clic en **Aceptar**.

7 Haga clic en **Finalizar**.

Resultados

Esta autorización te permite requerir diferentes aprobaciones en componentes de blueprint distintos.

Pasos siguientes

Solicite el elemento de CentOS con MySQL en el catálogo de servicios como miembro del grupo empresarial para comprobar que la autorización y las aprobaciones se comportan del modo esperado.

Solicitar el aprovisionamiento de máquinas a través de un blueprint parametrizado

Cuando se solicita el aprovisionamiento de máquinas para un blueprint de máquina de vSphere que se ha diseñado para incluir los perfiles de los componentes de imagen o de tamaño, se debe especificar la configuración de aprovisionamiento mediante la selección de un conjunto de valores disponibles.

Cuando se solicita el aprovisionamiento desde el catálogo, se puede seleccionar una de las opciones de conjunto de valores disponibles relativas a los perfiles de componente Size y Image. Al elegir uno de los conjuntos de valores, sus valores de propiedad correspondientes se enlazan a la solicitud.

El conjunto de valores del perfil de componente se aplica a todas las máquinas de vSphere en un clúster.

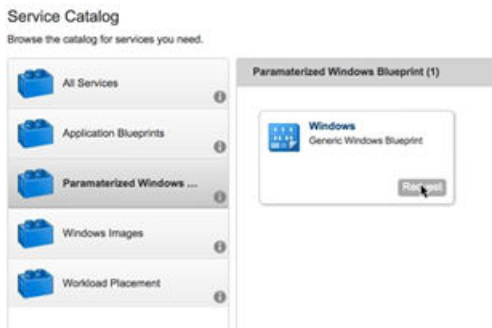
Para obtener más información sobre la configuración del perfil de componentes, consulte [Descripción y el uso de la parametrización de blueprints](#).

Requisitos previos

- Defina los conjuntos de valores para los perfiles de los componentes de Size o Image. Consulte y en *Referencia de propiedades personalizadas*.
- Cree un blueprint que contenga un componente de máquina de vSphere con un perfil de componentes de Image o Size. Consulte [Configurar un blueprint de máquina](#) y [Configuración de los componentes de máquina de vSphere](#).
- Publique el blueprint en el catálogo. Consulte [Publicar un blueprint](#).
- Configure el blueprint en el catálogo. Consulte [Lista de comprobación para configurar el catálogo de servicios](#) y [Ejemplos de políticas de aprobación basadas en el tipo de política de máquina virtual](#).

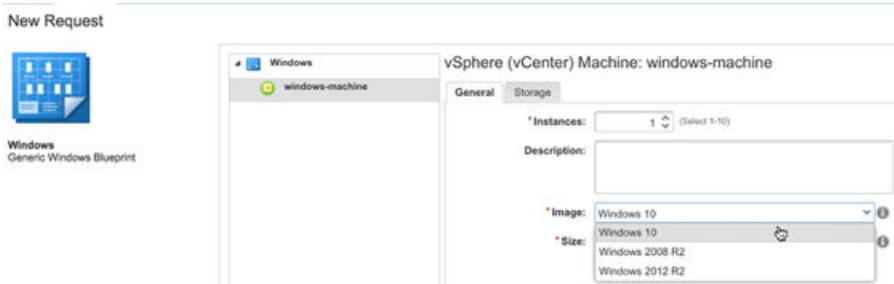
Procedimiento

- 1 Haga clic en **Catálogo**.
- 2 Seleccione el servicio del catálogo para solicitar y haga clic en **Solicitar**.

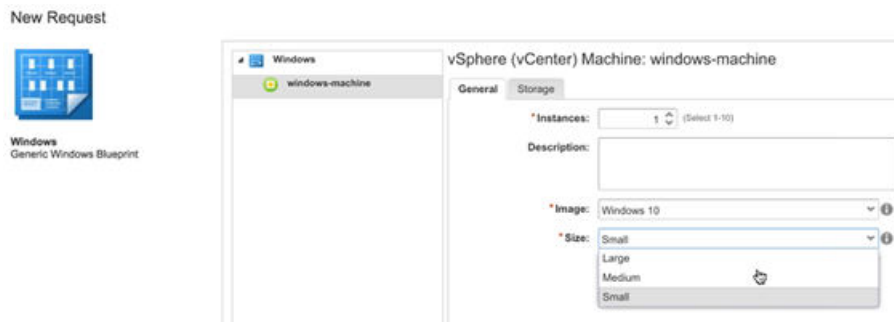


- 3 Seleccione el componente de máquina de vSphere que desea aprovisionar y especifique el número de instancias que deben aprovisionarse.

- 4 Seleccione una opción de conjunto de valores de imagen en el menú desplegable **Imagen**.



- 5 Seleccione una opción de conjunto de valores de tamaño en el menú desplegable **Tamaño**.



- 6 Haga clic en **Enviar**.

Pasos siguientes

Los conjuntos de valores que haya definido para los perfiles de componentes de Size y Image ahora se encuentran disponibles en los menús desplegables **Imagen** y **Tamaño** en la pestaña **Catálogo** en el formulario de solicitud de aprovisionamiento de catálogos.

Escenario: Hacer que el blueprint de aplicación CentOS con MySQL esté disponible en el catálogo de servicios

Como administrador de tenants, ha solicitado que los arquitectos de blueprints creen un elemento del catálogo para proporcionar máquinas virtuales MySQL en CentOS para que los ingenieros de desarrollo y calidad ejecuten casos de prueba. Según el arquitecto de software, el elemento del catálogo está listo para los usuarios. Para que el elemento esté disponible para los usuarios empresariales, debe asociar los blueprints y el componente de Software a un servicio del catálogo y, a continuación, debe autorizar a los miembros del grupo empresarial para que soliciten el elemento del catálogo.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants** o **administrador del catálogo**.
- Publique un blueprint de aplicación para proporcionar MySQL en máquinas virtuales de vSphere CentOS. Consulte *Instalación y configuración de vRealize Automation para el escenario de Rainpole*.

- Si crea blueprints en un entorno de desarrollo, importe el blueprint en su entorno de producción. Consulte [Exportar e importar blueprints y contenido](#).
- Cree una reserva para asignar recursos de vSphere al grupo empresarial de desarrollo y calidad. Consulte [Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer](#).

Procedimiento

1 [Escenario: Crear un servicio del catálogo de ingeniería de desarrollo y calidad](#)

Como administrador de tenants, desea crear un servicio del catálogo independiente para su grupo de ingeniería de desarrollo y calidad para que los demás grupos (por ejemplo, de finanzas y de recursos humanos) no vean los elementos del catálogo especializados. Debe crear un servicio del catálogo denominado Servicio de desarrollo y calidad para publicar todos los elementos del catálogo que el grupo de ingeniería y desarrollo necesita para ejecutar sus casos de prueba.

2 [Escenario: Añadir CentOS con MySQL al servicio de desarrollo y calidad](#)

Como administrador de tenants, desea añadir el elemento del catálogo CentOS con MySQL al servicio de desarrollo y calidad.

3 [Escenario: Autorizar a los usuarios para solicitar elementos de servicio de desarrollo y calidad como elementos del catálogo](#)

Como administrador de tenant, cree una autorización de desarrollo y calidad y añada los elementos del catálogo y algunas acciones relevantes para que los usuarios de ingeniería de desarrollo y calidad puedan solicitar el elemento del catálogo CentOS con MySQL, y ejecutar acciones en la máquina y en la implementación.

Escenario: Crear un servicio del catálogo de ingeniería de desarrollo y calidad

Como administrador de tenants, desea crear un servicio del catálogo independiente para su grupo de ingeniería de desarrollo y calidad para que los demás grupos (por ejemplo, de finanzas y de recursos humanos) no vean los elementos del catálogo especializados. Debe crear un servicio del catálogo denominado Servicio de desarrollo y calidad para publicar todos los elementos del catálogo que el grupo de ingeniería y desarrollo necesita para ejecutar sus casos de prueba.

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Servicios**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Escriba el nombre **Dev and QE Service** en el cuadro de texto **Nombre**.
- 4 Escriba la descripción **Dev and QE application catalog items for test cases** en el cuadro de texto **Descripción**.
- 5 Seleccione **Activo** en el menú desplegable **Estado**.

6 Como administrador del catálogo que crea el servicio, utilice la opción de búsqueda para añadir su nombre como propietario.

7 Añada el grupo de usuarios personalizado Equipo de soporte.

Por ejemplo, añada un grupo de usuarios personalizado que incluya los arquitectos de IaaS y arquitectos de software para que tanto usted como los usuarios del catálogo de servicios tengan alguien a quien consultar en caso de que surja algún problema durante el aprovisionamiento de los elementos del catálogo.

8 Haga clic en **Aceptar**.

Resultados

Ha creado y activado un servicio del catálogo de desarrollo y calidad, pero todavía no contiene ningún elemento de catálogo.

Escenario: Añadir CentOS con MySQL al servicio de desarrollo y calidad

Como administrador de tenants, desea añadir el elemento del catálogo CentOS con MySQL al servicio de desarrollo y calidad.

Procedimiento

1 Seleccione **Administración > Administración de catálogos > Servicios**.

2 Seleccione la fila del servicio de desarrollo y calidad en la lista **Servicios** y haga clic en **Administrar elementos del catálogo**.

3 Haga clic en el icono **Nuevo** (+).

4 Seleccione **CentOS con MySQL**.

Solo aparecen en la lista los componentes y blueprints publicados que todavía no estén asociados a un servicio. Si no ve el blueprint, compruebe que se haya publicado o que no se haya incluido en otro servicio.

5 Haga clic en **Aceptar**.

6 Haga clic en **Cerrar**.

Resultados

Ha publicado el elemento del catálogo CentOS con MySQL en el servicio de desarrollo y calidad, pero debe autorizar a los usuarios en el elemento o servicio para que puedan ver o solicitar el elemento.

Escenario: Autorizar a los usuarios para solicitar elementos de servicio de desarrollo y calidad como elementos del catálogo

Como administrador de tenant, cree una autorización de desarrollo y calidad y añada los elementos del catálogo y algunas acciones relevantes para que los usuarios de ingeniería de desarrollo y calidad puedan solicitar el elemento del catálogo CentOS con MySQL, y ejecutar acciones en la máquina y en la implementación.

En este escenario, autoriza el servicio porque desea que los usuarios tengan autorización para cualquier futuro elemento del catálogo que se añada a este servicio. También desea permitir que los usuarios administren su implementación aprovisionada, de modo que añade a la autorización acciones tales como encender y apagar, snapshot y destruir implementación.

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Autorizaciones**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Configure los detalles.
 - a Escriba el nombre **Dev and QE Entitlement** en el cuadro de texto **Nombre**.
 - b En el menú desplegable **Estado**, seleccione **Activo**.
 - c En el menú desplegable **Grupo empresarial**, seleccione el grupo **Desarrollo y calidad**.
 - d En el área Usuarios y grupos, añada uno o varios usuarios.

Añádase únicamente a sí mismo, a menos que esté seguro de que el blueprint funciona del modo previsto. En tal caso, puede añadir usuarios individuales y grupos de usuarios personalizados.

- e Haga clic en **Siguiente**.
- 4 Añada el servicio.

Aunque esté añadiendo los elementos del catálogo CentOS y MySQL por separado, añadir el servicio garantiza que cualquier elemento que añada al servicio posteriormente estará disponible para los miembros del grupo empresarial en el catálogo de servicios.

 - a Haga clic en el icono **Añadir servicios** (+) junto al encabezado Servicios autorizados.
 - b Seleccione **Servicio de desarrollo y calidad**.
 - c Haga clic en **Aceptar**.

El servicio de desarrollo y calidad se añade a la lista Servicios autorizados.

5 Añada acciones.

- a Haga clic en el icono **Añadir acciones** (+) junto al encabezado Acciones autorizadas.
- b Haga clic en el encabezado de columna Tipo para ordenar la lista.

Seleccione las siguientes acciones en función del tipo. Estas acciones son útiles para los usuarios de ingeniería de desarrollo y calidad que trabajan con sus máquinas de pruebas, y son las únicas acciones que desea que utilicen estos miembros del grupo empresarial.

Tipo	Nombre de acción
Máquina	Encender
Máquina	Apagar
Máquina virtual	Crear snapshot
Máquina virtual	Restaurar el snapshot
Implementación	Destruir
	La acción Destruir implementación destruye toda la implementación y no solamente la máquina virtual.

- c Haga clic en **Aceptar**.

Las cinco acciones se añaden a la lista Acciones autorizadas.

6 Haga clic en **Finalizar**.

Resultados

Ha añadido el elemento del catálogo CentOS con MySQL al nuevo servicio del catálogo Desarrollo y calidad y ha autorizado a los miembros del grupo empresarial a solicitar y administrar el elemento.

Pasos siguientes

Después de comprobar su trabajo aprovisionando el elemento del catálogo CentOS con MySQL, puede añadir otros usuarios a la autorización para que el elemento del catálogo esté disponible públicamente para los usuarios de ingeniería de desarrollo y calidad. Si ya no desea gobernar el aprovisionamiento de recursos en su entorno, puede crear políticas de aprobación para el componente de Software MySQL y la máquina CentOS para pruebas de software. Consulte [Escenario: Crear y aplicar políticas de aprobación de CentOS con MySQL](#).

Administrar los elementos de catálogo implementados

Puede ver las implementaciones aprovisionadas, y actuar en ellas, incluidos las máquinas, los equilibradores de carga, las redes y otros recursos de la implementación.

Ejecutar acciones en recursos aprovisionados

Las acciones que están disponibles en un recurso aprovisionado dependen del tipo de recurso, del modo en que se configuró la acción y quedó disponible para los elementos aprovisionados y del estado operativo del elemento.

Las acciones configuradas disponibles de una máquina aprovisionada o implementación aparecen en el menú **Acciones** del recurso seleccionado en la pestaña **Elementos**.

Si el elemento fue aprovisionado por IaaS mediante un blueprint de IaaS, la lista de acciones disponibles está determinada por lo seleccionado en la pestaña **Acciones** para el componente del tipo de máquina cuando se creó el blueprint y, después, por lo que se aplique en función del tipo de máquina o estado.

Si el elemento se aprovisionaba con un blueprint XaaS, las acciones personalizadas deben crearse, publicarse y autorizarse en el mismo servicio que se utiliza para aprovisionar el elemento. La lista de acciones disponibles está determinada por el tipo de elemento y el estado actual del mismo.

Las acciones disponibles de un elemento que se haya aprovisionado como una máquina de IaaS también podrían incluir acciones personalizadas de XaaS si las acciones se asignan al elemento.

Comandos del menú Acción en recursos aprovisionados

Las acciones son cambios que pueden realizarse en los recursos aprovisionados. Las acciones de vRealize Automation se usan para administrar el ciclo de vida de los recursos.

Los comandos del menú **Acción** para un recurso aprovisionado incluyen las acciones especificadas en el blueprint, las cuales pueden incluir operaciones de menú personalizadas creadas por los arquitectos de servicio. Las acciones disponibles dependen de cómo el administrador de tenants o de grupo empresarial haya configurado la autorización que contiene el recurso donde se ejecutan las acciones.

No debe administrar objetos NSX administrados por vRealize Automation fuera de vRealize Automation. Por ejemplo, si modifica el puerto de miembro de un equilibrador de carga de NSX implementado en NSX, en lugar de en vRealize Automation, la recopilación de datos de NSX rompe la asociación que existía entre la máquina implementada y el grupo de miembros de equilibradores de carga. Los resultados de las operaciones de escalado vertical y escalado horizontal tampoco se pueden prever cuando un puerto de miembro de equilibrador de carga se modifica fuera de vRealize Automation.

Las acciones que se enumeran en la siguiente tabla no son válidas para todos los tipos de recursos implementados. Por ejemplo, algunos elementos de integración de NSX no admiten ninguna de estas acciones.

Tabla 3-79. Comandos del menú Acción

Acción	Tipo de recurso	Descripción
Asociar IP flotante	Máquina (OpenStack)	Asocie una dirección IP flotante a una máquina de OpenStack.
Cancelar reconfiguración	Máquina	Cancele una acción de reconfiguración en ejecución.
Cambiar concesión	Implementación y Máquina	Cambie el número de días restantes en la concesión de una máquina determinada o de todos los recursos que se incluyen en una implementación. Si no proporciona ningún valor, la concesión no caduca.
Cambiar reglas NAT	Red NAT	<p>Añada nuevas reglas de enrutamiento de puerto NAT o reordene, edite o elimine las ya existentes.</p> <p>Para obtener más información, consulte Cambiar las reglas NAT en una implementación.</p>
Cambiar propietario	Implementación	<p>Cambie el propietario de la implementación y de todos los recursos incluidos. Solo los administradores de grupo empresarial y los usuarios de soporte pueden cambiar la propiedad de una implementación.</p> <p>La máquina debe estar en estado Activado, Desactivado o Activo cuando se inicia la acción de cambio de propietario, o cuando se produce un error en la acción y se muestra el siguiente mensaje:</p> <p>La acción no es válida para la máquina.</p>
Cambiar seguridad	Implementación	<p>Puede añadir o quitar etiquetas de seguridad y grupos de seguridad de NSX existentes. También puede quitar grupos de seguridad a petición.</p> <p>Para obtener más información, consulte Agregar o quitar elementos de seguridad en una implementación.</p>
Conectar mediante VMRC	Máquina	<p>Conéctese a la máquina virtual con una aplicación VMRC 8.x.</p> <p>Para usar esta acción, la aplicación VMRC debe estar instalada en el sistema local del usuario del catálogo de servicios que está ejecutando la acción.</p> <p>Para obtener instrucciones de instalación y de uso, consulte la documentación de VMware Remote Console. Para descargarla, visite la página de descarga de VMware Remote Console.</p> <p>La aplicación VMRC 8.x reemplaza la instancia anterior de VMware Remote Console.</p>

Tabla 3-79. Comandos del menú Acción (continuación)

Acción	Tipo de recurso	Descripción
Conectar con la consola remota	Máquina	<p>Conéctese a la máquina seleccionada mediante VMware Remote Console.</p> <p>La consola de la máquina virtual aparece en el navegador. La aplicación VMRC 8.x reemplaza VMware Remote Console.</p>
Conectar mediante ticket de consola	Máquina (OpenStack y KVM)	Conéctese a la máquina virtual OpenStack o KVM con un ticket de consola para una conexión de VMware Remote Console.
Conectar mediante ICA	Máquina (Citrix)	Conéctese a la máquina de Citrix mediante Independent Computing Architecture.
Conectar mediante RDP	Máquina	Conéctese a la máquina seleccionada mediante Microsoft Remote Desktop Protocol.
Conectar mediante SSH	Máquina	<p>Conecte con la máquina seleccionada mediante SSH.</p> <p>La opción Conectar mediante SSH requiere que el navegador tenga un complemento que admita SSH, como el cliente de terminal SSH FireSSH para Mozilla Firefox y Google Chrome. Cuando el complemento está instalado, se muestra una consola de SSH que le solicita las credenciales de administrador al seleccionar Conectar mediante SSH.</p> <p>Para usar esta acción, se debe incluir la propiedad personalizada Machine.SSH y establecerla en True en el componente de máquina del blueprint, ya sea en un grupo de propiedades o en una propiedad personalizada individual.</p>
Conectar mediante escritorio virtual	Máquina	Conéctese a la máquina seleccionada mediante el escritorio virtual de Microsoft.
Crear snapshot	Máquina virtual	<p>Cree un snapshot de la máquina virtual. Si se permiten solo dos snapshots y ya los tiene, el comando no estará disponible hasta que elimine uno.</p> <p>Para obtener más información, consulte Crear un snapshot en la máquina.</p>
Eliminar snapshot	Máquina virtual	Elimine un snapshot de la máquina virtual.

Tabla 3-79. Comandos del menú Acción (continuación)

Acción	Tipo de recurso	Descripción
Destruir	Implementación, máquina y grupo de seguridad a petición	<p data-bbox="943 268 1326 321">Destruya inmediatamente un recurso provisionado.</p> <p data-bbox="943 338 1406 516">Excepto en el caso de XaaS, destruir componentes de una implementación no es una práctica que se recomienda. Utilice la acción de escalado vertical para reducir el número de máquinas en la implementación o bien destruir toda la implementación.</p> <p data-bbox="943 533 1406 680">Debe ejecutar esta acción para destruir recursos de XaaS, incluso si forman parte de la implementación que está destruyendo. Otros recursos se destruyen cuando su concesión o período de archivado finaliza.</p> <p data-bbox="943 697 1414 749">La opción Destruir no está disponible para las siguientes situaciones de implementación:</p> <ul data-bbox="943 766 1390 955" style="list-style-type: none"> ■ implementaciones de máquinas físicas ■ implementaciones con una red de NSX existente o un recurso de seguridad de NSX existente ■ implementaciones con un recurso de equilibrador de carga a petición de NSX <p data-bbox="943 972 1406 1245">Puesto que un equilibrador de carga de NSX pertenece a una instancia de NSX Edge, cuando se destruye una instancia de NSX Edge, también se destruye el recurso de equilibrador de carga y se liberan los recursos. Cuando se destruye un nivel de máquina con equilibrio de carga, se elimina el grupo de equilibradores de carga en el NSX Edge correspondiente.</p> <p data-bbox="943 1276 1422 1770">Nota La acción Destruir puede devolver un mensaje de operación correcta aunque no pueda quitar una implementación de máquina del endpoint (por ejemplo, si una máquina de vSphere se encuentra en un almacén de datos que no es de vSAN y su archivo .vmx contiene datos dañados o no válidos). Debe comprobar el log de solicitudes para obtener información adicional, incluso si el mensaje de Destruir indica que la operación se ha realizado correctamente. La destrucción forzada de una máquina en este estado puede dejarla en ejecución en el endpoint y causar conflictos de IP. Si corrige los daños en el endpoint (fuera de vRealize Automation), puede volver a ejecutar la acción Destruir.</p>

Tabla 3-79. Comandos del menú Acción (continuación)

Acción	Tipo de recurso	Descripción
		<p>Los administradores de grupo empresarial pueden elegir forzar la destrucción de una implementación después de que se produzca un error en una solicitud de destrucción. En la destrucción forzada, vRealize Automation recibe instrucciones para ignorar los errores por la destrucción de recursos individuales mientras se destruye la implementación. Para obtener más información sobre cómo usar la destrucción forzada, consulte Forzar la destrucción de una implementación tras una solicitud de destrucción fallida.</p> <p>Nota El almacenamiento y la memoria que se asignan a una máquina aprovisionada por una reserva se liberan cuando se elimina en vRealize Automation la máquina a la que están asignados, mediante la acción Destruir. El almacenamiento y la memoria no se liberan si la máquina se elimina en vCenter Server.</p> <p>Cuando se destruye una implementación con un componente de máquina de Amazon, es posible destruir más de un volumen de EBS al mismo tiempo en función de la forma en la que se configuró la opción Eliminar volúmenes en el blueprint. Para obtener más información, consulte Configuración de componentes de máquina de Amazon.</p> <p>Al destruir una implementación que contiene un componente de máquina de Amazon, se desconectan todos los volúmenes de EBS que se agregaron a la máquina durante este ciclo de vida, en lugar de destruirse. vRealize Automation no proporciona una opción para destruir los volúmenes de EBS.</p>
Desasociar IP flotante	Máquina (OpenStack)	Elimine la dirección IP flotante de la máquina de OpenStack.
Ejecutar reconfiguración	Máquina	Reemplace una configuración programada, o vuelva a ejecutar o programar una reconfiguración con errores.
Caducidad	Implementación y Máquina	Finalice la concesión de la máquina o la implementación para todos los recursos incluidos en la implementación.
Exportar certificado	Máquina	Exporte el certificado desde una máquina en la nube.
Obtener recordatorio de caducidad	Máquina	Descarga un archivo de evento de calendario para la fecha de caducidad de la concesión actual.

Tabla 3-79. Comandos del menú Acción (continuación)

Acción	Tipo de recurso	Descripción
Instalar VMware Tools	Máquina	Instale VMware Tools en una máquina virtual de vSphere.
Ciclo de energía	Máquina	Apague la máquina y vuelva a encenderla.
Apagar	Máquina	Apague la máquina sin cerrar el sistema operativo invitado.
Encender	Máquina	Encienda la máquina. Si la máquina estaba suspendida, el funcionamiento normal se reanudará desde el punto en el que la máquina había quedado suspendida.
Reiniciar	Máquina	Reinicie el sistema operativo invitado en una máquina virtual de vSphere. VMware Tools debe estar instalado en la máquina para poder usar esta acción.

Tabla 3-79. Comandos del menú Acción (continuación)

Acción	Tipo de recurso	Descripción
Reconfigurar	Máquina	<p data-bbox="943 268 1390 420">Un administrador de grupo empresarial, un usuario de soporte o un propietario de máquina pueden realizar las siguientes acciones de reconfiguración de la máquina virtual de vSphere seleccionada:</p> <ul data-bbox="943 432 1422 831" style="list-style-type: none"> <li data-bbox="943 432 1214 453">■ Cambiar la descripción <li data-bbox="943 468 1414 527">■ Cambiar los ajustes de CPU, memoria, red y disco. <li data-bbox="943 539 1406 598">■ Agregar, editar y eliminar propiedades personalizadas y grupos de propiedades <li data-bbox="943 611 1374 699">■ Añadir, editar, reordenar o eliminar un adaptador de red para las reglas de enrutamiento de puerto NAT <li data-bbox="943 711 1238 732">■ Reconfigurar el apagado <li data-bbox="943 745 1422 831">■ Cambiar el propietario de la máquina (disponible para administradores de grupo empresarial y usuarios de soporte solo) <p data-bbox="943 846 1414 934">No puede cambiar una política de reserva de almacenamiento si con ello se cambia el perfil de almacenamiento de un disco.</p> <p data-bbox="943 947 1406 1066">Para obtener más información, consulte Especificar los ajustes de reconfiguración de máquinas y consideraciones de reconfiguración.</p> <p data-bbox="943 1079 1422 1453">Si seleccionó la opción Propagar actualizaciones a implementaciones existentes en la página Configuración de blueprints en el blueprint de origen, cualquier aumento o ampliación de los valores máximos y mínimos de la CPU, la memoria o el almacenamiento del blueprint se insertarán en las implementaciones activas que se aprovisionaron desde dicho blueprint. Para obtener más información, consulte Configuración de las propiedades de blueprint.</p>

Tabla 3-79. Comandos del menú Acción (continuación)

Acción	Tipo de recurso	Descripción
Reconfigurar el equilibrador de carga	Implementación	<p>Los propietarios de máquinas, los usuarios de soporte, los administradores de tenants o los administradores de grupos empresariales que estén autorizados pueden modificar la configuración de un servidor virtual, así como agregar o quitar servidores virtuales del equilibrador de carga de NSX:</p> <p>Para obtener más información, consulte Reconfigurar un equilibrador de carga en una implementación.</p> <p>Para obtener información sobre la configuración del servidor virtual en el equilibrador de carga, consulte Añadir un componente de equilibrador de carga a petición.</p>
Registrar VDI	Máquina virtual (XenServer)	Registre la imagen de disco virtual en elementos de XenServer.
Reaprovisionar	Máquina	<p>Destruye la máquina y después inicia el flujo de trabajo de aprovisionamiento para crear una máquina con el mismo nombre.</p> <p>Cuando solicita que se reaprovisione una máquina, existe un problema conocido que puede hacer que vRealize Automation muestre el estado de reaprovisionamiento como Completado en el catálogo, aunque realmente sea En curso. Después de enviar una solicitud para reaprovisionar una máquina, puede usar cualquiera de las secuencias siguientes para comprobar el estado de la máquina reaprovisionada:</p> <ul style="list-style-type: none"> ■ Infraestructura > Máquinas administradas ■ Elementos > Detalles del elemento ■ Administración > Eventos > Logs de eventos <p>Nota No se puede reaprovisionar una máquina de Amazon.</p> <p>Para obtener información relacionada, consulte el artículo 2065873 de la base de conocimientos de VMware relacionado con las tareas de máquinas reaprovisionadas en http://kb.vmware.com/kb/2065873.</p>

Tabla 3-79. Comandos del menú Acción (continuación)

Acción	Tipo de recurso	Descripción
Reanudar	Implementación	Si se produce un error en una implementación, lo que puede deberse a problemas temporales de entorno, problemas de infraestructura, agotamiento del tiempo de espera u otros problemas locales, puede reanudar el proceso de aprovisionamiento en lugar de crear una nueva solicitud de aprovisionamiento.
Restaurar el snapshot	Máquina virtual	Restaure un snapshot anterior de la máquina. Debe tener ya un snapshot para usar esta acción.
Escalado vertical	Implementación	<p>En la implementación, destruya las instancias innecesarias de las máquinas para ajustarse a los requisitos de capacidad reducida. Se destruirán los componentes de máquina y los componentes de software que estén instalados en ellos. Los componentes de software dependientes y los componentes de redes y seguridad se actualizan para la nueva configuración de implementación. Los componentes de XaaS no pueden escalarse y no se actualizan durante las operaciones de escalado.</p> <p>Puede volver a escalar la implementación para intentar reparar las operaciones de escalado parcialmente correcto. Sin embargo, no puede escalar una implementación a su tamaño actual. Además, al reparar un escalado parcialmente correcto de este modo, no se anula la asignación de los recursos pendientes. Para decidir si desea reparar el escalado parcialmente correcto con otra operación de escalado, puede ver la pantalla de detalles de ejecución de la solicitud y buscar las tareas y los nodos donde se produjeron errores. Las operaciones de escalado incorrecto y parcialmente correcto no afectan a la funcionalidad de la implementación original, y puede seguir usando los elementos del catálogo al solucionar problemas.</p>

Tabla 3-79. Comandos del menú Acción (continuación)

Acción	Tipo de recurso	Descripción
Escalado horizontal	Implementación	<p>Durante la implementación, aprovisiona otras instancias de máquinas para ajustarse a los requisitos de capacidad en expansión. Se aprovisionan los componentes de máquina y los componentes de software que estén instalados en ellos. Los componentes de software dependientes y los componentes de redes y seguridad se actualizan para la nueva configuración de implementación. Los componentes de XaaS no pueden escalarse y no se actualizan durante las operaciones de escalado.</p> <p>Puede volver a escalar la implementación para intentar reparar las operaciones de escalado parcialmente correcto. Sin embargo, no puede escalar una implementación a su tamaño actual. Además, al reparar un escalado parcialmente correcto de este modo, no se anula la asignación de los recursos pendientes. Para decidir si desea reparar el escalado parcialmente correcto con otra operación de escalado, puede ver la pantalla de detalles de ejecución de la solicitud y buscar las tareas y los nodos donde se produjeron errores. Las operaciones de escalado incorrecto y parcialmente correcto no afectan a la funcionalidad de la implementación original, y puede seguir usando los elementos del catálogo al solucionar problemas.</p>
Desconectar	Máquina	Cierre el sistema operativo invitado y apague la máquina. VMware Tools debe estar instalado en la máquina para poder usar esta acción.
Suspender	Máquina	Ponga en pausa la máquina para que no se pueda utilizar y no consuma ningún otro recurso del sistema que no sea el almacenamiento que está usando.
Eliminar del registro	Máquina	Elimine la máquina del inventario sin destruirla. No se pueden usar las máquinas que no estén registradas.
Eliminar del registro	Red	Quite la red del inventario sin destruirla. No se pueden usar redes que no estén registradas.
Eliminar VDI del registro	Máquina virtual (XenServer)	Elimine la imagen de disco virtual del registro en elementos de XenServer.

Configurar un proveedor de métricas

vRealize Automation se puede configurar para que use métricas de recurso y estado de vRealize Operations Manager para máquinas virtuales de vSphere.

Para obtener información sobre las métricas y notificaciones de estado de vRealize Operations Manager, consulte la documentación de vRealize Operations Manager.

Requisitos previos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants**, **administrador de grupo empresarial** o **propietario de la máquina**.
- Cree una cuenta de usuario de vRealize Operations Manager con privilegios de visualización y consulta de métricas de recurso en todos los servidores de vSphere que integre con vRealize Automation.
- Cree instancias de adaptador de vRealize Operations Manager para todos los servidores de vSphere que añada como endpoints en vRealize Automation. Para obtener información sobre cómo crear instancias de adaptador, consulte la documentación de vRealize Operations Manager.

Procedimiento

- 1 Seleccione **Administración > Recuperación > Proveedor de métricas**.
- 2 Seleccione un proveedor de métricas.

Opción	Descripción
(Predeterminado) Proveedor de métricas de vRealize Automation	Si no tiene una instancia de vRealize Operations Manager, vRealize Automation suministra métricas de máquina básicas.
Endpoint de vRealize Operations Manager	Proporcione la información de conexión de la instancia de vRealize Operations Manager que quiera usar como proveedor de métricas de las máquinas virtuales de vSphere.

- 3 Haga clic en **Probar conexión**.
- 4 Haga clic en **Guardar**.

Resultados

Los administradores de tenants, propietarios de máquinas y administradores del grupo empresarial donde reside la máquina pueden ver los distintivos de estado en las páginas de detalles del elemento para las máquinas virtuales vSphere. También pueden consultar métricas y distintivos de estado de vRealize Operations Manager si filtran por tipo de plataforma vSphere en la página de recuperación.

Pasos siguientes

[Enviar solicitudes de recuperación.](#)

Enviar solicitudes de recuperación

Puede ver y administrar implementaciones, así como enviar solicitudes de recuperación a los propietarios de la implementación. En una solicitud de recuperación se especifica la duración de la nueva concesión en días, el tiempo que tiene el propietario de la implementación para responder y las máquinas que son objeto de la recuperación.

Requisitos previos

- Inicie sesión en vRealize Automation como **administrador de tenants**.
- (opcional) Para ver los distintivos de estado o las métricas proporcionadas por vRealize Operations Manager, consulte [Configurar un proveedor de métricas](#).

Procedimiento

- 1 Seleccione **Administración > Recuperación > Implementaciones**.

2 Encuentre las implementaciones de máquina virtual que coinciden con sus criterios de búsqueda.

Debe seleccionar el tipo de plataforma vSphere para ver las métricas proporcionadas por vRealize Operations Manager.

- Haga clic en la flecha hacia abajo de **Búsqueda avanzada** para abrir el cuadro de búsqueda.
- Escriba o seleccione uno o más valores de búsqueda.

Opción	Acción
El nombre de la máquina virtual contiene	Escriba uno o varios caracteres en el cuadro de texto para buscar los nombres de máquina virtual coincidentes.
El nombre del propietario contiene	Escriba un nombre en el cuadro de texto para buscar los nombres de propietario coincidentes.
El nombre del grupo empresarial contiene	Escriba un nombre en el cuadro de texto para buscar los nombres de grupo empresarial coincidentes.
Tipo de plataforma	<p>Seleccione un tipo de plataforma en el menú desplegable. Seleccione vSphere para ver las métricas proporcionadas por vRealize Operations Manager.</p> <p>Obligatorio para vRealize Operations Manager.</p>
Estado de energía	Seleccione un valor de estado de energía en el menú desplegable para buscar las máquinas virtuales con un estado de energía coincidente.
Fecha de caducidad entre	Haga clic en los iconos de calendario y seleccione una fecha inicial y una fecha final para buscar fechas de caducidad dentro del rango.
Uso de CPU	<p>Seleccione un valor en el menú desplegable para buscar máquinas virtuales con uso alto de CPU (superior al 80%), uso bajo de CPU (inferior al 5%) o ninguno (sin valor).</p> <p>Si realiza consultas de métricas de vRealize Operations Manager, no puede utilizar este filtro en las consultas ni puede ordenar los resultados por uso de CPU.</p>
Uso de memoria	<p>Seleccione un valor del menú desplegable para buscar máquinas virtuales con uso alto de memoria (superior al 80%), uso bajo de memoria (inferior al 10%) o ninguno (sin valor).</p> <p>Si realiza consultas de métricas de vRealize Operations Manager, no puede utilizar este filtro en las consultas ni puede ordenar los resultados por uso de memoria.</p>
Uso de disco	<p>Seleccione un valor del menú desplegable para buscar máquinas virtuales con uso bajo de disco duro (menos de 2 KB/s) o ninguno (sin valor).</p> <p>Si realiza consultas de métricas de vRealize Operations Manager, no puede utilizar este filtro en las consultas ni puede ordenar los resultados por uso de disco.</p>
Uso de la red	Seleccione un valor en el menú desplegable para buscar máquinas virtuales con uso bajo de red (menos de 1 KB/s) o ninguno (sin valor).

Opción	Acción
	Si realiza consultas de métricas de vRealize Operations Manager, no puede utilizar este filtro en las consultas ni puede ordenar los resultados por uso de red.
Métrica compleja	<p>Seleccione un valor en el menú desplegable para buscar máquinas virtuales en función de métricas complejas. Por ejemplo, seleccione Inactivo para buscar máquinas cuyos valores de uso de CPU, red, memoria y disco estén por debajo del 20%.</p> <p>No puede utilizar este filtro en consultas de métricas de vRealize Operations Manager.</p>

c Haga clic en el icono de búsqueda (.

- 3 En la página Implementaciones, seleccione una o varias máquinas cuya implementación principal desea recuperar.

Solo se recuperan las máquinas seleccionadas que son visibles en la página de resultados actual.

- 4 Haga clic en **Recuperar**.

En la solicitud se incluyen las implementaciones que contienen máquinas virtuales que están seleccionadas en la página actual.

Nota En la página Recuperar implementación también pueden aparecer máquinas que no se pueden recuperar (por ejemplo, máquinas cuya concesión ha caducado). Si especifica una máquina que no está disponible para la recuperación, recibirá el siguiente error:

```
Selection Error: Virtual machine name is not in valid state for reclamation.
```

- 5 Especifique la duración de la nueva concesión en el cuadro de texto **Duración de la nueva concesión (días)**.

El valor mínimo es 1 día, el máximo 365 días y el predeterminado es 7 días.

- 6 En el cuadro de texto **Esperar antes de forzar la concesión (días)** especifique la cantidad de días que tiene el propietario de la implementación para responder a la solicitud de recuperación.

Una vez que se cumpla el plazo, la implementación obtendrá una nueva concesión con la duración de la nueva concesión. El período mínimo de espera es 1 día, el máximo es 365 días y el predeterminado es 3 días.

- 7 Escriba un motivo de la solicitud en el cuadro de texto **Motivo de la solicitud**.

- 8 Haga clic en **Enviar**.

- 9 Haga clic en **Aceptar**.

Resultados

Cuando se envía una solicitud de recuperación, esta aparece en la bandeja de entrada del propietario de la implementación. Si el propietario no responde a la solicitud dentro del número de días requerido, la implementación obtiene una nueva concesión con la duración especificada, a menos que su concesión actual sea más corta. Si el propietario hace clic en **Elemento en uso** en la solicitud de recuperación, la concesión de la implementación no se modifica. Si el propietario hace clic en **Liberar para la recuperación**, la concesión de la implementación caduca de inmediato.

Pasos siguientes

[Realizar un seguimiento de las solicitudes de recuperación.](#)

Realizar un seguimiento de las solicitudes de recuperación

Puede realizar un seguimiento del estado actual de las solicitudes de recuperación y otros detalles.

Se pueden utilizar los siguientes métodos alternativos para comprobar una solicitud de recuperación reciente:

- Haga clic en la pestaña **Bandeja de entrada** y seleccione **Solicitudes de recuperación** para ver la información de las solicitudes de recuperación.
- Haga clic en la pestaña **Solicitudes de recuperación** y vea la lista de solicitudes recientes.
- Haga clic en la pestaña **Elementos** y seleccione **Implementaciones** para ver los cambios de implementaciones más recientes.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tenants**.


Procedimiento

- 1 Seleccione **Administración > Recuperación > Solicitudes de recuperación**.

2 Encuentre las máquinas virtuales que coincidan con sus criterios de búsqueda.

- Haga clic en la flecha hacia abajo de **Búsqueda avanzada** para abrir el cuadro de búsqueda.
- Escriba o seleccione uno o más valores de búsqueda.

Opción	Acción
El nombre de la máquina virtual contiene	Escriba uno o varios caracteres en el cuadro de texto para buscar los nombres de máquina virtual coincidentes.
El nombre del propietario contiene	Escriba uno o varios caracteres en el cuadro de texto para buscar los nombres de propietario coincidentes.
El motivo de la solicitud contiene	Escriba uno o varios caracteres en el cuadro de texto para buscar un motivo de la solicitud coincidente.
Estado de la solicitud	Seleccione un valor de estado de la solicitud en el menú desplegable para buscar las máquinas virtuales con un estado de la solicitud coincidente.

- Haga clic en el icono **Buscar** () o pulse Entrar para iniciar la búsqueda.
- Haga clic en la flecha hacia arriba de **Búsqueda avanzada** para cerrar el cuadro de búsqueda.

3 (opcional) Haga clic en **Actualizar datos** para actualizar la visualización de las solicitudes de reclamación.

Cambiar la reserva de una máquina administrada

Puede cambiar la configuración de almacenamiento o reserva de una máquina administrada. Esto resulta útil cuando una máquina se mueve a una nueva ruta de almacenamiento que no está disponible en su reserva actual. Para una implementación de una sola máquina, también puede cambiar el grupo empresarial de la máquina.

Puede trasladar una máquina de una implementación con una sola máquina a otro grupo empresarial si el propietario de la máquina es miembro del grupo empresarial de destino. Para cambiar la configuración del grupo empresarial, debe ser administrador de los grupos empresariales de origen y de destino.

Nota Si hay una política de reserva asignada a la máquina, no puede cambiar su grupo empresarial.

Puede crear reservas adicionales para el recurso informático asociado mediante las opciones de menú **Administración > Recurso informático**.

El almacenamiento y la memoria que se asignan a una máquina aprovisionada por una reserva se liberan cuando se elimina en vRealize Automation la máquina a la que están asignados, mediante la acción Destruir. El almacenamiento y la memoria no se liberan si la máquina se elimina en vCenter Server.

Por ejemplo, no puede eliminar una reserva que esté asociada con máquinas en una implementación existente. Si mueve o elimina de forma manual máquinas implementadas en vCenter Server, vRealize Automation las sigue reconociendo como activas y le impide eliminar las reservas asociadas.

Si el cambio de la reserva supone el traslado de una máquina en vCenter Server a una nueva ruta de almacenamiento que no forma parte de la reserva de dicha máquina en vRealize Automation, compruebe que la ruta de almacenamiento de destino o la nueva estén seleccionadas en la reserva de destino de la máquina antes de cambiar la reserva de la máquina.

Requisitos previos

Inicie sesión en vRealize Automation como **administrador de tejido**.

Procedimiento

- 1 Seleccione **Infraestructura > Máquinas administradas**.
- 2 Localice la máquina con la reserva que se desea cambiar.
- 3 Haga clic en **Cambiar reserva** en el menú desplegable.
Puede ver información acerca de la máquina administrada (como el recurso informático y el blueprint asociados) haciendo clic en la opción **Ver** del menú desplegable.
- 4 (opcional) Seleccione un grupo empresarial en el menú desplegable **Grupo empresarial**.
- 5 (opcional) Seleccione una reserva del menú desplegable **Reserva**.
- 6 (opcional) Seleccione una política de almacenamiento del menú desplegable **Almacenamiento**.
- 7 Haga clic en **Aceptar**.

Cómo funciona la acción Reanudar

Puede utilizar Reanudar en las implementaciones con errores para reiniciar el proceso de aprovisionamiento desde el punto de error y en determinadas circunstancias. Cuando se habilita, la acción Reanudar queda disponible para las solicitudes de aprovisionamiento con errores o las acciones aplicables.

Para utilizar la reanudación en las solicitudes de aprovisionamiento, debe añadir la propiedad personalizada `_debug_deployment = true` al blueprint. De forma predeterminada, las implementaciones con errores se revierten y se borran para poder recuperar los recursos. La propiedad `_debug_deployment = true` mantiene la implementación en el punto de error y, en función de la compatibilidad y el funcionamiento, permite una acción Reanudar. Si solo se utiliza Reanudar en las acciones compatibles, no es necesario habilitar la propiedad `_debug_deployment`.

Para obtener más información sobre `_debug_deployment`, consulte *Referencia de propiedades personalizadas*.

Para utilizar Reanudar en una solicitud de aprovisionamiento o en las acciones disponibles, autorice a los usuarios para la acción Reanudar. Consulte [Autorizar usuarios a servicios, elementos de catálogo y acciones](#).

Puede autorizar a los usuarios para la acción Reanudar en estas actividades de aprovisionamiento.

- Solicitudes de aprovisionamiento
- Acción Reanudar
- Acción Escalado vertical
- Acción Escalado horizontal
- Acción Destruir

Restricciones de la acción Reanudar

Al decidir si puede usar Reanudar en lugar de solicitar una nueva instancia de un blueprint, tenga en cuenta las restricciones.

- El blueprint no se puede modificar desde el momento de la solicitud.

En el momento de la solicitud, se asocia una versión no modificable del blueprint a la solicitud de catálogo. Esta versión estática contiene todas las especificaciones, incluidos atributos, propiedades personalizadas, opciones de configuración y otros elementos, que existían cuando se inició el aprovisionamiento. Si existe un error productor de fallo en el blueprint, corregir el error y, a continuación, usar Reanudar no funciona debido a que estas acciones hacen referencia a la versión asociada a la solicitud. En este escenario, se debe aprovisionar una nueva instancia.

Ejemplos

- El blueprint A solicita 5 GB de RAM, pero se produce un error en la solicitud debido a que las reservas solo llegan a 3 GB. Si se actualiza el blueprint para necesitar solo 3 GB y, a continuación, se ejecuta Reanudar, se produce un error en la acción Reanudar. Cuando se ejecuta Reanudar, se comprueba la solicitud original y se siguen buscando los 5 GB. Sin embargo, si se aumenta la reserva del sistema para el grupo empresarial a 5 GB y se ejecuta Reanudar, la acción Reanudar se ejecuta correctamente.
- Cuando se solicita el blueprint B, el que incluye una especificación de personalización de invitado, se produce un error. La investigación revela que se cambió el nombre de la especificación de personalización de invitado en la instancia de vCenter Server. Si se actualiza el blueprint con el nuevo nombre y se ejecuta Reanudar, se produce un error. Se actualizó el blueprint, pero se utilizó la versión original para la acción Reanudar. Si el nuevo nombre es el que se desea utilizar en el futuro, se debe implementar una nueva instancia del blueprint en lugar de usar Reanudar. De lo contrario, se debe cambiar el nombre de la especificación de personalización de invitado en la instancia de vCenter Server de vuelta al esperado por la versión original y ejecutar Reanudar. Si no desea que la próxima solicitud de aprovisionamiento genere un error, no olvide actualizar el blueprint con la especificación de personalización de invitado correcta.

Reanudar funciona si se puede actualizar el entorno de implementación de destino para admitir las especificaciones de blueprint existentes en el momento de la solicitud.

- Volver a intentar solo se ejecuta desde el punto de error.

La acción Reanudar vuelve a intentar las tareas del componente desde el punto de error. No vuelve a enviar la solicitud de aprovisionamiento completa.

Ejemplos

- El blueprint C crea una máquina virtual de aplicación y una máquina virtual de base de datos. La máquina virtual de base de datos se implementa correctamente, pero se produce un error en el aprovisionamiento en la máquina virtual de aplicación. Si se ejecuta la acción Reanudar, solo se vuelve a intentar el aprovisionamiento de la máquina virtual de aplicación.

Si se marca un componente como Fallido, se lo trata como si nunca se hubiera ejecutado. Si se produce un error en la instalación durante la fase de configuración en la máquina virtual de base de datos, por ejemplo, debido a un error de creación de scripts, pero la base de datos está intacta, esta sigue existiendo cuando se ejecuta el script durante una acción Reanudar. El script de instalación, que incluye el script de configuración, no se vuelve a ejecutar. La reanudación no se realizó correctamente. Debe corregir el script y aprovisionar una nueva instancia.

- Otra variación que se debe tener en cuenta es si la asignación de paso se realizó correctamente, pero se produjo un error en el aprovisionamiento. En este ejemplo, al reanudar, cuando se vuelve a intentar desde el punto de aprovisionamiento con errores, la solicitud de reanudación procesa información de asignación obsoleta y se produce un error en la reanudación.

Crear un snapshot en la máquina

Según el modo en que los administradores hayan configurado el entorno, se puede crear un snapshot de su máquina virtual. Un snapshot es una imagen de una máquina virtual realizado en un momento concreto. Se trata de una copia de la imagen de máquina virtual original que hace un uso eficaz del espacio. Los snapshots constituyen un modo sencillo de recuperar un sistema de algún daño, pérdida de datos o amenaza de seguridad. Después de crear un snapshot de la máquina virtual, se puede aplicar y restablecer el sistema de vuelta al punto en el que dicho snapshot se tomó.

Al crear un snapshot de memoria, dicho snapshot captura el estado de la configuración de encendido de la máquina virtual y, opcionalmente, la memoria de esa máquina virtual. Cuando se captura el estado de memoria de la máquina virtual, la operación de snapshot tarda más en completarse. También percibirá un fallo puntual en la respuesta a través de la red.

Requisitos previos

- Hay una máquina virtual encendida, apagada o suspendida.

- Si la máquina virtual está configurada para uno o varios discos independientes, apáguela antes de crear el snapshot. Si está encendida, el snapshot no se podrá crear. Para obtener información sobre la configuración de disco, consulte la *tabla de propiedades personalizadas por V*.
- El administrador de tenants o el administrador de grupo empresarial le autorizó para la acción de snapshot.

Procedimiento

1 Seleccione **Elementos > Máquinas**.

También puede seleccionar **Elementos > Implementación** e ir a la máquina en la implementación.

2 Localice la máquina de la que quiera crear el snapshot.

3 En la columna Acciones, haga clic en la flecha abajo y en **Ver detalles**.

4 Haga clic en **Crear snapshot** en el menú Acciones.

5 Especifique un nombre y, opcionalmente, una descripción.

6 Si quiere capturar la configuración de energía y de la memoria de la máquina, seleccione **Incluir memoria**.

7 Haga clic en **Enviar**.

Conectarse a una máquina de forma remota

Puede conectarse a una máquina de forma remota desde la consola de vRealize Automation.

Requisitos previos

- Inicie sesión en vRealize Automation como **propietario de la máquina, administrador de tenants o administrador de grupo empresarial**.

- Compruebe que VMware Tools esté instalado.

VMware Tools debe estar instalado en el cliente de vRealize Automation para admitir el acceso totalmente funcional al conectar con VMware Remote Console. Si VMware Tools no está instalado, se producen errores, como que el puntero y las teclas del mouse no funcionan después de conectarse a la máquina de destino. Para obtener más información sobre las versiones compatibles de VMware Tools, consulte *Matriz de soporte de vRealize Automation*.

- Compruebe que la máquina aprovisionada esté encendida.

Procedimiento

1 Seleccione **Elementos > Implementación**.

2 Haga clic en **Acciones** en la fila del nombre de máquina o seleccione la máquina y haga clic en **Acciones** en la página de su máquina.

3 Seleccione el método de conexión remota.

- Seleccione **Conectar mediante RDP** para conectar utilizando RDP.
- Seleccione **Conectar con consola remota** para conectar mediante VMware Remote Console.

Responda a los avisos.

4 Haga clic en **Conectar** y siga las instrucciones para iniciar sesión en la máquina.

5 Cuando haya terminado, cierre la sesión y la ventana del navegador.

Configurar consolas remotas para vSphere con certificados SSL que no son de confianza

Si la implementación de vRealize Automation utiliza certificados que no son de confianza, antes de poder utilizar consolas remotas con VMware Remote Console, debe configurar el navegador del cliente para confiar en el certificado. Los pasos para hacerlo varían en función del navegador.

Si se ha configurado vRealize Automation con un certificado SSL de confianza para su entorno, VMware Remote Console no requerirá ninguna configuración adicional en los navegadores de los clientes. Cuando un certificado de dispositivo de vRealize Automation se reemplaza y es un certificado de confianza, no es necesario actualizar la información de certificado para el cliente del navegador web.

Si desea reemplazar el certificado, consulte el tema relativo a la sustitución de un certificado Dispositivo de vRealize Automation en la guía de *Administración del sistema* de vRealize Automation.

Las conexiones remotas que utilizan VMware Remote Console para las máquinas aprovisionadas en vSphere están protegidas por certificados de dispositivo de vRealize Automation a través de una consola proxy. VMware Remote Console requiere que se admitan WebSockets en el navegador y los navegadores deben confiar en los certificados de dispositivo de vRealize Automation. Para obtener el certificado vaya al dispositivo virtual de nivel raíz en una dirección con la convención `https://vra-vb.eng.mycompany.com/`.

Para obtener información sobre los requisitos de compatibilidad con navegadores y vSphere, consulte el *Matriz de soporte de vRealize Automation*.

Configurar Firefox para que confíe en un certificado de vRealize Automation

Los certificados del dispositivo de vRealize Automation que no son de confianza deben importarse manualmente en los navegadores de los clientes para poder admitir VMware Remote Console en los clientes aprovisionados en vSphere.

Para obtener información sobre las versiones compatibles de Firefox, consulte la *matriz de soporte de VMware vRealize* en el [Centro de información](#) de vRealize Automation.

Nota Si se ha configurado vRealize Automation con un certificado SSL de confianza para su entorno, VMware Remote Console no requerirá ninguna configuración adicional en los navegadores de los clientes.

Procedimiento

- 1 En un navegador Firefox, inicie sesión en el dispositivo de vRealize Automation.
Aparecerá un mensaje indicando que el certificado no es de confianza.
- 2 Seleccione **Menú Abrir > Opciones**.
- 3 Haga clic en **Privacidad y seguridad** y, a continuación, en **Ver certificados**.
- 4 En el cuadro de diálogo Administrador de certificados, haga clic en **Servidores** y, a continuación, en **Agregar excepción**.
- 5 Agregue la URL del dispositivo de vRealize Automation con el puerto 8444.
Por ejemplo, `https://your-vra-fqdn-domain:8444`.
- 6 Haga clic en **Obtener certificado** y, a continuación, en **Confirmar excepción de seguridad**.
- 7 Haga clic en **Aceptar**.

Resultados

Ahora ya podrá conectarse a la consola remota sin errores de certificado.

Configurar Internet Explorer para que confíe en un certificado del dispositivo vRealize Automation

Los certificados del Dispositivo de vRealize Automation que no son de confianza deben importarse manualmente en los exploradores de los clientes para poder admitir VMware Remote Console en los clientes aprovisionados en vSphere.

Nota Si se ha configurado vRealize Automation con un certificado SSL de confianza para su entorno, VMware Remote Console no requerirá ninguna configuración adicional en los exploradores de los clientes.

Los pasos descritos en este procedimiento se aplican a certificados autofirmados y a certificados emitidos por una entidad de certificación.

Para obtener información acerca de las versiones de Internet Explorer admitidas, consulte la *matriz de soporte de VMware vRealize* en el sitio web de VMware.

Procedimiento

- 1 En Internet Explorer, inicie sesión en el Dispositivo de vRealize Automation.
- 2 Haga clic en **Ver certificado** en el mensaje de error del certificado que aparece en la barra de direcciones del explorador.
- 3 Haga clic en la pestaña **General** de la ventana Información del certificado.
- 4 Compruebe que la información del certificado es correcta y haga clic en **Instalar certificado**.
- 5 En el cuadro de diálogo Almacén de certificados, seleccione **Colocar todos los certificados en el siguiente almacén**.

- 6 Haga clic en **Examinar** para buscar el almacén de certificados.
- 7 Seleccione **Entidad de certificación raíz de confianza** y haga clic en **Aceptar**.
- 8 En el cuadro de diálogo Almacén de certificados, haga clic en **Siguiente**.
- 9 Haga clic en **Sí** en el cuadro de diálogo Advertencia de seguridad para instalar el certificado.
- 10 Reinicie el explorador.

Resultados

Ahora ya podrá conectarse a la consola remota sin errores de certificado.

Configurar Chrome para que confíe en un certificado del dispositivo de vRealize Automation

Los certificados del Dispositivo de vRealize Automation que no son de confianza deben importarse manualmente en los exploradores de los clientes para poder admitir VMware Remote Console en los clientes aprovisionados en vSphere.

Para obtener información sobre las versiones compatibles de Chrome, consulte la *Matriz de soporte de VMware vRealize* en el sitio web de VMware.

Nota Si se ha configurado vRealize Automation con un certificado SSL de confianza para su entorno, VMware Remote Console no requerirá ninguna configuración adicional en los exploradores de los clientes.

En Windows, Chrome e Internet Explorer comparten el mismo almacén de certificados. Esto significa que los certificados que son de confianza para Internet Explorer también lo son para Chrome. Para establecer certificados de confianza para Chrome, impórtelos a través de Internet Explorer. Para obtener información sobre este procedimiento, consulte [Configurar Internet Explorer para que confíe en un certificado del dispositivo vRealize Automation](#).

Cuando haya completado el procedimiento, reinicie Chrome.

Para confiar permanentemente en un certificado en el sistema operativo Macintosh, descargue el archivo del certificado e instale el certificado como de confianza en su herramienta de administración de certificados.

Procedimiento

- 1 En un explorador Chrome, inicie sesión en el Dispositivo de vRealize Automation.
- 2 Haga clic en el icono de la barra de direcciones.
- 3 Haga clic en el vínculo de información del certificado.
- 4 Arrastre el icono del certificado hasta el escritorio para guardar el certificado.
- 5 Inicie la aplicación Keychain Access.
- 6 Seleccione **File > Import Items**.

- 7 En la pantalla de Keychain Access, seleccione el archivo de certificado que guardó anteriormente.

Defina el valor de **Destination Key** en **System**.

- 8 Haga clic en **Open** para importar el certificado.
- 9 Reinicie el explorador.

Forzar la destrucción de una implementación tras una solicitud de destrucción fallida

Puede forzar la destrucción de una implementación que tenga un estado incoherente como resultado de una solicitud de destrucción fallida.

Cuando vRealize Automation no destruye un recurso de implementación durante una operación de destrucción de implementación, esa operación se detiene inmediatamente sin destruir el resto de recursos de la implementación. Este error deja la implementación en un estado incoherente, y se consumen recursos sin que se pueda destruir la implementación de forma obvia. Los administradores de grupos empresariales pueden forzar la destrucción de las implementaciones que estén en este estado incoherente.

Requisitos previos

- Confirme que ha iniciado sesión en vRealize Automation como un **administrador de grupo empresarial**.
- Antes de ejecutar la acción Forzar destrucción, revise la descripción de la acción Destruir en [Comandos del menú Acción en recursos aprovisionados](#).

Procedimiento

- 1 En la pestaña **Elementos**, haga clic en **Implementaciones** y seleccione la implementación que quiera destruir.
- 2 Haga clic en **Acciones** y, después, en **Destruir**.
- 3 Introduzca una descripción y un motivo de la solicitud.
- 4 Seleccione **Forzar destrucción** y haga clic en **Enviar**.

Resultados

vRealize Automation intenta destruir totalmente la implementación, incluidos todos los recursos que hay en ella. Si vRealize Automation no puede destruir un recurso de la implementación, lo omite y continúa destruyendo el resto de los recursos de la implementación.

Pasos siguientes

Haga clic en la pestaña **Solicitudes** y confirme que todos los recursos de la implementación se han destruido correctamente. Los recursos que no se hayan destruido durante una operación de destrucción forzada se deben destruir manualmente. Asegúrese también de que se destruyan los objetos de máquina virtual aprovisionados, ya que es posible que vRealize Automation intente reutilizar sus nombres de host, sus direcciones IP y otros detalles de configuración durante las operaciones de aprovisionamiento posteriores.

Solución de problemas de las acciones que faltan en el menú Acciones personalizadas

Como propietario de máquina o recurso, no visualiza todas las acciones autorizadas de un elemento aprovisionado.

Problema

En un entorno en el que sabe que una acción se autorizó para el usuario o grupo empresarial, espera ver todas las acciones cuando selecciona un elemento de la lista **Elementos**.

Causa

La disponibilidad de las acciones depende del tipo de recurso aprovisionado, del estado operativo del recurso, así como del modo en que se configuró y quedó disponible. En la siguiente lista se exponen algunos de los motivos por los que no visualiza todas las acciones configuradas.

- La acción no es aplicable debido al estado actual del recurso aprovisionado. Por ejemplo, Apagar solo está disponible cuando la máquina está encendida.
- La acción no se aplica al tipo de elemento seleccionado. Si el elemento no admite la acción, esta no aparece en la lista. Por ejemplo, la acción Crear snapshot no está disponible en una máquina física y la acción Conectar mediante RDP no estará disponible si el elemento seleccionado es una máquina Linux.
- La acción se aplica al tipo de recurso aprovisionado, pero la acción se desactiva en el Blueprint de la infraestructura. Si la acción está desactivada, nunca aparece como acción disponible en ninguno de los elementos que se aprovisionaron mediante el blueprint.
- La acción no está incluida en la autorización utilizada para aprovisionar el elemento en el que necesita ejecutar la acción. Solo las acciones autorizadas, bien como parte de un blueprint IaaS o como una acción personalizada de XaaS, pueden aparecer en el menú Acciones.
- La acción se crea como una acción personalizada de XaaS, pero no se incluye en la autorización utilizada para aprovisionar el elemento en el que necesita ejecutar la acción. Solo las acciones autorizadas aparecen en el menú Acciones.
- La acción puede ser limitada debido a los criterios de destino configurados para las acciones personalizadas de XaaS o las asignaciones de recursos a máquinas IaaS aprovisionadas.

Solución

- ◆ Compruebe que la acción sea aplicable al elemento aprovisionado o al estado del elemento aprovisionado.
- ◆ Compruebe que la acción esté configurada e incluida en la autorización utilizada para aprovisionar el elemento.

Solución de problemas de una implementación fallida que incluye un flujo de trabajo de vRealize Orchestrator

Si una implementación de blueprint fallida incluye un flujo de trabajo de vRealize Orchestrator, puede utilizar el ID de token para solucionar problemas con el flujo de trabajo. Utilice el ID de token para encontrar los logs en vRealize Orchestrator.

Solución

- 1 Busque el ID de token del flujo de trabajo fallido.
 - a En vRealize Automation, haga clic en la pestaña **Solicitar**.
 - b Haga clic en el número de la columna de solicitud.
La solicitud puede ser una implementación o una acción.
 - c Haga clic en la pestaña **General**.
Si el blueprint se basa en un flujo de trabajo de vRealize Orchestrator, el título de la página es Detalles de ejecución del flujo de trabajo de vRealize Orchestrator.
 - d Busque el ID de Token y cópielo en el portapapeles o en un archivo de texto.
Por ejemplo, ff8080815a685352015a6c8d450801ee.
- 2 Busque los logs de flujo de trabajo en vRealize Orchestrator mediante el Centro de control.
 - a Introduzca la dirección URL base para vRealize Automation en el cuadro de búsqueda del navegador.
Aparecerá la página del dispositivo de VMware vRealize Automation.
 - b Haga clic en **Centro de control de vRealize Orchestrator**.
 - c Inicie sesión como usuario con privilegios de raíz.
 - d Haga clic en **Inspeccionar los flujos de trabajo**.
 - e Haga clic en **Flujos de trabajo finalizados**.
 - f Pegue el token de flujo de trabajo en el cuadro de texto de ID de token.
La lista se muestra en el flujo de trabajo que coincide con el ID de token.
 - g Haga clic en la fila e inspeccione los logs para buscar la causa del error.

Especificar los ajustes de reconfiguración de máquinas y consideraciones de reconfiguración

Las plataformas vSphere, vCloud Air y vCloud Director admiten la reconfiguración de las máquinas existentes en una implementación para modificar ciertas especificaciones, como las de CPU, memoria y almacenamiento.

Las solicitudes de reconfiguración deben aprobarse en función de las autorizaciones, las políticas y las acciones habilitadas para el componente de máquina en el blueprint.

No es posible reconfigurar una máquina virtual que esté asignada a una red a petición. No se puede reconfigurar una NIC que esté conectada a una red a petición. Si intenta reconfigurar una red enrutada o NAT a petición, se muestra el error 'Original network [<network>] is not selected in the machine's reservation.', las redes de la máquina permanecen intactas y las direcciones IP de la máquina no se modifican.

Si está autorizado para realizar las acciones Cancelar reconfiguración (Máquina) y Ejecutar reconfiguración (Máquina), puede cancelar una reconfiguración o volver a intentar realizar una reconfiguración con errores.

No se admite la expansión de un disco en una máquina virtual que se haya aprovisionado a partir de un blueprint de clon vinculado.

No se pueden reconfigurar máquinas mediante los perfiles de componente Size o Image, pero el intervalo de CPU, memoria y almacenamiento que se calcula en función del perfil sigue disponible para las acciones de reconfiguración. Por ejemplo, si ha utilizado conjuntos de valores para Size pequeños (1 CPU, 1024 MB de memoria y 10 GB de almacenamiento) medianos (3 CPU, 2048 MB de memoria, 12 GB de almacenamiento) y grandes (5 CPU, 3072 MB de memoria, 15 GB de almacenamiento), los rangos disponibles durante la reconfiguración de máquina son 1-5 CPU, 1024-3072 MB de memoria y 1-15 GB de almacenamiento.

vRealize Automation crea una snapshot del blueprint en la implementación. Si tiene problemas de reconfiguración al actualizar las propiedades de la máquina, como la CPU y la RAM en una implementación, consulte el artículo de la base de conocimientos [2150829: Creación de snapshots de blueprint vRA 7.x](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **propietario de la máquina, usuario de soporte, usuario de grupo empresarial con función de acceso compartido o administrador de grupo empresarial**.
- La máquina que desea aprovisionar debe tener el estado Activada o Desactivada sin un estado de reconfiguración activo.
- El tipo de máquina debe ser vSphere, vCloud Air o vCloud Director a pesar de que la configuración de NSX se aplica solo a vSphere.
- Verifique si tiene autorización para reconfigurar una máquina.

Procedimiento**1** Seleccione **Elementos > Máquinas**.

También puede seleccionar **Elementos > Implementación** e ir a la máquina en la implementación.

2 Seleccione la máquina que desea reconfigurar.**3** Seleccione **Reconfigurar** en el menú desplegable **Acciones**.**4** Seleccione la pestaña correspondiente a la opción que desea reconfigurar.**Tabla 3-80. Solicitar cambios de reconfiguración**

Pestaña	Tema
General	Reconfigurar las CPU y la memoria
Almacenamiento	Editar la configuración de almacenamiento
Red	Cambiar la configuración de red Para cambiar las reglas NAT, consulte Cambiar las reglas NAT en una implementación .
Seguridad	Para reconfigurar las opciones de seguridad, consulte Agregar o quitar elementos de seguridad en una implementación .
Propiedades	Cambiar la configuración del grupo de propiedades y propiedades personalizadas

Pasos siguientes

[Ejecutar la reconfiguración de máquina solicitada](#) .

Reconfigurar las CPU y la memoria

Puede cambiar el número de CPU o la cantidad de memoria y almacenamiento que usa la máquina aprovisionada, siempre dentro de los límites establecidos por el blueprint de aprovisionamiento.

Para implementaciones aprovisionadas de Amazon, puede volver a configurar todos los volúmenes de almacenamiento de la implementación, a excepción del volumen raíz.

No se admite la expansión de un disco en una máquina virtual que se haya aprovisionado a partir de un blueprint de clon vinculado.

Requisitos previos

[Especificar los ajustes de reconfiguración de máquinas y consideraciones de reconfiguración](#).

Procedimiento

- 1 Haga clic en la pestaña **General**.
- 2 Introduzca el número de CPU en el cuadro de texto **CPU**.
- 3 Introduzca la cantidad de memoria en el cuadro de texto **Memoria (MB)**.
- 4 Introduzca la cantidad de almacenamiento en el cuadro de texto **Almacenamiento (GB)**.

Pasos siguientes

Especifique la configuración adicional de la reconfiguración de máquina. Si ha terminado de cambiar la configuración de la máquina, inicie la solicitud para su reconfiguración. Consulte [Ejecutar la reconfiguración de máquina solicitada](#) .

Editar la configuración de almacenamiento

Puede añadir, eliminar o cambiar el tamaño de un volumen de almacenamiento en una máquina virtual aprovisionada.

No se puede reconfigurar el almacenamiento del tipo de disco IDE.

El almacenamiento y la memoria que se asignan a una máquina aprovisionada por una reserva se liberan cuando se elimina en vRealize Automation la máquina a la que están asignados, mediante la acción Destruir. El almacenamiento y la memoria no se liberan si la máquina se elimina en vCenter Server.

Por ejemplo, no puede eliminar una reserva que esté asociada con máquinas en una implementación existente. Si mueve o elimina de forma manual máquinas implementadas en vCenter Server, vRealize Automation las sigue reconociendo como activas y le impide eliminar las reservas asociadas.


Requisitos previos

[Especificar los ajustes de reconfiguración de máquinas y consideraciones de reconfiguración.](#)


Para implementaciones aprovisionadas de Amazon, puede volver a configurar todos los volúmenes de almacenamiento de la implementación, a excepción del volumen raíz.

Procedimiento

- 1 Haga clic en la pestaña **Almacenamiento**.
El intervalo permitido del almacenamiento aparecerá bajo la tabla Volúmenes de almacenamiento.
- 2 Añada o edite la configuración de volumen de almacenamiento disponible.
 - a Haga clic en **Nuevo volumen**.
 - b Escriba la capacidad en el cuadro de texto **Capacidad (GB)**.

- c Seleccione una política de reserva de almacenamiento en el menú desplegable **Política de reserva de almacenamiento**.
- d Haga clic en el icono **Guardar** ()



3 Elimine un volumen.

- a Encuentre el volumen.
- b Haga clic en el icono **Eliminar** ()

Un icono que no se puede seleccionar indica que es un volumen que no se puede eliminar, como el de un clon vinculado.

4 Aumente el tamaño de un volumen.

No puede reducir el tamaño de los volúmenes existentes. El tamaño de un volumen está limitado por la cantidad total de almacenamiento especificada en el blueprint, menos la cantidad asignada a otros volúmenes.

- a Encuentre el volumen.
- b Haga clic en el icono **Editar** ()
- c Escriba el tamaño nuevo en el cuadro de texto **Capacidad (GB)**.
- d Haga clic en el icono **Guardar** ()

Pasos siguientes

Especifique la configuración adicional de la reconfiguración de máquina. Si ha terminado de cambiar la configuración de la máquina, inicie la solicitud para su reconfiguración. Consulte [Ejecutar la reconfiguración de máquina solicitada](#) .

Cambiar la configuración de red

Puede añadir, eliminar o editar un adaptador de red.

Puede cambiar la siguiente configuración de red durante el proceso de reconfiguración de máquinas:

- Añada o quite NIC.
- Asigne o libere direcciones IP para las NIC existentes.
- Asigne nuevas direcciones IP a las NIC, siempre que la red no sea una NAT a petición o una red con enrutamiento a petición.

No se pueden reconfigurar una red NAT a petición o una red con enrutamiento a petición.

La reconfiguración de la red requiere que se seleccionen las redes de origen y de destino en la reserva.

Cuando se añaden varias NIC, se asignan direcciones IP. Al quitar las NIC, se liberan las direcciones IP.

Después de cambiar la configuración de una red en función de la información de perfil de red y reserva, se asigna la nueva IP de red en vRealize Automation, pero la máquina implementada no se actualiza en el endpoint con la información de la nueva IP. Debe asignar la IP manualmente a la máquina una vez que termine el proceso de reconfiguración.



No es posible reconfigurar una máquina virtual que esté asignada a una red a petición. No se puede reconfigurar una NIC que esté conectada a una red a petición. Si intenta reconfigurar una red enrutada o NAT a petición, se muestra el error 'Original network [<network>] is not selected in the machine's reservation.', las redes de la máquina permanecen intactas y las direcciones IP de la máquina no se modifican.



No se permite cambiar la configuración de red de NSX en las implementaciones que se han actualizado o migrado de vRealize Automation 6.2.x a esta versión de vRealize Automation.

Requisitos previos

[Especificar los ajustes de reconfiguración de máquinas y consideraciones de reconfiguración.](#)

Procedimiento

- 1 Haga clic en la pestaña **Red**.
- 2 (opcional) Añada un adaptador de red.
 - a Haga clic en **Nuevo adaptador de red**.
 - b Seleccione una red en el menú desplegable **Nombre de red**.
Todas las redes seleccionadas en la reserva de la máquina están disponibles.
 - c Escriba una dirección IP estática para la red en el cuadro de texto **Dirección**.
La dirección IP no debe estar asignada en el perfil de red asignado de la reserva.
 - d Haga clic en el icono **Guardar** (.
- 3 (opcional) Elimine un adaptador de red.
 - a Encuentre el adaptador de red.
 - b Haga clic en el icono **Eliminar** (.

No se puede eliminar el adaptador de red 0.
- 4 (opcional) Edite un adaptador de red.
 - a Encuentre el adaptador de red.
 - b Haga clic en el icono **Editar** (.
 - c Seleccione una red en el menú desplegable **Nombre de red**.
 - d Haga clic en el icono **Guardar** (.

Pasos siguientes

Especifique la configuración adicional de la reconfiguración de máquina. Si ha terminado de cambiar la configuración de la máquina, inicie la solicitud para su reconfiguración. Consulte [Ejecutar la reconfiguración de máquina solicitada](#).

Cambiar la configuración del grupo de propiedades y propiedades personalizadas

Las propiedades personalizadas de la máquina implementada se pueden editar, añadir o eliminar.

No puede usar propiedades personalizadas para introducir valores de número de disco, capacidad, etiqueta o política de reserva de almacenamiento del volumen. Para introducirlos, debe agregar o editar un volumen en la tabla de volúmenes de almacenamiento. Consulte [Editar la configuración de almacenamiento](#).

Requisitos previos

[Especificar los ajustes de reconfiguración de máquinas y consideraciones de reconfiguración.](#)

Procedimiento

- 1** Haga clic en la pestaña **Propiedades**.
- 2** Para añadir una propiedad, haga clic en **Nueva propiedad**.
- 3** Escriba el nombre de la propiedad en el cuadro de texto **Nombre**.
- 4** Escriba el valor de la propiedad en el cuadro de texto **Valor**.
- 5** Active la casilla de verificación **Cifrado** para cifrar el valor.
- 6** Active la casilla de verificación **Preguntar al usuario** para consultar a los usuarios acerca del valor cuando soliciten la máquina.
- 7** Añada otra propiedad, edite una propiedad existente o elimine una propiedad.

Pasos siguientes

Especifique la configuración adicional de la reconfiguración de máquina. Si ha terminado de cambiar la configuración de la máquina, inicie la solicitud para su reconfiguración. Consulte [Ejecutar la reconfiguración de máquina solicitada](#).

Ejecutar la reconfiguración de máquina solicitada

Puede iniciar la reconfiguración inmediatamente o programarla para que se inicie en una fecha y a una hora en particular. También puede especificar la opción de encendido de la máquina antes de reconfigurarla.

Requisitos previos

[Especificar los ajustes de reconfiguración de máquinas y consideraciones de reconfiguración.](#)

Procedimiento

- 1 Si la pestaña **Ejecución** está visible, puede seleccionarla para especificar opciones de reconfiguración adicionales. Si no está visible, haga clic en **Enviar** para iniciar la reconfiguración de máquinas.
- 2 Si la pestaña **Ejecución** está visible, haga clic en **Ejecución** para programar la acción de reconfiguración.
- 3 (opcional) Seleccione una opción en el menú desplegable **Ejecutar solicitud**.

Opción	Descripción
Urgente	Inicia la reconfiguración tan pronto como sea posible tras la aprobación.
Programada	Inicia la reconfiguración en la fecha y a la hora especificadas. Escriba la fecha y la hora en los cuadros de texto que se muestran.

La hora programada es la hora local de la ubicación del servidor web de vRealize Automation. Si **Ejecutar solicitud** no está disponible, la reconfiguración de iniciará de forma inmediata.

- 4 (opcional) Seleccione una acción de energía en el menú desplegable **Acción de energía**.

Opción	Descripción
Reiniciar si es necesario	(Predeterminado) Si es necesario, reinicie la máquina antes de reconfigurarla.
Reiniciar	Reinicie la máquina antes de reconfigurarla, independientemente de si se requiere un reinicio.
No reiniciar	No reinicie el equipo antes de volver a configurarlo, incluso si se requiere un reinicio.

Las siguientes condiciones requieren que la máquina se reinicie antes de la reconfiguración:

- Cambio de CPU donde la adición en caliente no es compatible o no está activada.
- Cambio de memoria donde la memoria en caliente no es compatible o no está activada.
- Cambio de almacenamiento donde el almacenamiento en caliente está desactivado.

Si la máquina se encuentra en estado de apagado, no se reinicia.

Nota Puede desactivar la opción de adición en caliente de vSphere mediante la propiedad personalizada `VirtualMachine.Reconfigure.DisableHotCpu`.

- 5 Haga clic en **Aceptar**.

Pasos siguientes

Puede supervisar el progreso de la reconfiguración observando los estados del flujo de trabajo que se muestran en la interfaz de usuario. Consulte [Estado de flujo de trabajo de las operaciones de reconfiguración](#).

Estado de flujo de trabajo de las operaciones de reconfiguración

Cuando se inicia la reconfiguración, y a medida que progresa a través del flujo de trabajo, puede supervisar el progreso en la página Editar.

Tabla 3-81. Estado de flujo de trabajo de las operaciones de reconfiguración

Estado	Descripción
Pendiente de reconfiguración	Se ha creado el estado de la operación.
Programada	Se ha creado un flujo de trabajo programado para Distributed Execution Manager (DEM).
Reconfiguración	Se está ejecutando el flujo de trabajo específico de la interfaz.
Error de reconfiguración; esperando para reintentar	Se ha producido un error de reconfiguración y se está esperando a que el propietario solicite que se vuelva a intentar. Si el propietario de la máquina tiene autorización para las acciones de reconfiguración y de cancelación de reconfiguración, podrá volver a intentar la reconfiguración o cancelarla.
Error de reconfiguración	Se ha producido un error de reconfiguración y se está esperando a que el flujo de trabajo lleve a cabo la siguiente acción.
Reconfiguración correcta	La reconfiguración se ha completado correctamente y se está esperando a que el flujo de trabajo lleve a cabo la siguiente acción.
Cancelada	El usuario ha cancelado la reconfiguración. Los propietarios de máquinas que tienen autorización pueden cancelar una reconfiguración.
Completada	El flujo de trabajo de finalización establece este estado tras completar la limpieza, de modo que el flujo de trabajo pueda limpiar las operaciones de estado y las aprobaciones. El estado Completada indica que la solicitud de vRealize Automation ha finalizado, pero no significa que la reconfiguración de la máquina se haya completado correctamente.

Reconfigurar un equilibrador de carga en una implementación

Puede añadir, editar o eliminar un servidor virtual en un equilibrador de carga de NSX implementado.

Las siguientes consideraciones se aplican a las implementaciones que se hayan originado en vRealize Automation 7.2 o una versión anterior:

- La reconfiguración del equilibrador de carga se limita a las implementaciones que contienen un equilibrador de carga único.
- La página de detalles de elementos para cualquier equilibrador de carga en una implementación muestra los servidores virtuales que se utilizan en todos los equilibradores de carga en la implementación. Para obtener más información, consulte el [artículo 2150276 de la Base de conocimientos](#).
- No se admite la operación de reconfiguración del equilibrador de carga para implementaciones que se hayan actualizado o migrado desde vRealize Automation 6.2.x a esta versión de vRealize Automation.

Para los equilibradores de carga actualizados y los equilibradores de carga implementados en la versión actual de vRealize Automation, no edite un servidor virtual y agregue un servidor virtual en la misma solicitud. Para obtener más información, consulte el [artículo 2150240 de la Base de conocimientos](#).

Si envía una solicitud para reconfigurar un equilibrador de carga mientras se realiza otra acción en la implementación (por ejemplo, cuando una operación de escalado horizontal está en curso), se produce un error en la reconfiguración con un mensaje de soporte. En esta situación, puede esperar hasta que finalice la acción y, a continuación, puede enviar la solicitud de reconfiguración.

Nota Si el blueprint asociado a la implementación se importa desde un archivo YAML que contiene un equilibrador de carga a petición con un valor en el campo de nombre que sea diferente del valor en el campo de identificador, se produce un error en la acción **Reconfigurar**. Para habilitar la opción de reconfiguración del equilibrador de carga para una implementación que está basada en un blueprint importado, realice los siguientes pasos en el blueprint para permitir acciones posteriores al aprovisionamiento para los componentes del equilibrador de carga en futuras implementaciones.

- 1 En la consola de vRealize Automation, seleccione el blueprint.
- 2 Haga clic en **Editar** y cambie el nombre del blueprint. Esto permite establecer el nombre y el ID integrado con el mismo valor.
- 3 Seleccione el componente del equilibrador de carga en el blueprint.
- 4 Haga clic en **Editar** y vuelva a introducir el nombre del componente del componente. Esto permite establecer el nombre y el ID integrado con el mismo valor.
- 5 Repita para todos los componentes del equilibrador de carga en el blueprint.
- 6 Guarde el blueprint.

Al aprovisionar una nueva implementación mediante el blueprint modificado, la acción de reconfiguración del equilibrador de carga funcionará. Para evitar este problema, asegúrese de que todos los archivos YAML tienen los mismos valores de nombre e ID para todos los componentes de equilibrador de carga, red y seguridad antes de importarlos.

No debe administrar objetos NSX administrados por vRealize Automation fuera de vRealize Automation. Por ejemplo, si modifica el puerto de miembro de un equilibrador de carga de NSX implementado en NSX, en lugar de en vRealize Automation, la recopilación de datos de NSX rompe la asociación que existía entre la máquina implementada y el grupo de miembros de equilibradores de carga. Los resultados de las operaciones de escalado vertical y escalado horizontal tampoco se pueden prever cuando un puerto de miembro de equilibrador de carga se modifica fuera de vRealize Automation.

Para obtener más información sobre la configuración disponible al añadir o editar un servidor virtual, consulte [Añadir un componente de equilibrador de carga a petición](#).

Cuando se reconfigura un equilibrador de carga en vRealize Automation, algunas de las opciones que se configuraron en NSX y que no están disponibles como configuración en vRealize Automation se revierten a su valor predeterminado. Después de ejecutar la acción de reconfiguración del equilibrador de carga en vRealize Automation, verifique y actualice las siguientes opciones de configuración de NSX según sea necesario:

- Encabezado Insert-X-Forwarded for HTTP
- Dirección URL de redireccionamiento de HTTP
- Extensión del supervisor de servicios

Requisitos previos

- Inicie sesión en vRealize Automation como **propietario de la máquina, usuario de soporte, usuario de grupo empresarial con función de acceso compartido o administrador de grupo empresarial**.
- Verifique que tiene autorización para reconfigurar los equilibradores de carga en una implementación. La autorización de catálogo que se necesita es Reconfigurar (equilibrador de carga).

Procedimiento

- 1 Seleccione **Elementos > Implementación**.
- 2 Busque la implementación y muestre sus componentes de elementos secundarios.



- 3 Seleccione el equilibrador de carga de NSX que desea editar.



- 4 Seleccione **Reconfigurar** en el menú desplegable **Acciones**.
- 5 Añada, edite o quite servidores virtuales.

Virtual servers: + N... E... X Dele...

Protocol	Port	Description	Member Protocol	Member Port	Health Check Protocol	Health Check Port
HTTP	80		HTTP	80	HTTP	80
HTTP	81		HTTP	81	HTTP	81

- 6 Cuando termine de añadirlos, editarlos o eliminarlos, haga clic en **Enviar** para enviar la solicitud de reconfiguración.

Cambiar las reglas NAT en una implementación

Puede agregar, editar y eliminar reglas NAT de NSX existentes en una red NAT uno a muchos implementada.

También puede cambiar el orden en que las reglas NAT se procesan.

Nota Si el blueprint de origen de la implementación se importa desde un archivo YAML que contiene un componente de red NAT, y los valores de nombre e identificador de dicho componente no son idénticos, se produce un error en la acción **Cambiar reglas NAT**. Si desea permitir la acción **Cambiar reglas NAT** para una implementación basada en un blueprint importado, realice los pasos siguientes en el blueprint antes de aprovisionar una implementación.

- 1 Inicie vRealize Automation, haga clic en la pestaña Diseño y abra el blueprint.
- 2 Haga clic en **Editar** y cambie el nombre del blueprint. Esto permite establecer el nombre y el identificador integrado con el mismo valor.
- 3 Seleccione el componente de red NAT en el blueprint.
- 4 Haga clic en **Editar** y vuelva a introducir el nombre del componente del componente. Esto permite establecer el nombre y el identificador integrado con el mismo valor.
- 5 Repita para todos los componentes de red NAT en el blueprint.
- 6 Guarde el blueprint.

Para evitar este problema, asegúrese de que todos los archivos YAML tienen los mismos valores de nombre e identificador para todos los blueprints y componentes de equilibrador de carga, red y seguridad antes de importarlos.

Para obtener información relacionada, consulte [Crear y usar las reglas NAT](#) y [Añadir un componente de red enrutada a petición o red NAT a petición](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **propietario de la máquina, usuario de soporte, usuario de grupo empresarial con función de acceso compartido o administrador de grupo empresarial**.
- Confirme que tiene autorización para cambiar las reglas NAT de una red.
- Compruebe que la red NAT está configurada como una red NAT uno a muchos. Esta acción no es posible en redes NAT uno a uno.

Procedimiento

- 1 Seleccione **Elementos > Implementación**.
- 2 Busque la implementación y muestre sus componentes de elementos secundarios.



- 3 Seleccione el componente de red NAT que quiere editar.



El componente no se puede editar para una red NAT a petición asociada a un proveedor de IPAM de terceros. Sin embargo, se puede añadir manualmente una nueva dirección IP de destino. Cuando se añade una nueva dirección IP de destino, se anula el valor del componente. La nueva dirección IP de destino y el identificador nulo de máquina se procesan al enviar la solicitud de reconfiguración.

- 4 Haga clic en **Cambiar reglas NAT** en el menú **Acciones**.



- 5 Añada nuevas reglas de enrutamiento de puerto NAT o reordene, edite o elimine las ya existentes.
- 6 Cuando termine de realizar los cambios, haga clic en **Guardar** o en **Enviar** para enviar la solicitud de reconfiguración.

Agregar o quitar elementos de seguridad en una implementación

Es posible agregar o quitar etiquetas y grupos de seguridad de NSX existentes en una implementación de máquina. Los grupos de seguridad no se pueden añadir a petición, pero sí quitar.

La acción de cambio de la seguridad se basa en un clúster o un componente de la máquina. Por ejemplo, si la seguridad está asociada a un clúster denominado AppTier2 que consta de 2 máquinas, la operación de cambio de seguridad se debe realizar en el clúster AppTier2, no en cada máquina del clúster.

La operación Cambiar seguridad no se puede realizar en las implementaciones que se hayan actualizado o migrado desde vRealize Automation 6.2.x a esta versión de vRealize Automation.

Requisitos previos

- Inicie sesión en vRealize Automation como **propietario de la máquina, usuario de soporte, usuario de grupo empresarial con función de acceso compartido o administrador de grupo empresarial**.
- Compruebe que tiene autorización para cambiar la seguridad en una implementación. La autorización de catálogo que se necesita es Cambiar seguridad (implementación).

Procedimiento

- 1 Seleccione **Elementos > Implementación**.
- 2 Busque la implementación y muestre sus componentes de elementos secundarios.



- 3 En el menú **Acciones**, haga clic en **Cambiar seguridad**.



- 4 Seleccione el clúster o el componente de máquina implementado en el que desea agregar o quitar elementos de seguridad.



- 5 Agregue o quite grupos y etiquetas de seguridad existentes en cada clúster o componente de máquina de la implementación, según sea necesario.
- 6 Quite grupos de seguridad a petición en cada componente o clúster de máquina en la implementación, según convenga.
- 7 (opcional) Haga clic en la pestaña **Motivo** e introduzca una razón para la solicitud realizada.
- 8 Cuando termine de hacer cambios, haga clic en **Guardar** o haga clic en **Enviar** para enviar la solicitud de cambio.

Mostrar todas las reglas NAT de una instancia de NSX Edge existente

Puede mostrar información de las reglas NAT de las instancias de NSX Edge que se utilizan en las implementaciones activas.

Las reglas NAT se muestran en la vista de Edge como un añadido de todas las reglas NAT que se utilizan en la implementación. En la vista de Edge, las reglas no se muestran necesariamente en el orden en el que se procesan.

Para ver y, si lo desea, cambiar el orden en que las reglas NAT se procesan en una red NAT uno a muchos, consulte [Cambiar las reglas NAT en una implementación](#).

Requisitos previos

- Inicie sesión en vRealize Automation como **propietario de la máquina, usuario de soporte, usuario de grupo empresarial con función de acceso compartido o administrador de grupo empresarial**.

Procedimiento

- 1 Seleccione **Elementos > Implementación**.
- 2 Busque la implementación y muestre sus componentes de elementos secundarios.



- 3 Seleccione la instancia de NSX Edge que desea ver.



- 4 Haga clic en **Cerrar** cuando haya terminado.