

Configuración de vRealize Automation

vRealize Automation 7.2

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

ES-002290-05

vmware[®]

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

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

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

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

docfeedback@vmware.com

Copyright © 2015–2017 VMware, Inc. Todos los derechos reservados. [Copyright e información de marca registrada.](#)

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

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

Contenido

Configurar vRealize Automation 7

Información actualizada 9

1 Preparaciones externas para el aprovisionamiento 11

Preparar el entorno para la administración de vRealize Automation 11

Lista de comprobación para preparar la configuración de red y seguridad de NSX 12

Lista de comprobación para preparar la compatibilidad con proveedores de IPAM de terceros 16

Lista de comprobación para la configuración de Contenedores para vRealize Automation 18

Preparar el entorno de vCloud Director para vRealize Automation 19

Preparar el entorno de vCloud Air para vRealize Automation 20

Preparar el entorno de Amazon AWS 20

Preparar funciones de red y seguridad de Red Hat OpenStack 25

Preparar el entorno de SCVMM 26

Preparar el aprovisionamiento de máquinas 27

Elegir el método de aprovisionamiento de máquinas que se preparará 27

Lista de comprobación para ejecutar scripts de Visual Basic durante el aprovisionamiento 30

Usar el agente invitado de vRealize Automation durante el aprovisionamiento 31

Lista de comprobación para preparar el aprovisionamiento mediante clonación 38

Preparar el aprovisionamiento de vCloud Air y vCloud Director 52

Preparar el aprovisionamiento de Kickstart de Linux 53

Preparar el aprovisionamiento de SCCM 56

Preparar el aprovisionamiento de WIM 57

Preparar el aprovisionamiento de imágenes de máquina virtual 66

Preparar el aprovisionamiento de imágenes de máquina de Amazon 67

Escenario: Preparar recursos de vSphere para el aprovisionamiento de máquinas en Rainpole 69

Preparar el aprovisionamiento de Software 71

Preparar el aprovisionamiento de máquinas con Software 73

Escenario: Preparar una plantilla de CentOS de vSphere para los blueprints de componente de software y de máquina clonada 77

Escenario: Preparar la importación del blueprint de la aplicación de muestra Dukes Bank de vSphere 80

2 Configurar las opciones de tenant 85

Elegir opciones de configuración de Administración de directorios 86

Descripción de la administración de directorios 87

Usar Administración de directorios para crear un vínculo de Active Directory 90

Administrar atributos de usuario que se sincronizan desde Active Directory 107

Administración de conectores y clústeres de conectores 108

Unir una máquina de conector a un dominio 109

Acerca de la selección de controladoras de dominio 110

Administrar políticas de acceso 113

Integrar productos de autenticación de usuario alternativos con Administración de directorios	118
Actualizar conectores externos para Administración de directorios	137
Preparativos para actualizar un conector externo	137
Actualizar un conector externo en línea	138
Actualizar sin conexión un conector externo	139
Ajustar la configuración después de actualizar un conector externo	141
Solucionar problemas de actualización de conectores externos	142
Escenario: Configurar un vínculo de Active Directory para vRealize Automation de alta disponibilidad	144
Configurar la autenticación de tarjetas inteligentes para vRealize Automation	146
Generar un token de activación del conector	147
Implementar el archivo OVA del conector	147
Configurar los ajustes del conector	148
Aplicar la entidad de certificación pública	149
Crear un proveedor de identidades de área de trabajo	151
Configurar la autenticación mediante certificado y las reglas de la política de acceso predeterminada	151
Crear un vínculo de Active Directory con varios dominios o bosques	152
Configurar funciones de usuarios y grupos	154
Asignar funciones a usuarios o grupos de directorios	154
Crear un grupo personalizado	154
Crear un grupo empresarial	155
Solucionar problemas de rendimiento lento al mostrar miembros de grupos	157
Escenario: Configurar el tenant predeterminado para Rainpole	158
Escenario: Crear cuentas de usuario local para Rainpole	158
Escenario: Configurar su Active Directory corporativo para vRealize Automation para Rainpole	160
Escenario: Configurar personalización de marca para el tenant predeterminado para Rainpole	161
Escenario: Crear un grupo personalizado para los arquitectos de Rainpole	161
Escenario: Asignar privilegios de administrador de IaaS a su grupo personalizado de arquitectos de Rainpole	162
Crear tenants adicionales	163
Especificar la información de tenant	164
Configurar usuarios locales	164
Asignar administradores	165
Eliminar un tenant	165
Configurar la personalización de marca	166
Personalización de marca en la página de inicio de sesión de tenant	166
Personalización de marca en aplicaciones de tenant	167
Lista de comprobación para la configuración de notificaciones	168
Configurar servidores de correo electrónico globales para notificaciones	171
Añadir un servidor de correo electrónico saliente específico del tenant	173
Añadir un servidor de correo electrónico entrante específico del tenant	174
Reemplazar un servidor de correo electrónico saliente predeterminado de sistema	175
Reemplazar un servidor de correo electrónico entrante predeterminado de sistema	176
Revertir a los servidores de correo electrónico predeterminados del sistema	177
Configurar notificaciones	177
Personalizar la fecha de notificación de correo electrónico de caducidad de máquina	177
Configurar plantillas para correos electrónicos de IaaS automáticos	178
Suscribirse a notificaciones	178

Crear un archivo RDP personalizado para admitir conexiones RDP para máquinas aprovisionadas	179
Escenario: Añadir ubicaciones de centros de datos para implementaciones en varias regiones	179
Configurar vRealize Orchestrator y complementos	180
Configurar la carpeta de flujo de trabajo predeterminada de un tenant	181
Configurar un servidor de vRealize Orchestrator externo	181
Iniciar sesión en la interfaz de configuración de vRealize Orchestrator	182
Iniciar sesión en el cliente de vRealize Orchestrator	183

3 Configurar recursos 185

Lista de comprobación para la configuración de recursos de IaaS	185
Almacenar credenciales de usuario	186
Elegir un escenario de endpoint	188
Crear un grupo de tejidos	207
Configurar prefijos de máquina	207
Administrar pares de claves	208
Crear un perfil de red	210
Configurar las reservas y las políticas de reserva	228
Escenario: Configurar recursos de IaaS para Rainpole	264
Escenario: Aplicar una ubicación a un recurso informático para implementaciones entre regiones	268
Lista de comprobación para preparar el aprovisionamiento de una implementación de vRealize Automation con un proveedor de IPAM externo	269
Configurar recursos de XaaS	270
Configurar el complemento Active Directory como un endpoint	270
Configurar el complemento de HTTP-REST como un endpoint	271
Configurar el complemento de PowerShell como un endpoint	273
Configurar el complemento de SOAP como un endpoint	274
Configurar el complemento de vCenter Server como un endpoint	276
Crear un endpoint de Microsoft Azure	277
Crear y configurar contenedores	280
Ver y administrar hosts de contenedores	280
Usar colocaciones de implementación de contenedores	282
Usar zonas de colocación de contenedores	283
Configurar las opciones de contenedor	284
Configurar y usar plantillas e imágenes en Contenedores	289
Usar registros de contenedor	293
Configurar recursos de red para contenedores	295
Instalar complementos adicionales en el servidor predeterminado de vRealize Orchestrator	298
Trabajar con políticas de Active Directory	299
Crear y aplicar políticas de Active Directory	299

4 Proporcionar servicios a petición a los usuarios 303

Diseñar blueprints	303
Exportar e importar blueprints	305
Escenario: importar Dukes Bank para la aplicación de muestra de vSphere y configurar el entorno	306
Escenario: Probar la aplicación de muestra Dukes Bank	309

Crear la biblioteca de diseño	310
Diseñar blueprints de máquinas	313
Diseñar componentes de Software	379
Diseñar acciones personalizadas y blueprints XaaS	396
Publicar un blueprint	452
Ensamblar blueprints compuestos	453
Información sobre el comportamiento de blueprint anidado	454
Seleccionar un componente de máquina compatible con componentes de Software	456
Crear enlaces de propiedad entre componentes de blueprint	457
Crear dependencias explícitas y controlar el orden de aprovisionamiento	458
Escenario: Ensamblar y probar un blueprint para suministrar MySQL en máquinas de clones vinculados de Rainpole	459
Administrar el catálogo de servicios	462
Lista de comprobación para configurar el catálogo de servicios	463
Crear un servicio	464
Trabajar con elementos del catálogo y acciones	467
Crear autorizaciones	469
Trabajar con políticas de aprobación	476
Escenario: Configurar el catálogo para que los arquitectos de Rainpole prueben los blueprints	496
Escenario: Probar la máquina CentOS de Rainpole	499
Escenario: Hacer que el blueprint de aplicación CentOS con MySQL esté disponible en el catálogo de servicios	500
Escenario: Crear y aplicar políticas de aprobación de CentOS con MySQL	504
Índice	509

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.

Para obtener más información sobre las integraciones admitidas, consulte <https://www.vmware.com/pdf/vrealize-automation-72-support-matrix.pdf>.

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
ES-002290-05	<ul style="list-style-type: none">■ Se ha actualizado “Administración de conectores y clústeres de conectores,” página 108.■ Se ha actualizado “Configurar los ajustes del conector,” página 148.■ Se ha actualizado “Crear un endpoint de Microsoft Azure,” página 201.■ Se ha actualizado “Crear un blueprint para Microsoft Azure,” página 362.■ Se ha actualizado “Configurar una conexión del directorio OpenLDAP,” página 94.■ Se ha actualizado “Configurar una instancia del proveedor de identidades,” página 128.
ES-002290-04	<ul style="list-style-type: none">■ Se ha actualizado “Preparar una máquina Windows de referencia para que sea compatible con el Software,” página 73.■ Se ha actualizado “Información sobre el comportamiento de blueprint anidado,” página 454.■ Se ha actualizado “Crear un endpoint de Microsoft Azure,” página 201.■ Se ha actualizado “Crear un blueprint para Microsoft Azure,” página 362.
ES-002290-03	<ul style="list-style-type: none">■ Se ha actualizado “Preparar una máquina Windows de referencia para que sea compatible con el Software,” página 73.■ Se ha actualizado “Preparar una máquina Linux de referencia para que sea compatible con Software,” página 75.
ES-002290-02	<ul style="list-style-type: none">■ Se ha actualizado “Preparar el aprovisionamiento de Software,” página 71.■ Se ha actualizado “Diseñar componentes de Software,” página 379.
ES-002290-01	Se ha actualizado “Indicar la información del perfil de red externa mediante el endpoint de IPAM suministrado,” página 215.
ES-002290-00	Versión inicial.

Preparaciones externas para el aprovisionamiento

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 cubre los siguientes temas:

- [“Preparar el entorno para la administración de vRealize Automation,”](#) página 11
- [“Preparar el aprovisionamiento de máquinas,”](#) página 27
- [“Preparar el aprovisionamiento de Software,”](#) página 71

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
 NSX	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,” página 12.
 vCloud Director	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,” página 19.
 vCloud Air	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,” página 52.

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

Entorno	Preparativos
 Amazon AWS	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,” página 20.
 Red Hat OpenStack	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,” página 25.
 SCVMM	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,” página 26.
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 preparar la compatibilidad con proveedores de IPAM de terceros,” página 16.
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,” página 27.

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.

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,”](#) página 345.

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

Tarea	Ubicación	Detalles
<input type="checkbox"/> Instalar y configurar el complemento NSX.	Instale el complemento de NSX en vRealize Orchestrator.	Consulte “Instalar el complemento de NSX en vRealize Orchestrator,” página 13 y la <i>Guía de administración de NSX</i> .
<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,” página 15. 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.

NOTA: Si usa un vRealize Orchestrator integrado que contiene un complemento de NSX instalado, no necesita realizar estos pasos porque el complemento de NSX ya está instalado.

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

Prerequisitos

- 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 la versión correcta del complemento de NSX. Consulte *Matriz de soporte de vRealize Automation*.
- Compruebe que ha instalado el cliente de vRealize Orchestrator y que puede iniciar sesión con credenciales de administrador.

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.

Qué hacer a continuación

Cree un endpoint de vRealize Orchestrator en vRealize Automation para usarlo para ejecutar flujos de trabajo. Consulte [“Crear un endpoint de vRealize Orchestrator,”](#) página 191.

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.

Prerequisitos

- Confirme que hay un endpoint de vSphere registrado con un endpoint de NSX. Consulte “[Crear un endpoint de vSphere](#),” página 188.
- 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.

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.

Qué hacer a continuación

Aplicar las funciones de seguridad correspondientes al blueprint.

Requisitos del administrador para el aprovisionamiento de objetos universales de NSX

Para aprovisionar máquinas en una implementación de vCenter cruzada cuando se usan objetos universales de NSX, como una puerta de enlace de Edge o un equilibrador de carga, el aprovisionamiento se debe realizar en una región en la que el administrador de equipos de NSX tenga la función principal.

Solo hay un administrador principal de NSX en un entorno de vCenter cruzado con NSX. Para aprovisionar máquinas en una implementación de vCenter cruzada, las máquinas deben residir en una región en la que el administrador de equipos de NSX tenga la función principal. Si las máquinas existen en una región en la que el administrador de equipos de NSX tiene la función secundaria, se producirá un error en el aprovisionamiento.

Puede usar objetos locales de NSX, como una puerta de enlace de Edge o un equilibrador de carga locales. Cuando se usan objetos locales de NSX, también debe usar una zona de transporte local y un cable virtual de objetos de NSX específicos de la región. Puede configurar reservas de vRealize Automation para usar la zona de transporte local y los cables virtuales para las implementaciones en esa región local.

Para obtener más información, 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 NSX (2147240)* en <http://kb.vmware.com/kb/2147240>.

Consulte la *guía de administración de NSX* y la *guía de instalación de NSX en centros virtuales cruzados* para obtener información sobre cómo configurar y asignar la función de administrador de NSX principal para una implementación de vCenter cruzada.

Lista de comprobación para preparar la compatibilidad con proveedores 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 [“Lista de comprobación para preparar el aprovisionamiento de una implementación de vRealize Automation con un proveedor de IPAM externo,”](#) página 269.

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

Tarea	Ubicación	Detalles
<input type="checkbox"/> Obtenga e importe el complemento de vRealize Orchestrator del proveedor de IPAM externo compatible.	<p>Desde VMware Solution Exchange, descargue el complemento o el paquete de proveedor de IPAM (por ejemplo, el complemento de Infoblox IPAM o el paquete SDK de inicio de IPAM de terceros suministrado por VMware) e importe el complemento o el paquete a vRealize Orchestrator.</p> <p>Si VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_groups/cloud-management) 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 de soporte.</p>	<p>Consulte “Obtener e importar un paquete de proveedores de IPAM externos en vRealize Orchestrator,” página 16.</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,” página 17.</p>

Obtener e importar un paquete de proveedores de IPAM externos en vRealize Orchestrator

Para poder definir y usar un endpoint de proveedor de IPAM externo, primero debe obtener el paquete de proveedores de IPAM externos 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 utilizando el paquete de inicio suministrado por VMware y la documentación SDK adjunta para utilizarlo con otro proveedor de soluciones IPAM de terceros, como Bluecat.

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

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*.

Prerequisitos

- 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 de VMware Solution Exchange en <https://solutionexchange.vmware.com/store>.
- 2 Seleccione **Cloud Management Marketplace**.
- 3 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 Automation.
- 4 En vRealize Orchestrator, haga clic en la pestaña **Administrador** y luego haga clic en **Importar paquete**.
- 5 Por ejemplo, seleccione el paquete de IPAM de terceros de vRealize Orchestrator.

Seleccione `com.vmware.vra.ipam.service.sdk` desde `source\vcac\components\ipam\vro-sdk\target\ipam-package-sdk-7.1.0-SNAPSHOT.package`.
- 6 Seleccione todos los flujos de trabajo y artefactos y haga clic en **Importar elementos seleccionados**.

Qué hacer a continuación

[“Ejecutar el flujo de trabajo para registrar un tipo de endpoint de IPAM de terceros en vRealize Orchestrator,”](#) página 17.

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.

Para registrar los tipos de endpoint de IPAM en vRealize Orchestrator, se le pedirá que suministre credenciales de administrador de vRA de vRealize Automation.

Para obtener más información sobre cómo importar paquetes y ejecutar 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 y paquetes de vRealize Orchestrator, consulte *Extensibilidad del ciclo de vida*.

Prerequisitos

- [“Obtener e importar un paquete de proveedores de IPAM externos en vRealize Orchestrator,”](#) página 16
- Compruebe que ha iniciado sesión en vRealize Orchestrator con vRealize Automation con permiso para ejecutar flujos de trabajo.
- Prepárese para suministrar las credenciales de administrador de vRealize Automation de vRealize Automation cuando se le soliciten.

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 Cuando se le soliciten las credenciales de vRealize Automation, escriba las credenciales de administrador de vRA de vRealize Automation.

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 cuando defina los 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.

Qué hacer a continuación

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,”](#) página 192.

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> .
Mostrar el sistema de ayuda contextual de Contenedores.	Consulte la información de ayuda de Contenedores 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 de Xenon en vRealize Automation 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 interfaz de línea de comandos en el dispositivo de vRealize Automation.

Comando	Descripción
service xenon-service status	Muestra el estado del servicio (en ejecución o detenido).
service xenon-service start	Inicia el servicio.
service xenon-service stop	Detiene el servicio.
service xenon-service restart	Reinicia el servicio.
service xenon-service get_host	Muestra el nombre de host en el que se está ejecutando el servicio.
service xenon-service get_port	Muestra el puerto del servicio.
service xenon-service status_cluster	Muestra información sobre todos los nodos en clúster en formato JSON.
service xenon-service reset	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 ejecutando el comando siguiente en una interfaz de línea de comandos:

```
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.

Debe disponer de ciertos derechos de acceso a Amazon para aprovisionar máquinas correctamente mediante vRealize Automation.

- Autorización de funciones y permisos en Amazon Web Services

La función Usuario avanzado de AWS proporciona a un usuario o grupo del servicio de directorio de AWS acceso completo a los servicios y recursos de AWS.

No se necesitan credenciales de AWS para crear un endpoint de AWS en vRealize Automation. Sin embargo, vRealize Automation espera que el usuario de AWS que crea una imagen de máquina de Amazon tenga la función Usuario avanzado.

- Credenciales de autenticación en Amazon Web Services

La función Usuario avanzado de AWS no permite administrar los usuarios y grupos de AWS Identity and Access Management (IAM). Para administrar los usuarios y grupos de IAM, debe estar configurado con credenciales de Administrador de acceso completo de AWS.

vRealize Automation requiere claves de acceso para credenciales de endpoint y no admite nombres de usuario ni contraseñas. Para obtener la clave de acceso necesaria para crear el endpoint de Amazon, el Usuario avanzado 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.

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 una recopilación de datos de inventario o estado, y deshabilitar o cambiar la frecuencia de la recopilación de datos de inventario o estado.

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,”](#) página 231.
- 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.

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

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

Prerequisitos

- Instale y configure por completo vRealize Automation. Consulte *Instalación y configuración de vRealize Automation para el escenario de Rainpole*.
- 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 Deshabilite 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.

Qué hacer a continuación

- 1 Instale el agente de arranque del software y el agente invitado en una máquina de referencia Windows o Linux para crear una imagen de máquina de Amazon que los arquitectos de IaaS puedan usar para crear blueprints. Consulte [“Preparar el aprovisionamiento de Software,”](#) página 71.
- 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,”](#) página 251.

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 7.2*.

Para obtener información relacionada con el aprovisionamiento de máquinas, consulte [“Crear un endpoint de Hyper-V \(SCVMM\)”](#), página 196.

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, las siguientes palabras 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.

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.

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 o 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,” página 30
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,” página 71.

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

Escenario	Endpoint compatible	Compatibilidad con agentes	Método de aprovisionamiento	Preparativos anteriores al aprovisionamiento
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 de aprovisionar, seleccione un método de aprovisionamiento que admita el agente invitado. Para obtener más información sobre el agente invitado, consulte “Usar el agente invitado de vRealize Automation durante el aprovisionamiento,” página 31.
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	Debe tener ya una máquina virtual de vSphere. Para admitir Software, debe instalar el agente invitado y el agente de arranque de software en la máquina que vaya a clonar. El snapshot de máquina virtual identificado en el blueprint debe apagarse antes de aprovisionar las máquinas virtuales de clon vinculado.
Aprovisionar una copia con espacio eficiente de una máquina virtual mediante la tecnología Net App FlexClone.	vSphere	(Opcional) Agente invitado	NetApp FlexClone	“Lista de comprobación para preparar el aprovisionamiento mediante clonación,” página 38
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	Consulte “Lista de comprobación para preparar el aprovisionamiento mediante clonación,” página 38. Para admitir Software, debe instalar el agente invitado y el agente de arranque de software en la máquina de vSphere que vaya a clonar.
Aprovisione 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	Consulte “Preparar el aprovisionamiento de vCloud Air y vCloud Director,” página 52. 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.

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

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,” página 53
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,” página 56
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. Puede usar PEBuilder para crear una imagen WinPE que incluya el agente invitado. Puede crear la imagen WinPE mediante otro método, pero debe insertar manualmente el agente invitado.	WIM	“Preparar el aprovisionamiento de WIM,” página 57
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,” página 66.
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
<input type="checkbox"/> Instalar y configurar el agente de EPI de scripts de Visual Basic.	Normalmente, el host de Manager Service.	Consulte <i>Instalación de vRealize Automation 7.2</i> .
<input type="checkbox"/> Crear los scripts de Visual Basic.	Máquina en la que está instalado el agente de EPI.	vRealize Automation incluye un script de Visual Basic de ejemplo (<code>PrePostProvisioningExample.vbs</code>) en el subdirectorio <code>Scripts</code> 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. 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.
<input type="checkbox"/> Reunir la información necesaria para incluir sus scripts en los blueprints.	La información se captura y transfiere a los arquitectos de la infraestructura. NOTA: Un administrador de tejido puede crear un grupo de propiedades mediante los conjuntos de propiedades <code>ExternalPreProvisioningVbScript</code> y <code>ExternalPostProvisioningVbScript</code> para proporcionar la información necesaria. De este modo, será más fácil que los arquitectos de blueprints incluyan esta información correctamente en sus blueprints.	<ul style="list-style-type: none"> ■ La ruta completa del script de Visual Basic, incluidos el nombre de archivo y la extensión. Por ejemplo: <code>%Unidad del sistema %Archivos de programa (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs</code>. ■ 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 <code>ExternalPreProvisioningVbScript</code>. Para ejecutar un script después del aprovisionamiento, es necesario usar la propiedad personalizada <code>ExternalPostProvisioningVbScript</code>.

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 le permite almacenar información cifrada que el agente invitado puede descifrar y comprender como argumento de línea de comandos válido.

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 (Continúa)

Propiedad personalizada	Descripción
<code>VirtualMachine.SoftwareN.ScriptPath</code>	<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>
<code>VirtualMachine.ScriptPath.Decrypt</code>	<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> <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 <code>[MyPassword]</code> 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>.

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

Propiedad personalizada	Descripción
	<ul style="list-style-type: none"> ■ Establezca la propiedad personalizada <code>VirtualMachine.Software0.ScriptPath</code> en <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat [MyPassword]</code>. Si establece <code>VirtualMachine.ScriptPath.Decrypt</code> en <code>False</code> o no crea la propiedad personalizada <code>VirtualMachine.ScriptPath.Decrypt</code>, no se descifrá la cadena que está entre corchetes ([y]).

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 `gugent`

`C:\VRMGuestAgent\cert.pem`

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

`/usr/share/gugent/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.

NOTA: Opcionalmente, puede configurar el agente invitado para que rellene el archivo `cert.pem` de confianza en el primer uso, pero este método es menos seguro que la instalación manual del archivo `cert.pem` en cada plantilla. Considere utilizar esta alternativa si emplea una sola plantilla para varios servidores. Para permitir que el agente invitado confíe en el primer servidor al que se conecte, cree una plantilla sin ningún archivo `cert.pem` en el directorio `VRMGuestAgent` de Windows o el directorio `/usr/share/gugent` de Linux. El agente invitado rellena el archivo `cert.pem` la primera vez que se conecta a un servidor.

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 de PEBuilder. 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,”](#) página 35 o [“Instalar el agente invitado en una máquina de referencia de Windows,”](#) página 37.

La plantilla siempre confía en el primer sistema al que se conecte. Para mayor seguridad, el agente invitado no busca un certificado si existe un archivo `cert.pem` en el directorio `VRMGuestAgent` de Windows o el directorio `/usr/share/gugent` de Linux. Si el certificado de servidor cambia, debe quitar el archivo `cert.pem` del directorio `VRMGuestAgent` de Windows o el directorio `/usr/share/gugent` de Linux. El agente invitado instala el nuevo archivo `cert.pem` la próxima vez que se conecta al servidor.

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.

Prerequisitos

- 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,”](#) página 34.

Procedimiento

- 1 Vaya a la página de la consola de administración de vCloud Automation Center Appliance.
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>

Qué hacer a continuación

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 en una máquina de referencia de Windows para ejecutarlo como un servicio de Windows y permitir una mayor personalización de las máquinas.

Prerequisitos

- 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,”](#) página 34.

Procedimiento

- 1 Vaya a la página de la consola de administración de vCloud Automation Center Appliance.
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 a la que la máquina de Windows pueda acceder.

Se creará el directorio `C:\VRMGuestAgent`. No cambie el nombre de este directorio.
- 5 Configure el agente invitado para que se comunique con Manager Service.
 - a Abra una ventana de símbolo del sistema con privilegios elevados.
 - b Vaya a `C:\VRMGuestAgent`.

- c Configure el agente invitado para que confíe en la máquina de Manager Service.

Opción	Descripción
Permita que el agente invitado confíe en la primera máquina a la que se conecte.	No se requiere configuración.
Instale manualmente el archivo PEM de confianza.	Coloque el archivo PEM de Manager Service en el directorio C:\VRMGuestAgent\.

- d Ejecute `win service -i -h Manager_Service_Hostname_fdn: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>

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

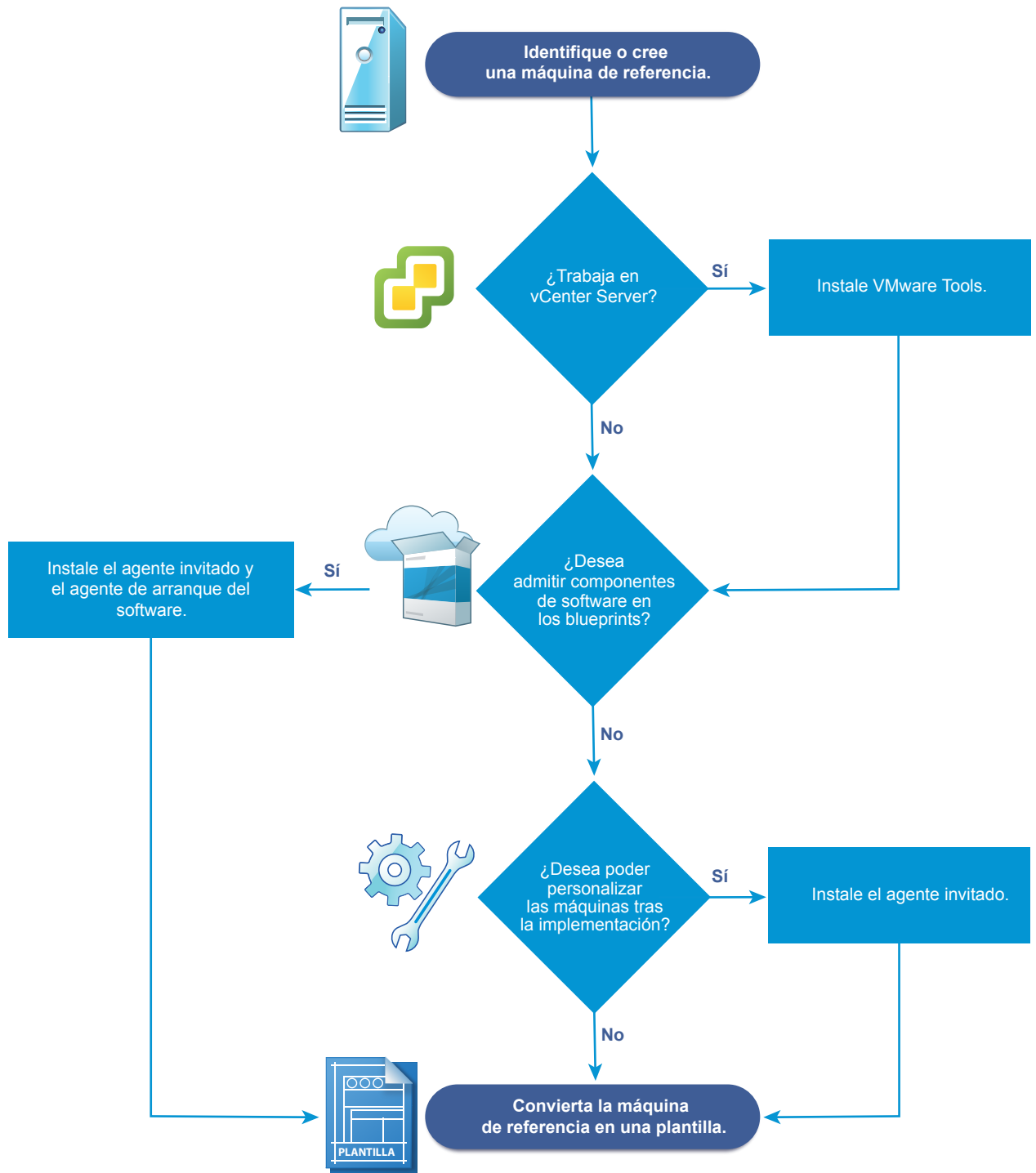
Qué hacer a continuación

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	Para máquinas Windows de referencia, consulte “Preparar una máquina Windows de referencia para que sea compatible con el Software,” página 73. Para máquinas Linux de referencia, consulte “Preparar una máquina Linux de referencia para que sea compatible con Software,” página 75.
<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,” página 31.
<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	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. Consulte la documentación que le ha proporcionado el hipervisor.
<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	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. Consulte la documentación que le ha proporcionado el hipervisor.
<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,” página 41.

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%</i> Archivos de programa (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs.
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%</i> Archivos de programa (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs

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.AllowLogins</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 deshabilitar 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.

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

Propiedad personalizada	Mi valor	Descripción
<code>VirtualMachine.DiskN.Size</code>		<p>Define el tamaño en GB del disco <i>N</i>. Por ejemplo, para que un disco <i>G</i> tenga un tamaño de 150 GB, defina la propiedad personalizada <code>VirtualMachine.Disk0.Size</code> y establezca un valor de 150. La numeración de discos debe ser secuencial. De forma predeterminada, una máquina tiene un disco al que <code>VirtualMachine.Disk0.Size</code> hace referencia, donde el tamaño se especifica por medio del valor de almacenamiento en el blueprint a partir del cual la máquina se aprovisiona. El valor de almacenamiento en la interfaz de usuario del blueprint reemplaza el valor en la propiedad <code>VirtualMachine.Disk0.Size</code>. La propiedad <code>VirtualMachine.Disk0.Size</code> no está disponible como una propiedad personalizada debido a su relación con la opción de almacenamiento en el blueprint. Se pueden añadir más discos indicando <code>VirtualMachine.Disk1.Size</code>, <code>VirtualMachine.Disk2.Size</code>, etc. <code>VirtualMachine.Admin.TotalDiskUsage</code> siempre representa el total de las propiedades <code>.DiskN.Size</code> más la asignación de tamaño de <code>VMware.Memory.Reservation</code>.</p>
<code>VirtualMachine.DiskN.Label</code>		<p>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.</p>
<code>VirtualMachine.DiskN.Letter</code>		<p>Especifica la letra de unidad o punto de montaje del disco <i>N</i> de una máquina. El valor predeterminado es <i>C</i>. Por ejemplo, para especificar la letra <i>D</i> para Disco 1, defina la propiedad personalizada como <code>VirtualMachine.Disk1.Letter</code> y escriba el valor <i>D</i>. 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.</p>

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

Propiedad personalizada	Mi valor	Descripción
VirtualMachine.Admin.CustomizeGuestOSDelay		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.
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.
VirtualMachine.SoftwareN.Name		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.
VirtualMachine.SoftwareN.ScriptPath		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. Puede transferir valores de propiedad personalizada como parámetros al script si inserta <i>{CustomPropertyName}</i> en la cadena de la ruta. Por ejemplo, si tiene una propiedad personalizada denominada <i>ActivationKey</i> 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.

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

Propiedad personalizada	Mi valor	Descripción
<code>VirtualMachine.SoftwareN.ISOName</code>		Especifica la ruta y el nombre de archivo del archivo ISO relativo a la raíz de almacén de datos. El formato es <code>/folder_name/subfolder_name/file_name.iso</code> . Si no se especifica ningún valor, la imagen ISO no se montará.
<code>VirtualMachine.SoftwareN.ISOLocation</code>		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, <code>netapp-1:it_nfs_1</code> . Si no se especifica ningún valor, la imagen ISO no se montará.

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 <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 (Continúa)

Propiedad personalizada	Mi valor	Descripción
<code>VirtualMachine.NetworkN.MacAddress</code>		<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 <code>VirtualMachine.NetworkN.MacAddressType</code> se genera, esta propiedad contiene la dirección generada.</p> <p>Si el valor de <code>VirtualMachine.NetworkN.MacAddressType</code> 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 <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 (Continúa)

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.</p> <p>Esta propiedad se puede añadir a un componente de máquina de vCloud Air o vCloud Directoren un blueprint. No se admite esta propiedad para redes enrutadas a petición o NAT a petición.</p>
<code>VirtualMachine.NetworkN.PortID</code>		<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 <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 (Continua)

Propiedad personalizada	Mi valor	Descripción
VirtualMachine.NetworkN.ProfileName		<p>Especifica el nombre de un perfil de red del que se asigna una dirección IP estática al dispositivo de red N o del que se obtiene un rango de direcciones IP estáticas que se pueden asignar al dispositivo de red N de una máquina clonada, donde N=0 corresponde al primer dispositivo, 1 al segundo, y así sucesivamente.</p> <p>Cuando se usa la propiedad VirtualMachine.NetworkN.ProfileName, el perfil de red al que apunta se utiliza para asignar una dirección IP. Sin embargo, la máquina aprovisionada se conecta a cualquier red seleccionada en la reserva mediante un modelo Round Robin de operación por turnos.</p>
<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.ProfileName.</p>

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

Propiedad personalizada	Mi valor	Descripción
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. Los nombres distinguen mayúsculas de 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 (Continúa)

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,”](#) página 54.
- 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,”](#) página 55.
 - 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,”](#) página 30.
- 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 Vaya a la página de la consola de administración de vCloud Automation Center Appliance.
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`.

Prerequisitos

- Prepare un archivo de configuración de kickstart o autoYaST. Consulte [“Preparar el archivo de muestra de configuración de Kickstart de Linux,”](#) página 54.
- 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 Convierta a su script en 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
```

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 Consulte a su administrador de red para asegurarse de que se cumplen los siguientes requisitos de red:
 - La comunicación con SCCM requiere el nombre de NetBios del servidor SCCM. Al menos un Distributed Execution Manager (DEM) debe poder resolver el nombre completo del servidor SCCM como su nombre de NetBios.
 - El servidor SCCM y el servidor de vRealize Automation deben estar en la misma red y a disposición el uno del otro.
- 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,”](#) página 57.
- 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.

NOTA: Puede crear un grupo de propiedades con el conjunto de propiedades SCCMProvisioningProperties para incluir la información necesaria. De este modo será más fácil incluir la información en los blueprints.

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 Vaya a la página de la consola de administración de vCloud Automation Center Appliance.
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. Debería ser un directorio de red que se pueda especificar como ruta UNC o que la máquina de referencia pueda montar como unidad de red, el sistema en el que se creará la imagen WinPE y el host de virtualización en el que se aprovisionan las máquinas.
- 2 Asegúrese de que hay un servidor DHCP disponible en la red. vRealize Automation no puede aprovisionar máquinas mediante 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,”](#) página 59. 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,”](#) página 59.
- 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. Puede usar el PEBuilder de vRealize Automation para crear una imagen WinPE que incluya el agente invitado.
 - [“Instalar PEBuilder,”](#) página 60.
 - (Opcional) Cree los scripts personalizados que desee usar para personalizar las máquinas aprovisionadas y colóquelos en el directorio de elementos de trabajo adecuado de la instalación de PEBuilder. Consulte [“Especificar scripts personalizados en un WinPE PEBuilder,”](#) página 61.
 - 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 [“Preparación del aprovisionamiento WIM con controladores VirtIO,”](#) página 61.
 - [“Crear una imagen de WinPE con PEBuilder,”](#) página 62.

Puede crear la imagen WinPE mediante otro método, pero deberá insertar manualmente el agente invitado de vRealize Automation. Consulte [“Introducir manualmente el agente invitado en una imagen de WinPE,”](#) página 63.
- 7 Coloque la imagen WinPE en la ubicación que requiera la plataforma de virtualización. Si desconoce la ubicación, consulte la documentación suministrada por el 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.

- 1 [Requisitos de máquina de referencia para el aprovisionamiento WIM](#) página 59
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](#) página 59
Un archivo de respuesta de SysPrep contiene varias configuraciones necesarias que se utilizan para el aprovisionamiento de WIM.
- 3 [Instalar PEBuilder](#) página 60
La herramienta PEBuilder que vRealize Automation suministra ofrece una forma muy sencilla de incluir el agente invitado de vRealize Automation en las imágenes de WinPE.

- 4 [Especificar scripts personalizados en un WinPE PEBuilder](#) página 61
Puede utilizar PEBuilder para personalizar máquinas, mediante la ejecución de scripts bat personalizados en puntos especificados del flujo de trabajo de aprovisionamiento.
- 5 [Preparación del aprovisionamiento WIM con controladores VirtIO](#) página 61
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).
- 6 [Crear una imagen de WinPE con PEBuilder](#) página 62
Use la herramienta PEBuilder que vRealize Automation suministra para crear un archivo ISO de WinPE que incluya el agente invitado de vRealize Automation.
- 7 [Introducir manualmente el agente invitado en una imagen de WinPE](#) página 63
No hay que usar PEBuilder de vRealize Automation para crear la imagen de WinPE. Sin embargo, si no utiliza PEBuilder, deberá insertar el agente invitado de vRealize Automation manualmente en la imagen de 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 7.2*.

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.

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

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 (Continúa)

Configuración de GuiUnattended	Valor
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
Username	<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).
Password	<i>password</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). 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.

Instalar PEBuilder

La herramienta PEBuilder que vRealize Automation suministra ofrece una forma muy sencilla de incluir el agente invitado de vRealize Automation en las imágenes de WinPE.

PEBuilder tiene un agente invitado de 32 bits. Si necesita ejecutar comandos específicos de 64 bits, instale PEBuilder y, luego, obtenga los archivos de 64 bits del archivo GugenZip64.zip.

Instale PEBuilder en una ubicación donde pueda tener acceso al entorno de almacenamiento provisional.

Prerequisitos

- Instale NET Framework 4.5.
- El Kit de instalación automatizada de Windows (AIK) para Windows 7 (WinPE 3.0 incluido) está instalado.

Procedimiento

- 1 Vaya a la página de la consola de administración de vCloud Automation Center Appliance.

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 la utilidad **PE Builder** en la sección de instalación de componentes de la página para descargar y guarde el archivo vCAC-WinPEBuilder-Setup.exe.
- 4 Ejecute vCAC-WinPEBuilder-Setup.exe.
- 5 Siga las indicaciones para instalar PEBuilder.
- 6 (Opcional) Reemplace los archivos de agente invitado de 32 bits de Windows ubicados en \PE Builder\Plugins\VRM Agent\VRMGuestAgent por los archivos de 64 bits para, de este modo, incluir el agente de 64 bits en su WinPE.

PEBuilder se puede utilizar para crear una imagen de WinPE para su uso en el aprovisionamiento de WIM.

Especificar scripts personalizados en un WinPE PEBuilder

Puede utilizar PEBuilder para personalizar máquinas, mediante la ejecución de scripts bat personalizados en puntos especificados del flujo de trabajo de aprovisionamiento.

Prerequisitos

[“Instalar PEBuilder,”](#) página 60.

Procedimiento

- 1 Cree o identifique el script bat que desea usar.
El script debe devolver un valor distinto de cero en caso de error para evitar un error de aprovisionamiento de máquina.
- 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 Convierta a su script en ejecutable.
- 4 Coloque los scripts en el subdirectorio de elemento de trabajo correspondiente al punto del flujo de trabajo de aprovisionamiento en el que desea ejecutar el script.
Por ejemplo, C:\Archivos de programa (x86)\VMware\VRM Agent\PE Builder\Plugins\VRM Agent\VRMGuestAgent\site\SetupOS.

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

Preparación del 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 están 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 controlador de VirtIO en el subdirectorio `Complementos` del directorio de instalación de PEBuilder antes de crear una imagen WinPE, o inserte los controladores en una imagen WinPE creada por otros medios.
- 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).

Crear una imagen de WinPE con PEBuilder

Use la herramienta PEBuilder que vRealize Automation suministra para crear un archivo ISO de WinPE que incluya el agente invitado de vRealize Automation.

Prerequisitos

- [“Instalar PEBuilder,”](#) página 60.
- (Opcional) Configure PEBuilder de forma que incluya el agente invitado de Windows de 64 bits en WinPE, en vez del de 32 bits. Consulte [“Instalar PEBuilder,”](#) página 60.
- (Opcional) Incluya en el subdirectorio `PlugIns` del directorio de instalación de PEBuilder todos aquellos complementos de terceros que quiera añadir a la imagen de WinPE.
- (Opcional) [“Especificar scripts personalizados en un WinPE PEBuilder,”](#) página 61.

Procedimiento

- 1 Ejecute PEBuilder.
- 2 Especifique la información de host de IaaS Manager Service.

Opción	Descripción
Si usa un equilibrador de carga	a Escriba el nombre de dominio completo del equilibrador de carga de IaaS Manager Service en el cuadro de texto Nombre de host de vCAC . Por ejemplo, <code>manager_service_LB.mycompany.com</code> .
	b Escriba el número de puerto del equilibrador de carga de IaaS Manager Service en el cuadro de texto Puerto vCAC . Por ejemplo, 443 .
Si no usa un equilibrador de carga	a Escriba el nombre de dominio completo de la máquina de IaaS Manager Service en el cuadro de texto Nombre de host de vCAC . Por ejemplo, <code>manager_service.mycompany.com</code> .
	b Escriba el número de puerto de la máquina de IaaS Manager Service en el cuadro de texto Puerto vCAC . Por ejemplo, 443 .

- 3 Escriba la ruta al directorio de complementos de PEBuilder.

Esto dependerá del directorio de instalación especificado durante la instalación. La ruta predeterminada es `C:\Program Files (x86)\VMware\vCAC\PE Builder\PlugIns`.

- 4 Escriba la ruta de salida el archivo ISO que está creando en el cuadro de texto **Ruta de salida de ISO**.
Esta ubicación debe estar en el área de almacenamiento provisional que haya preparado.
- 5 Haga clic en **Archivo > Avanzado**.

NOTA: No modifique los valores de **Arquitectura de WinPE** ni **Protocolo**.

- 6 Active la casilla **Incluir agente invitado de vCAC en ISO de WinPE**.
- 7 Haga clic en **Aceptar**.
- 8 Haga clic en **Compilar**.

Qué hacer a continuación

Colocar la imagen de WinPE en la ubicación que requiera la plataforma de integración. Si desconoce la ubicación, consulte la documentación suministrada por la plataforma.

Si está aprovisionando máquinas de HP iLO, coloque la imagen de WinPE en una ubicación accesible desde Internet. En el caso de las máquinas de Dell iDRAC, coloque la imagen en una ubicación disponible para NFS o CIFS. Registre la dirección.

Introducir manualmente el agente invitado en una imagen de WinPE

No hay que usar PEBuilder de vRealize Automation para crear la imagen de WinPE. Sin embargo, si no utiliza PEBuilder, deberá insertar el agente invitado de vRealize Automation manualmente en la imagen de WinPE.

Prerequisitos

- 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](#) página 64
Si decide no utilizar PEBuilder de vRealize Automation para crear su WinPE, deberá instalar PEBuilder para copiar manualmente los archivos de agente invitado en su imagen de WinPE.
- 2 [Configurar el archivo doagent.bat](#) página 64
Si decide no utilizar vRealize Automation PEBuilder, deberá configurar el archivo doagent.bat manualmente.
- 3 [Configurar el archivo doagentc.bat](#) página 65
Si decide no utilizar vRealize Automation PEBuilder, deberá configurar el archivo doagentc.bat manualmente.
- 4 [Configurar el archivo de propiedades de agente invitado](#) página 66
Si decide no utilizar vRealize Automation PEBuilder, deberá configurar el archivo de propiedades de agente invitado manualmente.

Procedimiento

- 1 [“Insertar el agente invitado en una imagen de WinPE,”](#) página 64.
- 2 [“Configurar el archivo doagent.bat,”](#) página 64.
- 3 [“Configurar el archivo doagentc.bat,”](#) página 65.
- 4 [“Configurar el archivo de propiedades de agente invitado,”](#) página 66.

Insertar el agente invitado en una imagen de WinPE

Si decide no utilizar PEBuilder de vRealize Automation para crear su WinPE, deberá instalar PEBuilder para copiar manualmente los archivos de agente invitado en su imagen de WinPE.

PEBuilder tiene un agente invitado de 32 bits. Si necesita ejecutar comandos específicos de 64 bits, instale PEBuilder y, luego, obtenga los archivos de 64 bits del archivo `GugentZipx64.zip`.

Prerequisitos

- 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 Vaya a la página de la consola de administración de vCloud Automation Center Appliance.
Por ejemplo: `https://va-hostname.domain.com`.
- 2 Descargue PEBuilder.
- 3 (Opcional) Descargue el paquete de agente invitado de 64 bits de Windows si quiere incluir el agente invitado de 64 bits de Windows en su WinPE en lugar del de 32 bits.
- 4 Ejecute `vCAC-WinPEBuilder-Setup.exe`.
- 5 Anule la selección de **Plugins** y **PEBuilder**.
- 6 Expanda **Plugins** y seleccione **VRMAgent**.
- 7 Siga las indicaciones para completar la instalación.
- 8 (Opcional) Cuando la instalación finalice, reemplace los archivos de agente invitado de 32 bits de Windows ubicados en `\PE Builder\Plugins\VRM Agent\VRMGuestAgent` por los archivos de 64 bits para, de este modo, incluir el agente de 64 bits en su WinPE.
- 9 Copie el contenido de `%SystemDrive%\Program Files (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent` en una nueva ubicación de la imagen de WinPE.
Por ejemplo: `C:\Program Files (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent`.

Qué hacer a continuación

[“Configurar el archivo doagent.bat,”](#) página 64.

Configurar el archivo doagent.bat

Si decide no utilizar vRealize Automation PEBuilder, deberá configurar el archivo `doagent.bat` manualmente.

Prerequisitos

[“Insertar el agente invitado en una imagen de WinPE,”](#) página 64.

Procedimiento

- 1 Vaya al directorio `VRMGuestAgent` dentro de la imagen de WinPE.
Por ejemplo: `C:\Program Files (x86)\VMware\PE Builder\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.

- 4 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	Escriba el nombre de dominio completo y el puerto del equilibrador de carga de IaaS Manager Service. Por ejemplo: manager_service_LB.mycompany.com:443
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el puerto de la máquina en la que está instalado IaaS Manager Service. Por ejemplo: manager_service.mycompany.com:443

- 5 Reemplace todas las instancias de la cadena #Protocol# por la cadena /ssl.
- 6 Reemplace todas las instancias de la cadena #Comment# por la cadena REM (REM debe ir seguida de un espacio).
- 7 (Opcional) Si utiliza certificados autofirmados, quite la marca de comentario del comando openssl.
echo QUIT | c:\VRMGuestAgent\bin\openssl s_client -connect
- 8 Guarde y cierre el archivo.
- 9 Modifique el script Startnet.cmd de WinPE de forma que incluya doagent.bat como script personalizado.

Qué hacer a continuación

[“Configurar el archivo doagentc.bat,”](#) página 65.

Configurar el archivo doagentc.bat

Si decide no utilizar vRealize Automation PEBuilder, deberá configurar el archivo doagentc.bat manualmente.

Prerequisitos

[“Configurar el archivo doagent.bat,”](#) página 64.

Procedimiento

- 1 Vaya al directorio VRMGuestAgent dentro de la imagen de WinPE.
Por ejemplo: C:\Program Files (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent.
- 2 Haga una copia del archivo doagentsvc-template.bat y póngale el nombre doagentc.bat.
- 3 Abra doagentc.bat en un editor de texto.
- 4 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	Escriba el nombre de dominio completo y el puerto del equilibrador de carga de Manager Service. Por ejemplo: load_balancer_manager_service.mycompany.com:443
Si no usa un equilibrador de carga	Escriba el nombre de dominio completo y el puerto de Manager Service. Por ejemplo: manager_service.mycompany.com:443

- 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.

Qué hacer a continuación

[“Configurar el archivo de propiedades de agente invitado,”](#) página 66.

Configurar el archivo de propiedades de agente invitado

Si decide no utilizar vRealize Automation PEBuilder, deberá configurar el archivo de propiedades de agente invitado manualmente.

Prerequisitos

[“Configurar el archivo doagentc.bat,”](#) página 65.

Procedimiento

- 1 Vaya al directorio VRMGuestAgent dentro de la imagen de WinPE.
Por ejemplo: C:\Program Files (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent.
- 2 Haga una copia del archivo gument.properties y póngale el nombre gument.properties.template.
- 3 Haga una copia del archivo gument.properties.template y póngale el nombre gumentc.properties.
- 4 Abra gument.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 gumentc.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 han quitado de un blueprint, el blueprint se deshabilita y no se puede utilizar en solicitudes de máquina hasta que se edite para añadir 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 7.2*.
- 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.

Prerequisitos

Inicie sesión en la consola de 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/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** (✓).

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

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

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](#) página 70
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](#) página 71

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**.

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

Qué hacer a continuación

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**.

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

Qué hacer a continuación

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.

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,” página 38.
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.
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,” página 38.
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,” página 38.
Amazon AWS	Imagen de máquina de Amazon	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. Para que el agente invitado y el agente de arranque de Software funcionen en máquinas aprovisionadas, debe configurar la conectividad de red a VPC.

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

Instale la versión de Java Runtime Environment compatible, el agente invitado y el agente de arranque de Software en una máquina Windows de referencia para crear una plantilla, un snapshot o una instancia 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: Dado que no se debe interrumpir el proceso de arranque, configure la máquina virtual para que nada provoque que se detenga el proceso de arranque de la máquina virtual antes de que se alcance el mensaje final de inicio de sesión en el sistema operativo. Por ejemplo, asegúrese de que ningún proceso o script solicite la interacción del usuario cuando se inicie la máquina virtual.

El archivo `install.bat` configura el agente invitado para se comunique con Manager Service. El archivo `install.bat` puede recibir los siguientes esquemas de argumento:

- `[Backwards compatible darwin Local User] password=Password`
- `password=Password localUser=Username`
- `password=Password domainUser=Domainname\Username`
- `localSystem=true`

Si se encuentra con `passwordNeverExpire=false`(default), la caducidad de la contraseña seguirá la política de grupo. Si se establece como `true` o se deja en blanco, la contraseña nunca caduca.

Prerequisitos

- Identifique o cree una máquina de referencia.
- Si ya ha instalado el agente invitado o el agente de arranque de Software en esta máquina, quite los agentes y los logs en tiempo de ejecución. Consulte [“Actualizar plantillas de máquina virtual existentes en vRealize Automation,”](#) página 76.
- Si tiene previsto acceder de forma remota al escritorio remoto de Windows de la máquina virtual para solucionar problemas o para cualquier otro fin, instale Servicios de Escritorio remoto (RDS) para Windows.
- Compruebe que todos los artefactos de configuración de red se eliminen de los archivos de configuración de red.
- Establezca confianza segura entre el agente invitado y la máquina de Manager Service. Consulte [“Configurar el agente invitado para confiar en un servidor,”](#) página 34.
- Compruebe que el usuario `darwin` tenga derechos de `Log on as a service access` en la máquina de referencia de Windows.

Procedimiento

- 1 Inicie sesión en la máquina Windows de referencia como administrador de Windows y abra una ventana de símbolo del sistema.

- 2 Descargue e instale la versión de Java Runtime Environment compatible desde https://vRealize_VA_Hostname_fqdn/software/index.html.
 - a Descargue el archivo .zip de Java SE Runtime Environment:
https://vRealize_VA_Hostname_fqdn/software/download/jre-version-win64.zip.
 - b Cree una carpeta `c:\opt\vmware-jre` y descomprima el archivo .zip de JRE en la carpeta.
 - c Abra una ventana de símbolo del sistema e introduzca `c:\opt\vmware-jre\bin\java -version` para comprobar la instalación.

Se mostrará la versión instalada de Java.
- 3 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.
- 4 Descargue el archivo de arranque del agente de Software desde https://vRealize_VA_Hostname_fqdn/software/index.html.
 - a Descargue el archivo del agente de arranque de Software
https://vRealize_VA_Hostname_fqdn/software/download/vmware-vra-software-agent-bootstrap-windows_version.zip.
 - b Haga clic con el botón derecho en el archivo y seleccione **Propiedades**.
 - c Haga clic en **General**.
 - d Haga clic en **Desbloquear**.

IMPORTANTE: Si no desactiva esta característica de seguridad de Windows, no podrá usar el archivo de arranque del agente de Software.

- e Descomprima el archivo `vmware-vra-software-agent-bootstrap-windows_version.zip` en la carpeta `c:\temp`.
- 5 Instale el agente de arranque de Software.
 - a Abra una consola de símbolo del sistema de Windows y navegue a la carpeta `c:\temp`.
 - b Introduzca el comando para instalar el servicio de arranque del agente.


```
install.bat password=Password managerServiceHost=manager_service_machine.mycompany.com
managerServicePort=443 httpsMode=true cloudProvider=ec2|vca|vcd|vsphere
```

El número de puerto predeterminado de Manager Service es 443. Los valores aceptados para `cloudprovider` son `ec2`, `vca`, `vcd` y `vsphere`. El script `install.bat` crea una cuenta de usuario denominada `darwin` para el agente de arranque de software con la contraseña que estableció en el comando de instalación. La contraseña que establezca en `Password` debe cumplir los requisitos de contraseñas de Windows.

Si la instalación no se realiza correctamente debido a una dependencia de .NET, consulte el siguiente artículo para obtener ayuda: <https://technet.microsoft.com/en-us/library/dn482071.aspx>

- 6 Compruebe que existe el usuario **darwin**.
 - a Especifique `lusrmgr.msc` en el símbolo del sistema.
 - b Compruebe que existe el usuario **darwin_user** y que pertenece al grupo de administradores.
 - c Establezca la contraseña para que no caduque nunca.

La opción asegura que la plantilla siga siendo utilizable después de 30 días.

Si el usuario no está disponible, compruebe que la contraseña del servidor de Windows sea correcta.

- 7 Desconecte la máquina virtual de Windows.

Qué hacer a continuación

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.

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

Utilice un solo script para instalar la versión de Java Runtime Environment compatible, el agente invitado y el agente de arranque de Software en una máquina Linux de referencia para crear una plantilla, un snapshot o una instancia de máquina de Amazon que admita los componentes de Software.

Software admite scripts de Bash.

IMPORTANTE: Dado que no se debe interrumpir el proceso de arranque, configure la máquina virtual para que nada provoque que se detenga el proceso de arranque de la máquina virtual antes de que se alcance el mensaje final de inicio de sesión en el sistema operativo. Por ejemplo, asegúrese de que ningún proceso o script solicite la interacción del usuario cuando se inicie la máquina virtual.

Prerequisitos

- Identifique o cree una máquina Linux de referencia y compruebe que los siguientes comandos estén disponibles en función de su sistema Linux:
 - `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

Para obtener información relacionada con los requisitos previos para Linux, consulte el script `prepare_vra_template.sh`.

- Si piensa acceder de forma remota a la máquina virtual con el log `ssh` de Linux para solucionar problemas o por otros motivos, instale el servidor OpenSSH y el cliente para Linux.
- Quite los artefactos de configuración de red de los archivos de configuración de la red.

Procedimiento

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

- 2 Descargue el script de instalación desde su el 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.

- 6 Desconecte la máquina virtual de Linux.

El script quita cualquier instalación anterior del agente de arranque de Software e instala las versiones compatibles de Java Runtime Environment, el agente invitado y el agente de arranque de Software.

Qué hacer a continuación

En su hipervisor o proveedor de nube, convierta su máquina de referencia en una plantilla, un snapshot, o una imagen de máquina de Amazon que los arquitectos de la infraestructura puedan usar 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\agent_bootstrap_removal.bat  
c:\opt\vmware-appdirector\agent-bootstrap\agent_reset.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.

Prerequisitos

- 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](#) página 78
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](#) página 78
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](#) página 79
Cree una especificación de personalización que los arquitectos de blueprints puedan usar con la plantilla `cpb_centos_63_x84`.

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.

Qué hacer a continuación

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 [“Escenario: Crear un blueprint de CentOS de vSphere para clonar en Rainpole,”](#) página 369.

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`.

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**.

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**.

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. Deshabilita 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.

Prerequisitos

- Instale y configure por completo vRealize Automation. Consulte *Instalación y configuración de vRealize Automation para el escenario de Rainpole*.
- 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](#) página 81

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](#) página 81

Tras la instalación del agente invitado y el agente de arranque de software en la máquina de referencia, deshabilita 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](#) página 82

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

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 desde su 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.

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 el agente de arranque de software en la máquina de referencia, deshabilita 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 deshabilitar SELinux.


```
SELINUX=disabled
```

Si no deshabilita 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**.

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**.

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

Qué hacer a continuación

- 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,”](#) página 217.
- 2 Asigne el perfil de red externa a la reserva de vSphere. Consulte [“Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer,”](#) página 256. 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,”](#) página 306.

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
<input type="checkbox"/> 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 "Escenario: Crear cuentas de usuario local para Rainpole," página 158.
<input type="checkbox"/> 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," página 86
<input type="checkbox"/> 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," página 154
<input type="checkbox"/> (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," página 163
<input type="checkbox"/> (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," página 166
<input type="checkbox"/> (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," página 168
<input type="checkbox"/> (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 y complementos," página 180

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

Tarea	Función de vRealize Automation	Detalles
<input type="checkbox"/> (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,” página 179
<input type="checkbox"/> (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,” página 179.

Este capítulo cubre los siguientes temas:

- [“Elegir opciones de configuración de Administración de directorios,”](#) página 86
- [“Actualizar conectores externos para Administración de directorios,”](#) página 137
- [“Escenario: Configurar un vínculo de Active Directory para vRealize Automation de alta disponibilidad,”](#) página 144
- [“Configurar la autenticación de tarjetas inteligentes para vRealize Automation,”](#) página 146
- [“Crear un vínculo de Active Directory con varios dominios o bosques,”](#) página 152
- [“Configurar funciones de usuarios y grupos,”](#) página 154
- [“Escenario: Configurar el tenant predeterminado para Rainpole,”](#) página 158
- [“Crear tenants adicionales,”](#) página 163
- [“Eliminar un tenant,”](#) página 165
- [“Configurar la personalización de marca,”](#) página 166
- [“Lista de comprobación para la configuración de notificaciones,”](#) página 168
- [“Crear un archivo RDP personalizado para admitir conexiones RDP para máquinas aprovisionadas,”](#) página 179
- [“Escenario: Añadir ubicaciones de centros de datos para implementaciones en varias regiones,”](#) página 179
- [“Configurar vRealize Orchestrator y complementos,”](#) página 180

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,” página 90. 2 Si configuró vRealize Automation para una alta disponibilidad, consulte “Configurar Administración de directorios para alta disponibilidad,” página 99.
(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,” página 100
(Opcional) Añadir usuarios y grupos a un vínculo de Active Directory existente.	“Añadir usuarios o grupos a una conexión de Active Directory,” página 104.
(Opcional) Editar la política predeterminada para aplicar reglas personalizadas para un vínculo de Active Directory.	“Administrar la política de acceso de usuarios,” página 117.
(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,” página 129.

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,” página 90.</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. Todo el dispositivo de vRealize Automation contiene un conector de manera predeterminada. Consulte “Administración de conectores y clústeres de conectores,” página 108.</p>

Tabla 2-3. Configuración de la administración de directorios (Continúa)

Configuración	Descripción
Atributos de usuario	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,” página 105.
Rangos de redes	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,” página 129.
Proveedores de identidades	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 proveedores de identidades y que resulta suficiente para muchas de las necesidades del usuario. Puede añadir instancias de proveedor de identidades de terceros o combinar ambas. Consulte “Configurar una instancia del proveedor de identidades,” página 128.
Políticas	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,” página 117.

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 en el servicio la información de los usuarios y los grupos desde Active Directory o el directorio LDAP.
- 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: Si usa proveedores de identidades de terceros, puede configurar el conector para que sincronice los datos de usuarios y grupos o puede configurar el aprovisionamiento de usuarios Just-in-Time. Consulte la sección Aprovisionamiento de usuarios Just-in-Time del tema sobre la *administración de VMware Identity Manager* para obtener más información.

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 tiene su propio concepto de directorio, correspondiente a Active Directory o al directorio LDAP que se encuentra en su entorno. Este directorio utiliza atributos para definir los usuarios y los grupos.

■ Active Directory

- 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.

■ Directorio LDAP

El servicio no tiene acceso directo a Active Directory o al directorio LDAP. Solo el conector tiene acceso directo. 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 o el directorio LDAP y el servicio a través de uno o varios trabajos.

IMPORTANTE: No puede tener dos trabajos del tipo Active Directory con 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,”](#) página 90. 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,”](#) página 90. 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,”](#) página 90. 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,”](#) página 90. 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,”](#) página 94.

Prerequisitos

- 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,”](#) página 105.
- 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.
- 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.
- Inicie sesión en la consola de 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) .
LDAP	Seleccione Active Directory en LDAP .

- 5 Configure el conector que sincroniza usuarios desde Active Directory hacia el directorio de VMwareDirectories 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	<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 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	<ul style="list-style-type: none"> ■ 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. ■ 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>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> <ul style="list-style-type: none"> ■ 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.
Detalles de unión a dominio: se muestra cuando se selecciona Active Directory (Autenticación de Windows integrada)	Escriba las credenciales apropiadas en los cuadros de texto Nombre de dominio , Nombre de usuario administrador del dominio y Contraseña del administrador del dominio .

- 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 a Active Directory hasta los 24 GB.

- 15 Haga clic en **Siguiente**.

- 16 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.

- 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.

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,”](#) página 154 para obtener más información.

Qué hacer a continuación

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,”](#) página 99.

- 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

Prerequisitos

- 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>

- 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.
- Haga clic en **Guardar y Siguiente**.
- 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 deshabilita 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 deshabilita esta opción, asegúrese de que selecciona todos los grupos cuyos usuarios desee 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.

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,”](#) página 154 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 el 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 Administración de directorios, es necesario configurar un segundo conector que se corresponda con el segundo el dispositivo de vRealize Automation, que se conecta con el proveedor de identidades y apunta al mismo 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.

Prerequisitos

- Configure la implementación de vRealize Automation con, al menos, dos instancias del el dispositivo de vRealize Automation.
- Instale vRealize Automation en modo Enterprise utilizando un único dominio con dos instancias del el dispositivo de vRealize Automation.
- Instale y configure un equilibrador de carga adecuado para que funcione con la implementación de vRealize Automation.
- Configure tenants y Administración de directorios usando uno de los conectores proporcionados con las instancias instaladas del el dispositivo de vRealize Automation. Para obtener más información acerca de la configuración de tenants, consulte [Capítulo 2, “Configurar las opciones de tenant,”](#) página 85.

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 se corresponda con el el 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.

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.

Prerequisitos

- 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 la consola de 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.
 - a Seleccione **Administración > Administración de directorios > Proveedores de identidades**.
 - b 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.

- c Guarde el archivo de metadatos de administración de directorios con el nombre `sp.xml`.
 - d Haga clic en **Agregar**.
- 4 Añada una regla a la política predeterminada.
 - a Seleccione **Administración > Administración de directorios > Políticas**.
 - b Haga clic en el nombre de la política predeterminada.
 - c 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 el rango de redes del usuario es "**Mi máquina**" y el usuario necesita acceder a contenido de "**Todos los tipos de dispositivos**", en el caso de una implementación típica, ese usuario deberá autenticarse con el siguiente método: **Nombre de usuario y contraseña de ADFS**.
 - d Haga clic en **Guardar** para guardar los cambios en la política.
 - e 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. Una vez creada la regla, deberá editarla añadiéndole el siguiente texto:

```
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/spnamequalifie
r"] = "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).

Prerequisitos

- Configure tenants para su implementación de vRealize Automation. Consulte [“Crear tenants adicionales,”](#) página 163.
- Establezca un vínculo de Active Directory adecuado que admita la autenticación básica con identificador de usuario y contraseña de Active Directory.
- Inicie sesión en la consola de 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	Seleccione los rangos de redes a los que desea que los usuarios tengan privilegios de acceso. Si desea autenticar usuarios desde una dirección IP, seleccione Todos los rangos .
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 del usuario de Administración de directorios importa datos de Active Directory cuando se añaden grupos y usuarios y la velocidad del sistema está limitada por las capacidades 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 se ve reducido o si se producen errores, cierre las aplicaciones que no sean necesarias y asegúrese de que su implementación tenga asignada a Active Directory la memoria adecuada. Si los problemas persisten, aumente la asignación de memoria a Active Directory según sea necesario. Para implementaciones con grandes números de usuarios y grupos, quizás deba aumentar la asignación de memoria de Active Directory hasta 24 GB.

Al ejecutar una operación de sincronización para una implementación de vRealize Automation con muchos usuarios y grupos, es probable que haya una demora después de que desaparezca el mensaje Sincronización en curso antes de que se muestren los detalles del log de sincronización. Además, la marca de hora del archivo de registro puede diferir de la hora que la interfaz de usuario indica como aquella en la que se completó la operación de sincronización.

NOTA: Las operaciones de sincronización no pueden cancelarse una vez iniciadas.

Prerequisitos

- Conector instalado y con el código de activación activado. Seleccione los atributos predeterminados necesarios y añada atributos adicionales a la página Atributos de usuario.
- 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.
- Para la Autenticación de Windows integrada de Active Directory, cuando se tiene configurado Active Directory con varios bosques y el grupo local de dominios contiene miembros de dominios de diferentes bosques, asegúrese de que el usuario de enlace se añada al grupo de Administradores del dominio en el que reside el grupo local de dominios. De lo contrario, estos miembros no estarán en el grupo local de dominios.
- Inicie sesión en la consola de 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 nueva 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 nueva 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 sincronizar para realizar las actualizaciones inmediatamente o bien haga clic en **Guardar y sincronizar** para guardar los cambios y sincronizar para implementar las actualizaciones inmediatamente.

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,”](#) página 107.

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**.

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 a el dispositivo de vRealize Automation. En la siguiente tabla se muestran las asignaciones de memoria para los respectivos componentes.

Tabla 2-5. Asignar memoria de el 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.

Prerequisitos

- 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 el 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 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`.

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 realizan y guardan en la página Atributos de usuario se añaden 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 se pueden asignar a atributos de Active Directory. Seleccione los atributos que sean obligatorios; también puede añadir otros atributos de Active Directory que desee para 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
<code>userPrincipalName</code>	<code>userPrincipalName</code>
<code>distinguishedName</code>	<code>distinguishedName</code>
<code>employeeId</code>	<code>employeeID</code>
<code>domain</code>	<code>canonicalName</code> . Añade el nombre de dominio completo del objeto.
<code>disabled</code> (usuario externo deshabilitado)	<code>userAccountControl</code> . Marcado con <code>UF_Account_Disable</code> 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.
<code>phone</code>	<code>telephoneNumber</code>
<code>lastName</code>	<code>sn</code>
<code>firstName</code>	<code>givenName</code>
<code>email</code>	<code>mail</code>
<code>userName</code>	<code>sAMAccountName</code>

En la página Atributos de usuario, se muestran los atributos de directorio predeterminados que se pueden asignar a atributos de Active Directory. Seleccione los atributos que sean obligatorios; también puede añadir otros atributos de Active Directory que desee para 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
<code>userPrincipalName</code>	<code>userPrincipalName</code>
<code>distinguishedName</code>	<code>distinguishedName</code>
<code>employeeId</code>	<code>employeeID</code>

Tabla 2-7. Atributos de Active Directory predeterminados para sincronizar con el directorio (Continúa)

Nombre del atributo de directorio	Asignación predeterminada al atributo de Active Directory
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

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 el 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,”](#) página 118.
- En la columna Proveedor de identidades, seleccione la IdP para ver, editar o desactivar. Consulte [“Configurar una instancia del proveedor de identidades,”](#) página 128.
- 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 dominio, 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](#) página 112

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`](#) página 112

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`](#) página 113

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,”](#) página 110.

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 dominio 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,”](#) página 131. 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 autenticquen 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 autenticquen 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,”](#) página 117.

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.

*** Nombre de directiva** default_access_policy_set DIRECTIVA PREDETERMINADA

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 añada 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 Applications
To be applied to Web applications that should have limited access.

Policy Name* Sensitive Web Applications

Description To be applied to Web applications that should have limited access.

Applies To Select the Web applications from your Catalog that this policy applies to.
AirWatch
Content Locker Edit Apps

Policy Rules

Network Range	Device type	Authentication Method	Re-authenticate (Hours)	
Internal Network	Web Browser	First, try: Kerberos and 1 more...	8	✗ +
ALL RANGES	Web Browser	SecurID	4	✗ +

- 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, ya 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.

Prerequisitos

- Seleccione o configure los proveedores de identidades apropiados para su implementación. Consulte [“Configurar una instancia del proveedor de identidades,”](#) página 128.
- Configure los rangos de redes apropiados para su implementación. Consulte [“Añadir o editar un rango de redes,”](#) página 129.
- Configure los métodos de autenticación apropiados para su implementación. Consulte [“Integrar productos de autenticación de usuario alternativos con Administración de directorios,”](#) página 118.
- 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 la consola de 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**.

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.

Tabla 2-8. Tipos de autenticación de usuario admitidos por Administración de directorios (Continúa)

Tipos de autenticación	Descripción
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** página 120

El servidor RSA SecurID debe configurarse con información acerca del dispositivo del 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** página 120

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 del 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.

Prerequisitos

- 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 del 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 el conector de Directories Management 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 es 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 de Directories Management.

Qué hacer a continuación

Vaya a la consola de administración 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.

Prerequisitos

- 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 **SecurIDdpAdapter**.
Se le redirige a la página de inicio de sesión del administrador de identidades.

- 4 En la página Adaptadores de autenticación, en la fila SecurIDdpAdapter, 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**.

Qué hacer a continuación

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,”](#) página 122.

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.

Prerequisitos

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 la consola de 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.
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**.

Qué hacer a continuación

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](#) página 124
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 de Directories Management deben poseer un UPN válido que se corresponda con el UPN en el certificado.
- [Entidad de certificación necesaria para la autenticación](#) página 125
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](#) página 125
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](#) página 126
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 de Directories Management deben poseer un UPN válido que se corresponda con el UPN en el certificado.

Puede configurar el de 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.

Prerequisitos

- 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 lista de revocación de certificados y 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 requiere 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 Configure la página Adaptador de autenticación de certificado.

NOTA: Un asterisco indica que la información es obligatoria.

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.
Certificados de CA cargados	Los archivos de certificado cargados aparecen en la sección Certificados de CA cargados del formulario.
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	Cree una lista de los identificadores de objeto que se aceptan en las extensiones de las políticas de certificados. 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.
Habilitar revocación de certificados	Active esta casilla para habilitar la comprobación de revocación de certificados. La comprobación de la revocación de certificados 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.

Opción	Descripción
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 CRL y OCSP. Seleccione esta casilla de verificación para usar 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.

5 Haga clic en **Guardar**.

Qué hacer a continuación

- 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 instancia del proveedor de identidades

vRealize Automation se proporciona con una instancia predeterminada del proveedor de identidades. Es posible que los usuarios deseen crear otras instancias del proveedor de identidades.

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.

Prerequisitos

- 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,”](#) página 129.
- Acceda al documento de metadatos de terceros. Puede ser la dirección URL de los metadatos o los propios metadatos.
- Inicie sesión en la consola de vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 Vaya a **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** y edite la configuración de la instancia del proveedor de identidades.

Elemento del formulario	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.
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>

Elemento del formulario	Descripción
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.
Hostname	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.

3 Haga clic en **Agregar**.

Qué hacer a continuación

- 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 inician 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.

Prerequisitos

- 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 la consola de 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.
Ver Pods	La opción Ver Pods solo aparece cuando está habilitado el módulo Ver. Host de URL de acceso de cliente. Escriba la URL de acceso de Horizon Client para el rango de redes. Puerto de acceso de cliente. Escriba el número de puerto de acceso de Horizon Client para el rango de redes.
Rangos de IP	Edite o añada rangos de IP hasta que se hayan incluido todas las direcciones IP deseadas y excluido las no deseadas.

Qué hacer a continuación

- 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,”](#) página 114.

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,”](#) página 107.

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**.

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,”](#) página 113.

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.

Prerequisitos

Habilite y configure los métodos de autenticación que su organización admita. Consulte [“Integrar productos de autenticación de usuario alternativos con Administración de directorios,”](#) página 118

Procedimiento

- 1 Seleccione **Administración > Administración de directorios > Políticas**
- 2 Haga clic en la política de acceso predeterminada para editarla.
- 3 Para abrir y editar una página de reglas de directiva, haga clic en el nombre de autenticación en la columna Método de autenticación, o bien haga clic en el icono + para agregar una nueva regla de directiva.
 - a Compruebe que el rango de redes sea el correcto. Si va a agregar una nueva regla, seleccione el rango de redes para esta regla de directiva.
 - b Seleccione el tipo de dispositivo que administrará esta regla en el menú desplegable **y el usuario intenta acceder a contenido con...**
 - c Configure el orden de autenticación. En el menú desplegable **entonces el usuario debe autenticarse con el siguiente método**, seleccione el método de autenticación que se aplicará en primer lugar.
Para requerir que los usuarios se autenticuen mediante dos métodos de autenticación, haga clic en + y escriba un segundo método de autenticación.
 - d (Opcional) Para configurar métodos de autenticación adicionales por si el primero no funciona, seleccione otro método de autenticación habilitado en el siguiente menú desplegable.
Puede añadir varios métodos de autenticación de reserva a una regla.
 - e En el cuadro de texto **Volver a autenticar después de** valor, introduzca el número de horas que deberán transcurrir para que el usuario se tenga que autenticar de nuevo.
 - f (Opcional) Cree un mensaje de error personalizado de acceso denegado que se muestra cuando falla la autenticación del usuario. Puede usar hasta 4000 caracteres, unas 650 palabras. Si desea enviar a los usuarios a otra página, agregue el vínculo de la URL en el cuadro de texto **URL del enlace**. En el cuadro de texto **Texto del enlace**, introduzca el texto que se mostrará para el vínculo. Si deja este cuadro de texto en blanco, se mostrará la palabra Continuar.
 - g Haga clic en **Guardar**.

- Haga clic en **Guardar**.

Editar regla de directivas

- 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](#) página 133

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](#) página 134

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](#) página 136

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](#) página 136

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

- Como administrador de tenants, navegue a **Administración > Administración de directorios > Conectores**
- 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.
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**.

Qué hacer a continuación

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.

Prerequisitos

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.

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.

Prerequisitos

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.

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.

Prerequisitos

- 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.

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](#) página 137
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](#) página 138
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.hzn updateinstaller`
- 3 Ejecute el comando siguiente para comprobar si existe una actualización en línea.
`/usr/local/horizon/update/updatemgr.hzn check`

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.

Prerequisitos

- 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`

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.

Prerequisitos

- 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.hzn updateinstaller`
- 3 Ejecute el comando siguiente para comprobar si existe una actualización en línea.
`/usr/local/horizon/update/updatemgr.hzn check`
- 4 Ejecute el comando siguiente para actualizar el dispositivo.
`/usr/local/horizon/update/updatemgr.hzn update`
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.hzn check`
- 6 Compruebe la versión del dispositivo actualizado.
`vamcli 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.

Prerequisitos

- 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](#) página 140
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](#) página 140
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.

Prerequisitos

- 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/updatesLocal.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.

Prerequisitos

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/updateslocal.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/updateslocal.hzn setdefault
```

- 3 Realice la actualización.

- a Ejecute el siguiente comando.

```
/usr/local/horizon/update/updatesmgr.hzn updateinstaller
```

- b Ejecute el comando siguiente para comprobar la versión de la actualización disponible.

```
/usr/local/horizon/update/updatesmgr.hzn check
```

- c Ejecute el comando siguiente para actualizar el conector.

```
/usr/local/horizon/update/updatesmgr.hzn update
```

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 `updatesmgr.hzn check`.

```
/usr/local/horizon/update/updatesmgr.hzn check
```

- 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
```

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,”](#) página 109 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,”](#) página 110 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](#) página 142
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](#) página 143
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](#) página 143
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)	<code>/opt/vmware/horizon/workspace/logs/catalina.log</code>	Apache Tomcat registra los mensajes que no se registran en otros archivos de registro.
Registros del configurador (configurator.log)	<code>/opt/vmware/horizon/workspace/logs/configurator.log</code>	Solicitudes que recibe el configurador del cliente REST y de la interfaz web.
Registros del conector (connector.log)	<code>/opt/vmware/horizon/workspace/logs/connector.log</code>	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 el 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 Administración de directorios, es necesario configurar un segundo conector que se corresponda con el segundo el dispositivo de vRealize Automation, que se conecta con el proveedor de identidades y apunta al mismo 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.

Prerequisitos

- Instale una implementación de vRealize Automation distribuida con los equilibradores de carga adecuados. Consulte *Instalación de vRealize Automation 7.2*.
- Inicie sesión en la consola de 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 el 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 .
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 el 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.

Previamente conectó el Active Directory corporativo a vRealize Automation y configuró la administración de directorios para la alta disponibilidad.

Qué hacer a continuación

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,”](#) página 100.

Configurar la autenticación de tarjetas inteligentes para vRealize Automation

Como administrador del sistema, debe configurar la autenticación de tarjetas inteligentes para la implementación de vRealize Automation mediante la administración de directorios.

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, 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.

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,”](#) página 124.

Prerequisitos

- 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 la consola de vRealize Automation como **administrador de tenants**.

Procedimiento

- 1 [Generar un token de activación del conector](#) página 147
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](#) página 147
Tras descargar un archivo OVA del conector, puede implementarlo mediante VMware vSphere Client o vSphere Web Client.
- 3 [Configurar los ajustes del conector](#) página 148
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](#) página 149
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](#) página 151
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](#) página 151
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.

Prerequisitos

- Inicie sesión en la consola de 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.

Prerequisitos

- 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.

Página	Descripción
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	<ol style="list-style-type: none"> En el campo Configuración de zona horaria, seleccione la zona horaria correcta. 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. 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. 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. IMPORTANTE: Si se deja en blanco cualquiera de los cuatro campos de dirección, incluido Nombre del host, se usará DHCP. Para configurar DHCP, deje los campos de dirección en blanco.
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.

Qué hacer a continuación

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.

Prerequisitos

- 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.

Qué hacer a continuación

En el servicio, configure el entorno en función de sus necesidades. Por ejemplo, si ha añadido un conector adicional debido a que desea sincronizar dos directorios de autenticación integrada de Windows, cree el directorio y asícielo 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.

NOTA: Si el Directories Management del apunta a un equilibrador de carga, el certificado SSL se aplicará a este último.

Prerequisitos

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 de administración, haga clic en **Configuración del dispositivo**.
La configuración de la VA se selecciona de forma predeterminada.

- 3 Haga clic en **Administrar configuración**.
- 4 En el cuadro de diálogo que se abrirá, escriba la contraseña de usuario administrador del servidor de Directories Management.
- 5 Seleccione **Instalar certificado**.
- 6 En la pestaña Finalizar SSL en el dispositivo de Identity Manager, 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+O05j5xsxzDJfWr1lqBIFf/OkIYCPcyK1

-----END CERTIFICATE-----

-----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.

Prerequisitos

- Inicie sesión en la consola de 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.

Prerequisitos

Inicie sesión en la consola de 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,”](#) página 126.
- 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.

Prerequisitos

- Instale una implementación de vRealize Automation distribuida con los equilibradores de carga adecuados. Consulte *Instalación de vRealize Automation 7.2*.
- Inicie sesión en la consola de 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 VMwareDirectories 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 el 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.

Qué hacer a continuación

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.

Prerequisitos

Inicie sesión en la consola de 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 Haga clic en **Actualizar**.

Los usuarios que han iniciado sesión en la consola de vRealize Automation deben cerrar la sesión de la consola de vRealize Automation y volver a iniciarla antes de poder navegar a las páginas a las que se les ha concedido acceso.

Qué hacer a continuación

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,”](#) página 154.

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.

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.

Prerequisitos

Inicie sesión en la consola de 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**.

Los usuarios que han iniciado sesión en la consola de vRealize Automation deben cerrar la sesión de la consola de vRealize Automation y volver a iniciarla antes de poder navegar a las páginas a las que se les ha concedido acceso.

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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 300. 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,”](#) página 207. 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.
Enviar correos electrónicos del administrador a	Introduzca uno o varios nombres de usuario o nombres de grupo. Separe varias entradas con una coma. Por ejemplo, JoeAdmin@mycompany.com, WeiMgr@mycompany.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 usuario con acceso compartido	Puede solicitar y administrar elementos del catálogo de servicios. Los usuarios con esta función no pueden realizar solicitudes en nombre de otros miembros del grupo empresarial. Esta función permite que el usuario comparta una implementación con su equipo, y permite a los usuarios con los que se ha compartido el acceso ejecutar acciones en la implementación.
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	<p>Seleccione un prefijo de máquina preconfigurado para el grupo empresarial.</p> <p>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.</p> <p>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.</p>
Contenedor de Active Directory	<p>Especifique un contenedor de Active Directory. Esta opción solo se aplica al aprovisionamiento de WIM.</p> <p>Otros métodos de aprovisionamiento precisan de más configuración para unir las máquinas aprovisionadas a un contenedor de AD.</p>

8 Haga clic en **Agregar**.

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.

Qué hacer a continuación

- Cree una reserva para su grupo empresarial basada en el lugar en que el grupo empresarial aprovisiona máquinas. Consulte [“Elegir un escenario de reserva,”](#) página 228.
- 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,”](#) página 472.

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.

Origen

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.

Escenario: Configurar el tenant predeterminado para Rainpole

Como administrador del sistema, desea configurar la instancia de vRealize Automation como un entorno de desarrollo continuo. Cree cuentas de usuario local y asígnese la función de administrador de tenant. Use los privilegios de administrador de tenant para empezar a configurar vRealize Automation como un entorno de desarrollo para crear y probar blueprints.



Procedimiento

- 1 [Escenario: Crear cuentas de usuario local para Rainpole](#) página 158
Puede usar sus privilegios de administrador del sistema predeterminado para crear dos cuentas de usuario locales en el tenant predeterminado. Asigne una de estas cuentas a la función de administrador de tenant para comenzar a configurar el tenant predeterminado. Más adelante, podrá usar la otra cuenta como inicio de sesión compartido para que los arquitectos prueben el acceso a los blueprints y al catálogo.
- 2 [Escenario: Configurar su Active Directory corporativo para vRealize Automation para Rainpole](#) página 160
Como administrador de tenant, desea que vRealize Automation autentique los inicios de sesión en el Active Directory corporativo. Configure una conexión entre vRealize Automation y el Active Directory de un solo dominio a través de LDAP.
- 3 [Escenario: Configurar personalización de marca para el tenant predeterminado para Rainpole](#) página 161
Con sus privilegios de administrador de tenants, personalice la apariencia de la consola de vRealize Automation. Cargue un nuevo logotipo, cambie los colores, actualice la información del encabezado y pie de página y configure la personalización de marca de pantalla de inicio de sesión.
- 4 [Escenario: Crear un grupo personalizado para los arquitectos de Rainpole](#) página 161
Use sus privilegios de administrador de tenant para crear un grupo personalizado para los miembros de la organización de TI que necesiten acceder con privilegios elevados a vRealize Automation. Asigne funciones en este grupo personalizado a medida que configura vRealize Automation.
- 5 [Escenario: Asignar privilegios de administrador de IaaS a su grupo personalizado de arquitectos de Rainpole](#) página 162
Con los privilegios de administrador del sistema predeterminados, asigne su grupo personalizado a la función de administrador de IaaS para permitir que el grupo configure los recursos de IaaS.

Escenario: Crear cuentas de usuario local para Rainpole

Puede usar sus privilegios de administrador del sistema predeterminado para crear dos cuentas de usuario locales en el tenant predeterminado. Asigne una de estas cuentas a la función de administrador de tenant para comenzar a configurar el tenant predeterminado. Más adelante, podrá usar la otra cuenta como inicio de sesión compartido para que los arquitectos prueben el acceso a los blueprints y al catálogo.

Procedimiento

- 1 Vaya a la consola de vRealize Automation, <https://vra01svr01.rainpole.local/vcac>.

- 2 Escriba el nombre de usuario del administrador del sistema predeterminado **administrator** y la contraseña **VMware1!**.
- 3 Seleccione **Administración > Tenants**.
- 4 Haga clic en **vsphere.local**.
- 5 Seleccione la pestaña **Usuarios locales**.
- 6 Haga clic en el icono **Nuevo (+)**.
- 7 Cree una cuenta de usuario local para asignarle la función de administrador de tenants.

Opción	Entrada
Nombre	Rainpole
Apellido	tenant admin
Correo electrónico	Escriba la dirección de correo electrónico o use el marcador de posición rainpole_tenant_admin@rainpole.com .
Nombre de usuario	Administrador de tenants de Rainpole
Contraseña	VMware1!

- 8 Haga clic en **Aceptar**.
- 9 Haga clic en el icono **Nuevo (+)**.
- 10 Cree una cuenta de usuario local que tanto usted como los arquitectos pueden configurar más tarde para probar el acceso a los blueprints y al catálogo.

Opción	Entrada
Nombre	test
Apellido	user
Correo electrónico	Escriba una dirección de correo electrónico o use el marcador de posición test_user@rainpole.com .
Nombre de usuario	test_user
Contraseña	VMware1!

- 11 Haga clic en **Aceptar**.
- 12 Haga clic en la pestaña **Administradores**.
- 13 Escriba **Rainpole** en el cuadro de texto **Administradores de tenants** y pulse Intro. Seleccione el usuario administrador de tenant de Rainpole.
La función de administrador de tenant se asigna al usuario administrador de tenant de Rainpole.
- 14 Haga clic en **Finalizar**.
- 15 Cierre sesión en la consola.

Puede utilizar el usuario administrador de tenant local de Rainpole para acceder a la configuración de administración de tenants y configurar el tenant. La cuenta **test_user** es útil como inicio de sesión compartido para los arquitectos y los administradores del catálogo. Estos pueden configurar la cuenta como un usuario básico para comprobar el acceso a los blueprints y al catálogo, así como para comportamientos de aprobación de pruebas.

Qué hacer a continuación

Configure vRealize Automation para autenticar inicios de sesión en el Active Directory corporativo actual.

Escenario: Configurar su Active Directory corporativo para vRealize Automation para Rainpole

Como administrador de tenant, desea que vRealize Automation autentique los inicios de sesión en el Active Directory corporativo. Configure una conexión entre vRealize Automation y el Active Directory de un solo dominio a través de LDAP.

Procedimiento

- 1 Vaya a la consola de vRealize Automation, <https://vra01svr01.rainpole.local/vcac>.
- 2 Escriba el nombre de usuario **Administrador de tenants de Rainpole** y la contraseña **VMware1!**.
- 3 Seleccione **Administración > Administración de directorios > Directorios**.
- 4 Haga clic en **Añadir directorio**.
- 5 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	vra01svr01.rainpole.local
DN de la base	Escriba el nombre distintivo (DN) del punto de inicio de las búsquedas en el servidor de directorios. Por ejemplo, cn=users,dc=rainpole,dc=local .
DN de enlace	Escriba el nombre distintivo (DN) completo, incluido el nombre común (CN), de una cuenta de usuario de Active Directory que tenga privilegios para buscar usuarios. Por ejemplo, cn=config_admin_infra,cn=users,dc=rainpole,dc=local .
Contraseña de DN de enlace	Escriba la contraseña de Active Directory para la cuenta que puede buscar usuarios.

- 6 Haga clic en el botón **Probar conexión** para probar la conexión con el directorio configurado.
- 7 Haga clic en **Guardar y Siguiente**.
Aparece la página de selección de dominios, que contiene una lista de dominios.
- 8 Acepte la configuración de dominio predeterminada y haga clic en **Siguiente**.
- 9 Compruebe que los nombres de atributo estén asignados a los atributos de Active Directory correctos y haga clic en **Siguiente**.
- 10 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=rainpole,dc=local**.
 - c Active la casilla **Seleccionar todo**.
 - d Haga clic en **Seleccionar**.
 - e Haga clic en **Siguiente**.
 - f Acepte los valores predeterminados de la página Seleccionar usuarios y haga clic en **Siguiente**.

- 11 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.

Puede asignar privilegios y otorgar acceso a cualquier usuario y grupo de Active Directory que haya sincronizado para vRealize Automation.

Qué hacer a continuación

Use sus privilegios de administrador de tenant para personalizar el aspecto de la consola de vRealize Automation.

Escenario: Configurar personalización de marca para el tenant predeterminado para Rainpole

Con sus privilegios de administrador de tenants, personalice la apariencia de la consola de vRealize Automation. Cargue un nuevo logotipo, cambie los colores, actualice la información del encabezado y pie de página y configure la personalización de marca de pantalla de inicio de sesión.

Procedimiento

- 1 Seleccione **Administración > Personalización de marca > Personalización de marca de encabezado y pie de página**.
- 2 Desactive la casilla **Usar predeterminado**.
- 3 Siga las indicaciones para crear un encabezado.
- 4 Haga clic en **Siguiente**.
- 5 Siga las indicaciones para crear un pie de página.
- 6 Haga clic en **Finalizar**.

La consola se actualizará con los cambios realizados.

- 7 Seleccione **Administración > Personalización de marca > Personalización de marca de pantalla de inicio de sesión**.
- 8 Siga las indicaciones para adaptar la personalización de marca de pantalla de inicio de sesión.
- 9 Haga clic en **Guardar**.

La consola se actualizará con los cambios realizados.

Ha actualizado la apariencia de la consola para el tenant predeterminado.

Qué hacer a continuación

Cree un grupo personalizado de miembros de su organización de TI que necesiten acceso de privilegio alto a vRealize Automation.

Escenario: Crear un grupo personalizado para los arquitectos de Rainpole

Use sus privilegios de administrador de tenant para crear un grupo personalizado para los miembros de la organización de TI que necesiten acceder con privilegios elevados a vRealize Automation. Asigne funciones en este grupo personalizado a medida que configura vRealize Automation.

Si desea añadir o deshabilitar el acceso de nivel elevado para los usuarios, puede cambiar la pertenencia al grupo en lugar de tener que editar la configuración de cada usuario en varias ubicaciones.

Procedimiento

- 1 Seleccione **Administración > Usuarios y grupos > Grupos personalizados**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Escriba **Rainpole architects** en el cuadro de texto **Nombre**.
- 4 Seleccione las funciones de la lista **Añada funciones a este grupo**.

En esta página no se pueden asignar funciones de administrador de IaaS, administrador de tejidos, administrador de grupo empresarial ni usuario empresarial. Puede asignar estas funciones mientras configura vRealize Automation.

Opción	Descripción
Administrador de tenants	Se encarga de la administración de usuarios y grupos, la personalización de marca, las notificaciones de los tenants y las políticas empresariales, como las aprobaciones y las autorizaciones. También lleva el seguimiento del uso de los recursos por parte de todos los usuarios del tenant e inicia solicitudes de recuperación para las máquinas virtuales.
Arquitecto de infraestructura (IaaS)	Crea y administra blueprints de máquina y de aplicación.
Arquitecto de XaaS	Para usuarios con licencia Advanced y Enterprise, se encarga de crear y administrar blueprints de XaaS.
Arquitecto de software	Para usuarios con licencia Enterprise, se encarga de crear y administrar componentes de software y blueprints de aplicación.

- 5 Haga clic en **Siguiente**.
- 6 Busque usuarios corporativos de Active Directory y seleccione los usuarios para añadirlos al grupo personalizado.

Asigne a este grupo todo aquel usuario que necesite un acceso de nivel muy elevado al entorno de desarrollo de vRealize Automation, incluido usted mismo.

- 7 Haga clic en **Finalizar**.

Ha otorgado al grupo personalizado los derechos para administrar el tenant predeterminado, crear blueprints y administrar el catálogo de servicios. Cuando configure vRealize Automation, añada permisos y funciones al grupo personalizado.

Qué hacer a continuación

Asigne el grupo personalizado a la función de administrador de IaaS.

Escenario: Asignar privilegios de administrador de IaaS a su grupo personalizado de arquitectos de Rainpole

Con los privilegios de administrador del sistema predeterminados, asigne su grupo personalizado a la función de administrador de IaaS para permitir que el grupo configure los recursos de IaaS.

Procedimiento

- 1 Cierre la sesión la consola de vRealize Automation.
- 2 Seleccione el dominio **vsphere.local** y haga clic en **Siguiente**.
- 3 Escriba el nombre de usuario del administrador del sistema predeterminado **administrator** y la contraseña **vmware**.
- 4 Seleccione **Administración > Tenants**.
- 5 Haga clic en el nombre de tenant predeterminado **vsphere.local**.

- 6 Haga clic en la pestaña **Administradores**.
- 7 Busque **Arquitectos de Rainpole** en el cuadro de texto **Administradores de IaaS** y seleccione su grupo personalizado.
- 8 Haga clic en **Finalizar**.
- 9 Cierre sesión en la consola.

Cualquier miembro de su grupo personalizado ahora puede administrar la infraestructura de almacenamiento, red, virtual y de nube para todos los tenants de su instancia de vRealize Automation. Puede actualizar su membresía de grupo en cualquier momento para otorgar o revocar estos privilegios.

Qué hacer a continuación

Mediante el uso de los privilegios de administrador de IaaS que otorgó a su grupo personalizado, puede configurar sus recursos de IaaS.

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.

Prerequisitos

Inicie sesión en la consola de vRealize Automation como **administrador del sistema**.

Procedimiento

- 1 [Especificar la información de tenant](#) página 164
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 [Configurar usuarios locales](#) página 164
El administrador del sistema de vRealize Automation debe configurar usuarios locales para cada tenant aplicable.
- 3 [Asignar administradores](#) página 165
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.

Prerequisitos

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.

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.

Prerequisitos

- Para poder asignar administradores de IaaS, debe instalar IaaS. Para obtener más información sobre cómo instalar IaaS, consulte *Instalación de vRealize Automation 7.2*.

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.

Prerequisitos

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**.

El tenant se eliminará de la implementación de vRealize Automation.

(Opcional) 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.

Prerequisitos

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.

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.

Prerequisitos

Si desea usar un logotipo personalizado con su personalización de marca, debe tener un archivo de imagen del logotipo.

Procedimiento

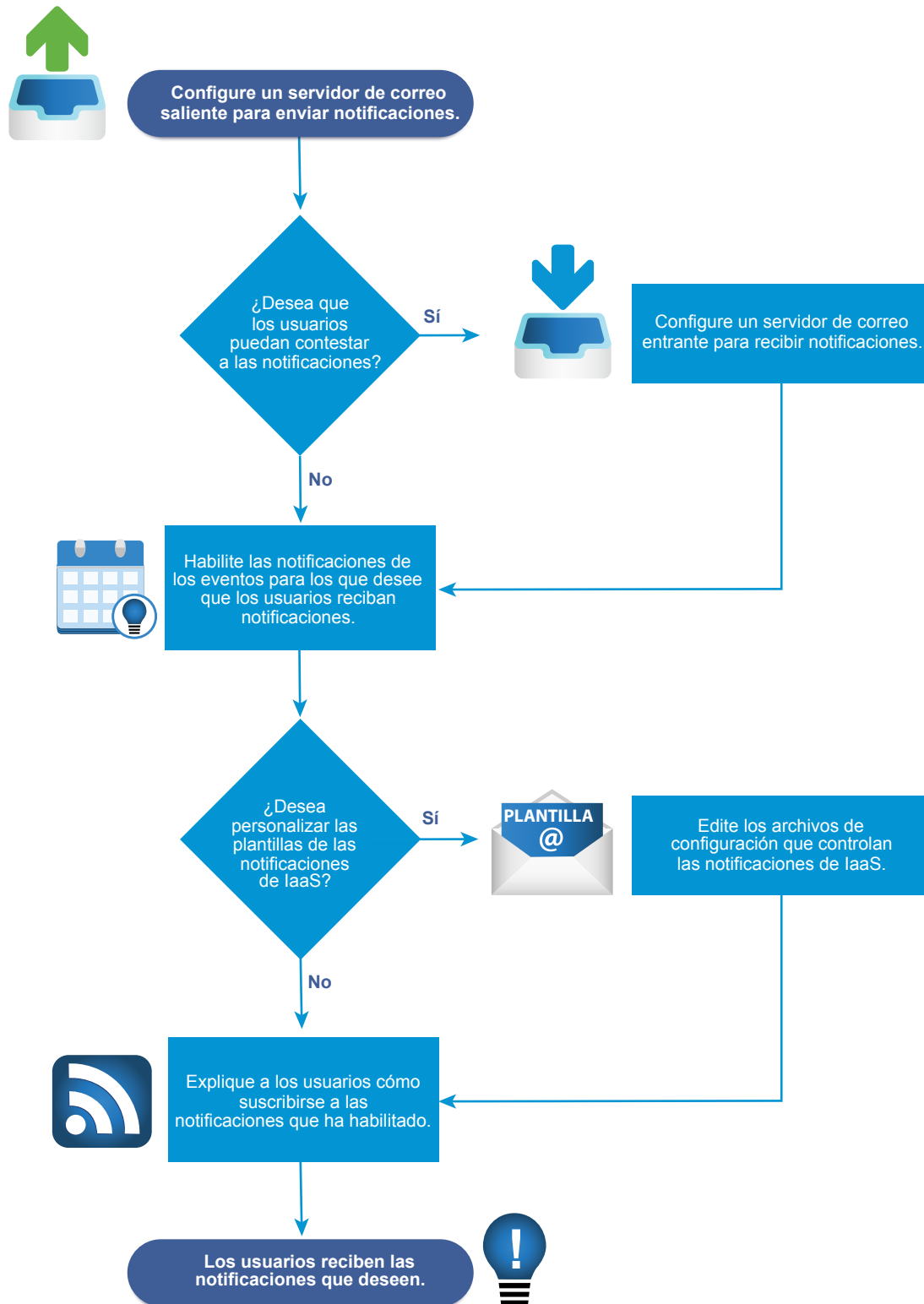
- 1 Inicie sesión en vRealize Automation como administrador del sistema o administrador de tenants.
- 2 Haga clic en la pestaña **Administración**.
- 3 Seleccione **Personalización de marca > Personalización de marca de aplicación**
- 4 Haga clic en la pestaña **Encabezado** si no está activa.
- 5 Si 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.

Los usuarios del tenant verán la personalización de marca en sus páginas de aplicación.

(Opcional) 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,” página 173. Si necesita reemplazar un servidor global predeterminado, consulte “Reemplazar un servidor de correo electrónico saliente predeterminado de sistema,” página 175. Para configurar servidores globales predeterminados para todos los tenants, consulte “Crear un servidor de correo electrónico saliente global,” página 172.</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,” página 174. Si necesita reemplazar un servidor global predeterminado, consulte “Reemplazar un servidor de correo electrónico entrante predeterminado de sistema,” página 176. Para configurar un servidor global predeterminado para todos los tenants, consulte “Crear un servidor de correo electrónico entrante global,” página 171.</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,” página 177.
<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,” página 177.

Tabla 2-10. Lista de comprobación para la configuración de notificaciones (Continúa)

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%\Program Files\VMware\VCAServer) puede configurar las plantillas de estas notificaciones de correo electrónico.	Consulte “Configurar plantillas para correos electrónicos de IaaS automáticos,” página 178.
<input type="checkbox"/> Proporcionar a los usuarios instrucciones acerca de 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,” página 178.

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.

Prerequisitos

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.

Prerequisitos

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,”](#) página 175.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 176.

Prerequisitos

- Inicie sesión en la consola de 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.

Prerequisitos

Inicie sesión en la consola de 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.

Prerequisitos

Inicie sesión en la consola de 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.

Prerequisitos

Inicie sesión en la consola de 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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 173.

Procedimiento

- 1 Seleccione **Administración > Notificaciones > Escenarios**.
- 2 Seleccione una o varias notificaciones.
- 3 Haga clic en **Activar**.

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
```

Qué hacer a continuación

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 han configurado las notificaciones, puede suscribirse para recibir notificaciones de vRealize Automation. Los eventos de notificaciones pueden ser la finalización correcta de una solicitud del catálogo o una aprobación necesaria.

Prerequisitos

Inicie sesión en la consola de 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**.

(Opcional) 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.

Prerequisitos

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\Website\Rdp`.

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,”](#) página 374.

(Opcional) 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.



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.

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,”](#) página 268.

Qué hacer a continuación

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 y complementos

VMware 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.

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.

Privilegios de configuración

Los administradores del sistema y de tenants pueden configurar vRealize Automation para utilizar un servidor externo 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.

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.

Prerequisitos

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**.

De este modo, ha definido la carpeta predeterminada de flujo de trabajo de vRealize Orchestrator de un tenant.

Qué hacer a continuación

Repita este procedimiento con todos los tenants para los que quiera definir una carpeta de flujo de trabajo predeterminada.

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 de servidor de vRealize Orchestrator externo 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.

Prerequisitos

- Instale y configure un servidor de vRealize Orchestrator externo. También puede implementar el dispositivo de vRealize Orchestrator. Consulte *Instalación y configuración de VMware vCenter Orchestrator*.
- Inicie sesión en la consola de vRealize Automation como **administrador del sistema** o **administrador de tenants**.

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**.
- 5 Escriba el número de puerto para la comunicación con el servidor de vRealize Orchestrator externo en el cuadro de texto **Puerto**.
8281 es el puerto predeterminado para vRealize Orchestrator.
- 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 aplicable si ha configurado vRealize Orchestrator y vRealize Automation para que utilicen 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 **Actualizar**.

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.

Qué hacer a continuación

Configure los complementos de vRealize Orchestrator como endpoints. Consulte [“Configurar recursos de XaaS,”](#) página 270.

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 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 de el dispositivo de vRealize Automation como raíz.
 - b Escriba **service vco-configurator start** y presione Entrar.
- 2 Vaya a la consola de administración de el dispositivo de vRealize Automation utilizando su nombre de dominio completo, <https://vra-vr-hostname.domain.name>.
- 3 Haga clic en **Centro de control de vRealize Orchestrator**.
Se le redirigirá a <https://vra-vr-hostname.domain.name:8283/vco-controlcenter>.
- 4 Inicie sesión en el centro de control de vRealize Orchestrator.
El nombre de usuario viene configurado por el administrador de el dispositivo de vRealize Automation.
- 5 (Opcional) Si es la primera vez que inicia sesión, cambie la contraseña predeterminada y haga clic en **Aplicar cambios**.
La nueva contraseña debe ser de ocho caracteres como mínimo y tener al menos un dígito, un carácter especial y una letra mayúscula.

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 Vaya a la consola de administración de el dispositivo de vRealize Automation utilizando su nombre de dominio completo, <https://vra-vr-hostname.domain.name>.
- 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 de el 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 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*.

Qué hacer a continuación

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 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.

Este capítulo cubre los siguientes temas:

- [“Lista de comprobación para la configuración de recursos de IaaS,”](#) página 185
- [“Configurar recursos de XaaS,”](#) página 270
- [“Crear y configurar contenedores,”](#) página 280
- [“Instalar complementos adicionales en el servidor predeterminado de vRealize Orchestrator,”](#) página 298
- [“Trabajar con políticas de Active Directory,”](#) página 299

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 3-1. Lista de comprobación para la configuración de recursos de IaaS

Tarea	Función de vRealize Automation	Detalles
<input type="checkbox"/> Almacenar las credenciales de administrador en la infraestructura.	Administrador de IaaS	<p>“Almacenar credenciales de usuario,” página 186.</p> <p>No tiene que proporcionar credenciales si está integrando una de las siguientes plataformas:</p> <ul style="list-style-type: none"> ■ Grupo de Xen en un XenServer ■ XenServer ■ vSphere y si el administrador del sistema configuró el agente de proxy para usar credenciales integradas
<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,” página 188.
<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,” página 207.
<input type="checkbox"/> Configurar prefijos de máquina utilizados para crear nombres para las máquinas aprovisionadas a través de vRealize Automation.	Administrador de tejido	“Configurar prefijos de máquina,” página 207.
<input type="checkbox"/> (Opcional) Crear perfiles de red para configurar opciones de red para las máquinas aprovisionadas.	Administrador de tejido	“Crear un perfil de red,” página 210.
<input type="checkbox"/> 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,” página 228.

Almacenar credenciales de usuario

Debe almacenar las credenciales a nivel de administrador del entorno para que vRealize Automation se pueda comunicar con los endpoints. Debido a que varios endpoints pueden usar las mismas credenciales, estas se administran de manera independiente a los endpoints y se asocian cuando los endpoints se crean o se editan.

Prerequisitos

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

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Credenciales**.
- 2 Haga clic en **Nuevas credenciales**.
- 3 Escriba un nombre en el cuadro de texto **Nombre**.
- 4 (Opcional) Escriba una descripción en el cuadro de texto **Descripción**.

- 5 Escriba el nombre de usuario en el cuadro de texto **Nombre de usuario**.

Plataforma	Formato e información
vSphere	domain\username Proporcione las credenciales con permiso para modificar los atributos personalizados.
vCloud Air	nombre de usuario como se especifica en la interfaz de usuario de endpoints Proporcione las credenciales de un administrador de la organización con autorización para conectarse mediante VMware Remote Console.
vCloud Director	nombre de usuario como se especifica en la interfaz de usuario de endpoints Proporcione las credenciales con autorización para conectarse mediante VMware Remote Console. <ul style="list-style-type: none"> ■ 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.
vRealize Orchestrator	username@domain Proporcione las credenciales de cada instancia de vRealize Orchestrator con permisos de ejecución en todos los flujos de trabajo que desee llamar desde vRealize Automation.
vCloud Networking and Security (solo vSphere)	domain\username
NSX (solo vSphere)	username
Amazon AWS	Especifique el identificador de clave de acceso. Para informarse sobre la obtención del identificador de clave de acceso y la clave de acceso secreta, consulte la documentación de Amazon AWS.
Cisco UCS Manager	username
Dell iDRAC	username
HP iLO	username
Hyper-V (SCVMM)	domain\username
KVM (RHEV)	username@domain
NetApp ONTAP	username
Red Hat OpenStack	username Proporcione las credenciales de un solo usuario que sea administrador en todos los tenants de Red Hat OpenStack, o cree credenciales independientes para cada tenant.

- 6 Escriba la contraseña en los cuadros de texto **Contraseña**.

Plataforma	Formato
Amazon AWS	Indique la clave de acceso secreta. Para informarse sobre la obtención del identificador de clave de acceso y la clave de acceso secreta, consulte la documentación de Amazon AWS.
Todas las demás	Escriba la contraseña del nombre de usuario que ha proporcionado.

- 7 Haga clic en el icono **Guardar** (✓).

Qué hacer a continuación

Ahora que las credenciales están almacenadas, es el momento de crear un endpoint. Consulte [“Elegir un escenario de endpoint,”](#) página 188.

Elegir un escenario de endpoint

Los endpoints se crean para hacer posible la comunicación de vRealize Automation con su infraestructura. El procedimiento para crear un endpoint depende de las necesidades de aprovisionamiento de máquinas.

Elija un escenario de endpoint en función del tipo de endpoint de destino.

Tabla 3-2. Elegir un escenario de endpoint

Entorno	Crear endpoint
vSphere	“Crear un endpoint de vSphere,” página 188
vSphere con NSX	“Crear un endpoint de vSphere con integración de red y seguridad,” página 190
vSphere con tecnología de almacenamiento Net App FlexClone	“Crear un endpoint de NetApp ONTAP,” página 197
vRealize Orchestrator	“Crear un endpoint de vRealize Orchestrator,” página 191
Endpoint del proveedor de IPAM externo	“Crear un endpoint de proveedor de IPAM de terceros,” página 192
Suscripción de vCloud Air u OnDemand	“Crear un endpoint de vCloud Air,” página 193
vCloud Director	“Crear un endpoint de vCloud Director,” página 194
Hyper-V Standalone	“Crear un endpoint independiente para Hyper-V,” página 196
Hyper-V con SCVMM (Microsoft Center Virtual Machine Manager)	“Crear un endpoint de Hyper-V (SCVMM),” página 196
KVM (RHEV)	“Crear un endpoint de KVM (RHEV),” página 197
Cuenta de servicio de nube de Amazon	<ul style="list-style-type: none"> ■ “Crear un endpoint de Amazon,” página 199 ■ (Opcional) “Añadir un tipo de instancia de Amazon,” página 68
Microsoft Azure	“Crear un endpoint de Microsoft Azure,” página 201
Tenant de OpenStack	“Crear un endpoint de OpenStack o PowerVC,” página 203
PowerVC	“Crear un endpoint de OpenStack o PowerVC,” página 203
Grupo de Xen en un XenServer	“Crear un endpoint de grupo de Xen,” página 198
XenServer	“Crear un endpoint de XenServer,” página 199
Importar una lista de endpoints	<ul style="list-style-type: none"> ■ “Preparar un archivo CSV de endpoints para importarlo,” página 205 ■ “Importar una lista de endpoints,” página 204

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.

Si su entorno de vSphere está integrado con NSX, consulte [“Crear un endpoint de vSphere con integración de red y seguridad,”](#) página 190.

Prerequisitos

- Inicie sesión en la consola de 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 7.2*.
- Si el administrador del sistema no configuró el proxy para usar credenciales integradas, deberá almacenar credenciales de nivel de administrador para el endpoint. Consulte [“Almacenar credenciales de usuario,”](#) página 186.

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 Haga clic en **Credenciales** y seleccione las credenciales de administración que almacenó para este endpoint.
Si el administrador del sistema configuró el agente de proxy de vSphere para usar credenciales integradas, puede seleccionar las credenciales **Integradas**.
- 7 No seleccione **Especificar administrador para la plataforma de red y seguridad** a menos que la configuración admita NSX.
Esta opción está pensada para implementaciones en las que se usa NSX y precisa de configuración adicional.
- 8 (Opcional) Haga clic en **Nuevo** en la sección Propiedades personalizadas para añadir propiedades de endpoint significativas para el proveedor de la solución 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.
- 9 Haga clic en **Aceptar**.

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

IMPORTANTE: 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.

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

Crear un endpoint de vSphere con integración de red y seguridad

Se pueden crear endpoints para que vRealize Automation pueda comunicarse con el entorno de vSphere y una instancia de NSX.

Prerequisitos

- Inicie sesión en la consola de 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 7.2*.
- Almacene las credenciales de administración del endpoint de vSphere y del endpoint de redes y de seguridad. Consulte [“Almacenar credenciales de usuario,”](#) página 186. Si el administrador del sistema configuró el agente de proxy para usar credenciales integradas, solo necesita almacenar las credenciales de NSX.
- Configure los ajustes de red. Consulte [“Configurar opciones del componente de red y seguridad,”](#) página 345.

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 Haga clic en **Credenciales** y seleccione las credenciales de administración que almacenó para este endpoint.
Si el administrador del sistema configuró el agente de proxy de vSphere para usar credenciales integradas, puede seleccionar las credenciales **Integradas**.
- 7 Configure una plataforma de solución de red.
Este paso es obligatorio para habilitar las características de redes y de seguridad de NSX.
 - a Seleccione **Especificar administrador para la plataforma de red y seguridad**.
 - b 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**.
 - c Haga clic en **Credenciales** y seleccione las credenciales de administración que almacenó para este endpoint.
- 8 (Opcional) Añada cualquier propiedad personalizada.
- 9 Haga clic en **Aceptar**.

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

IMPORTANTE: 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.

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

Crear un endpoint 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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de IaaS**.
- Configure las credenciales de usuario. Consulte *Configuración de vRealize Automation*.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Orquestación > vCenter 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 Especifique la prioridad de endpoint.
 - a Haga clic en **Nueva propiedad**.
 - b Escriba **VMware.VCenterOrchestrator.Priority** en el cuadro de texto **Nombre**.
El nombre de propiedad distingue mayúsculas de minúsculas.
 - c Escriba un entero mayor o igual que 1 en el cuadro de texto **Valor**.
Un valor inferior indica una mayor prioridad.
 - d Haga clic en el icono **Guardar** (🟢).
- 6 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,”](#) página 191.

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 utilizarla como endpoint de vRealize Orchestrator para ejecutar flujos de trabajo de vRealize Automation en un entorno de prueba o para crear una prueba de concepto.

También puede instalar un complemento en un servidor de vRealize Orchestrator externo.

Se recomienda utilizar este endpoint de vRealize Orchestrator para ejecutar flujos de trabajo de vRealize Automation en entornos de producción.

Para instalar el complemento, consulte el archivo LÉAME que se ofrece junto con el archivo del programa de instalación del complemento en el sitio de descarga de productos VMware en <http://vmware.com/web/vmware/downloads>, en los vínculos de NSX.

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.

Prerequisitos

- [“Obtener e importar un paquete de proveedores de IPAM externos en vRealize Orchestrator,”](#) página 16.
- [“Ejecutar el flujo de trabajo para registrar un tipo de endpoint de IPAM de terceros en vRealize Orchestrator,”](#) página 17.
- Inicie sesión en la consola de vRealize Automation como **administrador de IaaS**.
- Configure las credenciales de usuario. Consulte *Configuración de vRealize Automation*.

Para este ejemplo, cree un endpoint de Infoblox IPAM con un tipo de endpoint que haya registrado en el complemento o el paquete importados.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > 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 **Nuevo** en la sección Propiedades personalizadas para añadir propiedades de endpoint significativas para el proveedor de la solución 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**.

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

Crear un endpoint de vCloud Air

Puede crear un endpoint de vCloud Air para un servicio de suscripción u OnDemand.

Para obtener información sobre la consola de administración de vCloud Air, consulte la documentación de vCloud Air.

NOTA: Las reservas definidas para endpoints de vCloud Air y endpoints de vCloud Director no admiten el uso de perfiles de red para el aprovisionamiento de máquinas.

Prerequisitos

- Inicie sesión en la consola de 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.
- [“Almacenar credenciales de usuario,”](#) página 186.

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 Haga clic en **Credenciales** y seleccione las credenciales de administración que almacenó para este endpoint.

Las credenciales deben ser las del administrador de cuenta de OnDemand o del servicio de suscripción de vCloud Air.
- 6 (Opcional) Active la casilla **Usar servidor proxy** para configurar un nivel adicional de seguridad y obligar a que las conexiones atraviesen un servidor proxy.
 - a Escriba el nombre del host del servidor proxy en el cuadro de texto **Nombre del host**.
 - b Escriba el número de puerto que se va a usar para conectarse al servidor proxy en el cuadro de texto **Puerto**.
 - c (Opcional) Haga clic en el icono **Examinar** al lado del cuadro de texto **Credenciales**.

Si la configuración de proxy lo requiere, seleccione o cree las credenciales que representan el nombre de usuario y contraseña del servidor proxy.
- 7 (Opcional) Añada propiedades personalizadas.
- 8 Haga clic en **Aceptar**.

Qué hacer a continuación

[“Crear un grupo de tejidos,”](#) página 207.

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.

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 endpoints de vCloud Air y endpoints de vCloud Director no admiten el uso de perfiles de red para el aprovisionamiento de máquinas.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de IaaS**.
- [“Almacenar credenciales de usuario,”](#) página 186.

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 Haga clic en **Credenciales** y seleccione las credenciales de administración que almacenó para este endpoint.

- 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 el campo Organización vacío, 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 esta.

- 7 (Opcional) Active la casilla **Usar servidor proxy** para configurar un nivel adicional de seguridad y obligar a que las conexiones atraviesen un servidor proxy.
- a Escriba el nombre del host del servidor proxy en el cuadro de texto **Nombre del host**.
 - b Escriba el número de puerto que se va a usar para conectarse al servidor proxy en el cuadro de texto **Puerto**.
 - c (Opcional) Haga clic en el icono **Examinar** al lado del cuadro de texto **Credenciales**.
Si la configuración de proxy lo requiere, seleccione o cree las credenciales que representan el nombre de usuario y contraseña del servidor proxy.
- 8 (Opcional) Añada propiedades personalizadas.
- 9 Haga clic en **Aceptar**.

Qué hacer a continuación

[“Crear un grupo de tejidos,”](#) página 207.

Crear un endpoint de Hyper-V (SCVMM)

Los administradores de IaaS crean endpoints para que vRealize Automation pueda comunicarse con el entorno de SCVMM con el fin de detectar recursos informáticos, recopilar datos y aprovisionar máquinas.

Prerequisitos

- Inicie sesión en la consola de 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 7.2*.
- [“Almacenar credenciales de usuario,”](#) página 186.

Para obtener información relacionada, consulte [“Preparar el entorno de SCVMM,”](#) página 26.

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 Haga clic en **Credenciales** y seleccione las credenciales de administración que almacenó para este endpoint.
Si todavía no ha almacenado las credenciales, puede hacerlo ahora.
- 7 (Opcional) Añada propiedades personalizadas.
- 8 Haga clic en **Aceptar**.

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

Crear un endpoint independiente para Hyper-V

Se pueden crear endpoints para que vRealize Automation pueda comunicarse con el entorno de servidor de Hyper-V con el fin de detectar recursos informáticos, recopilar datos y aprovisionar máquinas.

Prerequisitos

- Inicie sesión en la consola de 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 7.2*.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Agentes**.
- 2 Escriba el nombre DNS completo del servidor de Hyper-V en el cuadro de texto **Recurso informático**.

- 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**.

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

Crear un endpoint de NetApp ONTAP

Se pueden crear endpoints para que vRealize Automation pueda comunicarse con los dispositivos de almacenamiento que emplean la tecnología de Net App FlexClone.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de IaaS**.
- [“Almacenar credenciales de usuario,”](#) página 186.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Almacenamiento > NetApp ONTAP**.
- 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: `netapp-1.mycompany.local`.
- 6 Haga clic en **Credenciales** y seleccione las credenciales de administración que almacenó para este endpoint.
Si todavía no ha almacenado las credenciales, puede hacerlo ahora.
- 7 (Opcional) Añada propiedades personalizadas.
- 8 Haga clic en **Aceptar**.

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

Crear un endpoint de KVM (RHEV)

Se pueden crear endpoints para que vRealize Automation pueda comunicarse con el entorno de KVM (RHEV) con el fin de detectar recursos informáticos, recopilar datos y aprovisionar máquinas.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de IaaS**.
- [“Almacenar credenciales de usuario,”](#) página 186.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Seleccione **Nuevo > Virtual > KVM (RHEV)**.
- 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: **https://FQDN** o **https://IP_address**.
Por ejemplo, **https://mycompany-kvmrhev1.mycompany.local**.
- 6 Haga clic en **Credenciales** y seleccione las credenciales de administración que almacenó para este endpoint.
Si todavía no ha almacenado las credenciales, puede hacerlo ahora.
- 7 (Opcional) Añada propiedades personalizadas.
- 8 Haga clic en **Aceptar**.

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

Crear un endpoint de grupo de Xen

Se pueden crear endpoints para que vRealize Automation pueda comunicarse con el máster de grupo de Xen con el fin de detectar recursos informáticos, recopilar datos y aprovisionar máquinas.

Prerequisitos

- Inicie sesión en la consola de 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 7.2*.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Agentes**.
- 2 Escriba el nombre del máster de grupo de Xen en el cuadro de texto **Recurso informático**.

NOTA: No escriba el nombre del grupo de Xen. Debe especificar el nombre del máster de grupo.

Para evitar entradas duplicadas en la tabla de recursos informáticos de vRealize Automation, especifique una dirección que coincida con la dirección de máster de grupo de Xen configurada. Por ejemplo, si la dirección de máster de grupo de Xen usa el nombre de host, escriba el nombre de host en lugar del FQDN. Si la dirección de máster de grupo de Xen usa un FQDN, entonces indique 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**.

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

Crear un endpoint de XenServer

Se pueden crear endpoints para que vRealize Automation pueda comunicarse con el entorno de XenServer con el fin de detectar recursos informáticos, recopilar datos y aprovisionar máquinas.

Prerequisitos

- Inicie sesión en la consola de 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 7.2*.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Agentes**.
- 2 Escriba el nombre DNS completo del servidor de XenServer en el cuadro de texto **Recurso informático**.
- 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**.

vRealize Automation recopila datos de su endpoint y detecta sus recursos informáticos.

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

Crear un endpoint de Amazon

Puede crear un endpoint para que se conecte a una instancia de Amazon Web Services.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de IaaS**.
- [“Almacenar credenciales de usuario,”](#) página 186.

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 Web Services que se corresponde con este endpoint.
- 4 Haga clic en **Credenciales** y seleccione las credenciales de administración que almacenó para este endpoint.
Solamente se puede asociar un endpoint con un ID de clave de acceso de Amazon.

- 5 (Opcional) Haga clic en la casilla de verificación **Usar servidor proxy** para configurar un mayor nivel de seguridad y obligar a que las conexiones con Amazon Web Services atraviesen un servidor proxy.
 - a Escriba el nombre de host del servidor proxy en el cuadro de texto **Nombre de host**.
 - b Escriba el número de puerto que se va a usar para conectarse al servidor proxy en el cuadro de texto **Puerto**.
 - c (Opcional) Haga clic en el icono **Examinar** al lado del cuadro de texto **Credenciales**.
Si la configuración de proxy lo requiere, seleccione o cree las credenciales que representan el nombre de usuario y contraseña del servidor proxy.
- 6 (Opcional) Añada propiedades personalizadas.
- 7 Haga clic en **Aceptar**.

Después de crear el endpoint, vRealize Automation empieza a recopilar datos de las regiones de Amazon Web Services.

Qué hacer a continuación

vRealize Automation ofrece varios tipos de instancia de Amazon Web Services para que los use al crear blueprints, pero si desea importar sus propios tipos de instancia, consulte [“Añadir un tipo de instancia de Amazon,”](#) página 68.

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

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.

Prerequisitos

Inicie sesión en la consola de 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/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** (✓).

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

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte “[Crear un grupo de tejidos](#),” página 207.

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.

Prerequisitos

- 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.
- La implementación de vRealize Automation debe tener 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
- Inicie sesión en la consola de 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 el 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.
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 Haga clic en **Finalizar**.

Qué hacer a continuación

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.

Crear un endpoint de OpenStack o PowerVC

El endpoint se crea para que vRealize Automation pueda comunicarse con su instancia OpenStack o PowerVC.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de IaaS**.
- [“Almacenar credenciales de usuario,”](#) página 186.
- 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 7.2*.
- Verifique que el tipo de OpenStack sea compatible actualmente. Consulte *Matriz de soporte de vRealize Automation*.

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 URL debe respetar el formato https://FQDN/powervc/openstack/service . Por ejemplo: https://openstack.mycompany.com/powervc/openstack/admin .
OpenStack	Esta URL debe tener el formato FQDN:5000 o IP_address:5000 . No incluya el sufijo /v2.0 en la dirección del endpoint. Por ejemplo: https://openstack.mycompany.com:5000 .

- 5 Haga clic en **Credenciales** y seleccione las credenciales de administración que almacenó para este endpoint.

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 (Opcional) Añada propiedades personalizadas.
- 8 Haga clic en **Aceptar**.

Qué hacer a continuación

Añadir los recursos informáticos desde su endpoint a un grupo de tejidos. Consulte [“Crear un grupo de tejidos,”](#) página 207.

Importar una lista de endpoints

Importar un archivo CSV de endpoints puede resultar más eficaz que añadirlos uno a uno con la consola de vRealize Automation.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de IaaS**.
- Almacene las credenciales de los endpoints.
- Prepare un archivo CSV de endpoints para importarlo.

Procedimiento

- 1 Seleccione **Infraestructura > Endpoint > Endpoint**.
- 2 Haga clic en **Importar endpoints**.
- 3 Haga clic en **Examinar**.
- 4 Busque el archivo CSV que contiene los endpoints.

5 Haga clic en **Abrir**.

Se abre un archivo CSV que contiene una lista de endpoints en el siguiente formato:

```
InterfaceType,Address,Credentials,Name,Description
vCloud,https://abxpoint2vco,svc-admin,abxpoint2vco,abxpoint
```

6 Haga clic en **Importar**.

Los endpoints se pueden editar y administrar en la consola de vRealize Automation.

Preparar un archivo CSV de endpoints para importarlo

En vez de añadir los endpoints de uno en uno mediante la consola de vRealize Automation, puede importar una lista de endpoints cargando un archivo CSV.

El archivo CSV debe contener una fila de encabezado con los campos requeridos. Los campos distinguen mayúsculas y minúsculas y deben seguir un orden específico. Puede cargar endpoints de varios tipos con el mismo archivo CSV. Para vCloud Director, se importan las cuentas de administrador del sistema, en vez de los endpoints de administrador de la organización.

Tabla 3-3. Campos del archivo CSV y su orden para importar endpoints

Campo	Descripción
InterfaceType	(Obligatorio) Puede cargar varios tipos de endpoint en un solo archivo. <ul style="list-style-type: none"> ■ vCloud Air ■ vCloud Director ■ vRealize Orchestrator ■ vSphere ■ Amazon EC2 ■ OpenStack ■ NetAppOnTap ■ SCVMM ■ KVM
Address	(Obligatorio para todos los tipos de interfaz, excepto para Amazon) La URL del endpoint. Para obtener información sobre el formato requerido para un tipo de plataforma concreto, consulte el procedimiento apropiado para crear un endpoint en dicha plataforma.
Credentials	(Obligatorio) El nombre indicado en las credenciales de usuario cuando se almacenaron en vRealize Automation.
Name	(Obligatorio) Proporcione un nombre para el endpoint. Para OpenStack, la dirección se utiliza como el nombre predeterminado.
Description	(Obligatorio) Proporcione una descripción para el endpoint.
OpenstackProject	(Obligatorio solo para OpenStack) Proporcione el nombre de proyecto para el endpoint.

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, suele 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.

Origen

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.
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**.

El agente de proxy puede conmutarse con el endpoint y la recopilación de datos se realiza correctamente.

Solucionar problemas para localizar la URL de administración de vCloud Air de un centro de datos virtual de la organización

Para crear un endpoint de vCloud Air, vRealize Automation se debe proporcionar con la región de vCloud Air y URL de administración necesarias.

Solución

La URL de administración de vCloud Air es también la URL del servidor de vCloud Director que se usa para administrar un centro de datos virtual (vDC) específico. Puede usar la información de región y la URL de administración para configurar su endpoint de vCloud Air.

Busque la URL de administración de cada vDC de región de la consola de vCloud Air.

Procedimiento

- 1 Inicie sesión en la consola de vCloud Air con privilegios administrativos.
- 2 En el panel de vCloud Air, seleccione el centro de datos virtual.
- 3 Haga clic en el vínculo para ver una URL del centro de datos virtual que se usa en comandos de API.

Por ejemplo: <https://mycompany.com:443/cloud/org/vCloudAutomation/>.

La URL de administración que necesita proporcionar a vRealize Automation es el fragmento de host y puerto de la URL del comando de API, mientras que la región es el fragmento de la URL que va detrás de `cloud/org/`. En el ejemplo que nos ocupa, la URL de administración es <https://mycompany.com:443> y la región, `vCloudAutomation`.

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 tejido a varios usuarios. Para ello, debe añadir varios usuarios, de uno en uno, o elegir un grupo de almacén de identidades o grupo personalizado como administrador de tejido.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de IaaS**.
- Cree al menos un 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**.

Los administradores de tejido ya pueden configurar prefijos de máquina. Consulte [“Configurar prefijos de máquina,”](#) página 207.

Los usuarios que han iniciado sesión en la consola de vRealize Automation deben cerrar la sesión de la consola de vRealize Automation y volver a iniciarla antes de poder navegar a 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.

Prerequisitos

Inicie sesión en la consola de 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 Escriba el número de dígitos de contador en el cuadro de texto **Número de dígitos**.
- 5 Escriba el número inicial del contador en el cuadro de texto **Siguiente número**.
- 6 Haga clic en el icono **Guardar** (✓).

Los administradores de tenants pueden crear empresariales para que los usuarios puedan acceder a vRealize Automation para solicitar máquinas.

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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 188 y [“Crear un grupo de tejidos,”](#) página 207.

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** (✓).

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tejido**.
- Debe contar previamente con un par de claves. Consulte [“Crear un par de claves,”](#) página 209.

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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 209.

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**.

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 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 usando un endpoint de proveedor de IPAM de terceros y desea especificar la red en la que se implementará la máquina, utilice un perfil de red independiente para cada VLAN.

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 la clonación o 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.

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 la *guía de administración de NSX*.

Tabla 3-4. 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 mediante el endpoint de IPAM suministrado,” página 214 y “Crear un perfil de red externa mediante un proveedor de IPAM de terceros,” página 217.</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>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,” página 224.</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 mediante el endpoint de IPAM suministrado,” página 220.</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 preparar la compatibilidad con proveedores de IPAM de terceros,”](#) página 16.

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,Unallocated
```

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. También puede permitir que un proveedor de IPAM externo suministre las direcciones IP.

- Importar un rango inicial de direcciones IP en un perfil de red de vRealize Automation
- Aplicar los valores importados para crear el primer rango de redes con nombre del perfil de red
- Eliminar una o varias direcciones IP del rango de redes de vRealize Automation
- Importar otro archivo CSV distinto, o uno modificado, para examinar cómo cambiar los valores del rango de redes

No hay ninguna opción **Importar de CSV** para los perfiles de red que use un tipo de endpoint de IPAM externo, ya que las direcciones IP no las administra vRealize Automation sino el proveedor de IPAM externo.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 217 y [“Comprender el formato de un archivo CSV para importar direcciones IP del perfil de red,”](#) página 212.

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,Unallocated
```

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.

Campo de CSV	Descripción
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.

Qué hacer a continuación

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,”](#) página 217.

Procedimiento

- 1 [Indicar la información del perfil de red externa mediante el endpoint de IPAM suministrado](#)
página 215
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](#)
página 216
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.

Qué hacer a continuación

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 preparar la compatibilidad con proveedores de IPAM de terceros,”](#) página 16 y [“Crear un perfil de red externa mediante un proveedor de IPAM de terceros,”](#) página 217. Use el procedimiento siguiente para crear un perfil de red mediante el endpoint de IPAM interno de VMware.

Prerequisitos

- Inicie sesión en la consola de 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**.

Qué hacer a continuación

Puede configurar rangos IP para direcciones IP estáticas. Consulte [“Configurar rangos de IP del perfil de red externa mediante el endpoint de IPAM suministrado,”](#) página 216.

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.

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.

Puede definir valores de rangos IP manualmente desde un archivo CSV importado o mediante las direcciones IP que proporcione un proveedor de IPAM externo.

Prerequisitos

[“Indicar la información del perfil de red externa mediante el endpoint de IPAM suministrado,”](#) página 215.

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,Unallocated
```


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.

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,”](#) página 214.

Procedimiento

- 1 [Indicar la información del perfil de red externa mediante un endpoint de IPAM de terceros](#) página 218
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](#) página 219
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.

Qué hacer a continuación

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.

Prerequisitos

- 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 preparar la compatibilidad con proveedores de IPAM de terceros,”](#) página 16.
- [“Crear un endpoint de proveedor de IPAM de terceros,”](#) página 192.
- 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 la consola de 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.

Qué hacer a continuación

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

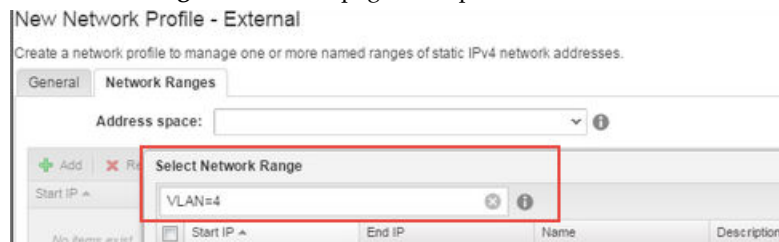
Se pueden definir uno o varios rangos de redes de direcciones IP estáticas en el perfil de red para usarlos al aprovisionar una máquina. Si no se especifica ningún rango, puede usar un perfil de red como política de reserva de red a fin de seleccionar un nombre de red de reserva para la tarjeta de red 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`.

Prerequisitos

[“Indicar la información del perfil de red externa mediante un endpoint de IPAM de terceros,”](#) página 218.

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.

- 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.

Qué hacer a continuación

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.

Procedimiento

- 1 [Indicar información de perfil de red enrutada con el endpoint de IPAM de vRealize Automation](#)
página 221
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](#)
página 222
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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 214.

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 interno de **IPAM de vRealize Automation** suministrado, o bien seleccione un endpoint de un proveedor de IPAM de terceros (como Infoblox) que haya importado y registrado en vRealize Orchestrator.
- 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 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**.

Qué hacer a continuación

[“Configurar rangos de IP de perfil de red enrutada con el endpoint de IPAM de vRealize Automation,”](#) página 222.

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.

Prerequisitos

[“Indicar información de perfil de red enrutada con el endpoint de IPAM de vRealize Automation,”](#) página 221.

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](#) página 223
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](#) página 224
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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tejido**.
- Cree un perfil de red externa. Consulte [“Crear un perfil de red externa mediante un proveedor de IPAM de terceros,”](#) página 217.

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.

Qué hacer a continuación

[“Configurar rangos de IP de perfil de red enrutada con un endpoint de IPAM de terceros,”](#) página 224.

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.

Prerequisitos

[“Indicar información de perfil de red enrutada con un endpoint de IPAM de terceros,”](#) página 223.

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.
 - a Haga clic en **Añadir**.
 - 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, relacionado con un perfil de red externa.

Puede asignar rangos de direcciones DHCP e IP estáticas a un 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.

Procedimiento

- 1 [Especificar la información de perfil de red NAT](#) página 225
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.

2 [Configurar rangos de IP de perfil de red NAT](#) página 226

Se pueden definir unos o varios rangos de direcciones IP estáticas para usarlos al aprovisionar una red.

Especificar la información de perfil de red NAT

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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 214 o [“Crear un perfil de red externa mediante un proveedor de IPAM de terceros,”](#) página 217.

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.

Los endpoints de IPAM de terceros no están disponibles para un perfil de red de NAT. Solo el endpoint de **IPAM de vRealize Automation** suministrado se puede utilizar para definir un perfil de red NAT.

- 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 muchos en el menú desplegable **Tipo de NAT**.

Opción	Descripción
Uno a uno	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.
Uno a muchos	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.

- 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**.

Qué hacer a continuación

[“Configurar rangos de IP de perfil de red NAT,”](#) página 226.

Configurar rangos de IP de perfil de red NAT

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.

Prerequisitos

[“Especificar la información de perfil de red NAT,”](#) página 225.

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,Unallocated
```

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**.

Destruir máquinas aprovisionadas y liberar direcciones IP

Cuando destruye una máquina implementada, los rangos de IP asignados quedan disponibles para aprovisionamientos posteriores.

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.

Cuando destruye una implementación, las direcciones IP se eliminan. A continuación, el rango del perfil de red asignado se libera y queda disponible para aprovisionamientos posteriores.

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.

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: 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
- Hyper-V
- KVM
- OpenStack
- SCVMM
- XenServer
- Microsoft Azure

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 3-5. Elegir un escenario de reserva

Escenario	Procedimiento
Crear una reserva de vSphere.	“Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer,” página 256
Crear una reserva para asignar recursos para un endpoint de vCloud Air.	“Crear una reserva de vCloud Air,” página 239
Crear una reserva para asignar recursos para un endpoint de vCloud Director.	“Crear una reserva de vCloud Director,” página 243
Crear una reserva para asignar recursos de Amazon (usando o no Amazon Virtual Private Cloud).	“Crear una reserva de Amazon,” página 231
Crear una reserva para asignar recursos de OpenStack.	“Crear una reserva de OpenStack,” página 235
Crear una reserva para asignar recursos para Hyper-V.	“Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer,” página 256
Crear una reserva para asignar recursos para KVM.	“Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer,” página 256
Crear una reserva para asignar recursos de OpenStack.	“Crear una reserva de OpenStack,” página 235
Crear una reserva para asignar recursos para SCVMM.	“Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer,” página 256
Crear una reserva para asignar recursos para XenServer.	“Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer,” página 256
Crear una reserva para asignar recursos para Microsoft Azure.	“Crear una reserva de Microsoft Azure,” página 247

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.

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.

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.

Crear una reserva de Amazon

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 .

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](#) página 232

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](#) página 233
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](#) página 234
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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 208.

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 (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.

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.

Para obtener información relacionada sobre los equilibradores de carga, consulte *Configuración de vRealize Automation*.

Prerequisitos

[“Especificar la información de reserva de Amazon,”](#) página 232.

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.

- 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.

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.

Prerequisitos

[“Especificar los recursos y valores de configuración de red de reservas de Amazon,”](#) página 233.

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 Escriba una o más direcciones de correo electrónico o nombres de grupo para recibir notificaciones de alerta en el cuadro de texto **Destinatarios**.
Pulse Intro 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.
- 12 Especifique la frecuencia de recordatorio (días).
- 13 Haga clic en **Guardar**.

La reserva se ha guardado y aparece en la lista Reservas.

Qué hacer a continuación

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](#) página 235
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](#) página 236
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](#) página 238
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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 208.
- 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.

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.

Prerequisitos

[“Especificar la información de reserva de OpenStack,”](#) página 235.

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.

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.

Prerequisitos

[“Especificar los recursos y valores de configuración de red de reservas de reserva de OpenStack,”](#) página 236.

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 Escriba una o más direcciones de correo electrónico o nombres de grupo para recibir notificaciones de alerta en el cuadro de texto **Destinatarios**.
Pulse Intro 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.
- 12 Especifique la frecuencia de recordatorio (días).
- 13 Haga clic en **Guardar**.

La reserva se ha guardado y aparece en la lista Reservas.

Qué hacer a continuación

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](#) página 240
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](#) página 241
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](#) página 242
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.

Qué hacer a continuación

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.

Prerequisitos

- Inicie sesión en la consola de 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.

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 endpoints de vCloud Air y endpoints de vCloud Director no admiten el uso de perfiles de red para el aprovisionamiento de máquinas.

Prerequisitos

[“Especificar la información de reserva de vCloud Director,”](#) página 244.

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.

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.

Prerequisitos

[“Especificar los recursos y valores de configuración de red de una reserva de vCloud Air,”](#) página 241

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 Escriba una o más direcciones de correo electrónico o nombres de grupo para recibir notificaciones de alerta en el cuadro de texto **Destinatarios**.
Pulse Intro 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.
- 14 Especifique la frecuencia de recordatorio (días).
- 15 Haga clic en **Guardar**.

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](#) página 244
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](#) página 245
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](#) página 246
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.

Qué hacer a continuación

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.

Prerequisitos

- Inicie sesión en la consola de 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.

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 endpoints de vCloud Air y endpoints de vCloud Director no admiten el uso de perfiles de red para el aprovisionamiento de máquinas.

Prerequisitos

[“Especificar la información de reserva de vCloud Director,”](#) página 244.

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.

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.

Prerequisitos

[“Especificar los recursos y valores de configuración de red de una reserva de vCloud Director,”](#) página 245.

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 Escriba una o más direcciones de correo electrónico o nombres de grupo para recibir notificaciones de alerta en el cuadro de texto **Destinatarios**.
Pulse Intro 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.
- 14 Especifique la frecuencia de recordatorio (días).
- 15 Haga clic en **Guardar**.

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.

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.

Prerequisitos

- Inicie sesión en la consola de 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 a Azure válido, el cual debe ser igual al que se utilice con el endpoint de Azure aplicable. Si utiliza varias suscripciones a Azure, debe crear una reserva para cada suscripción.

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.

Prerequisitos

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 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.

Prerequisitos

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.

Prerequisitos

- Inicie sesión en la consola de 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 [“Escenario: Configurar la conectividad de red a VPC de Amazon para un entorno de prueba de concepto,”](#) página 24.
- 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,”](#) página 155.
- 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](#) página 251
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](#) página 252
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](#) página 253
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.

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.

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**.

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.

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 **Exacta** y no hay reservas para un recurso informático asociado a esa ubicación que satisfaga los demás criterios, se producirá un error de aprovisionamiento.

Si el valor de *VRM.Datacenter.Policy* es **NotExact** y no hay reservas para un recurso informático asociado a esa ubicación que satisfaga los demás criterios, el aprovisionamiento podrá continuar en otra reserva sin importar la ubicación. Esta es la opción predeterminada.

- Si el blueprint o la solicitud especifican la propiedad personalizada *VirtualMachine.Host.TpmEnabled*, el hardware de confianza se deberá instalar 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 continuará con una ruta de almacenamiento externa a la política de reserva de almacenamiento especificada. El valor predeterminado de *VirtualMachine.DiskN.StorageReservationPolicyMode* es **Exacta**.

- 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 VMware NSX y ha instalado el complemento NSX para vRealize Automation, puede especificar la configuración de la zona de transporte, política de reserva de puerta de enlace enrutada y de Edge, y 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 Nuevo blueprint y Propiedades de blueprint.

La configuración del componente de redes y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario tener instalado el complemento NSX y 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](#) página 256
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](#) página 257
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](#) página 259
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.

Prerequisitos

- Inicie sesión en la consola de 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.

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.

Prerequisitos

[“Especificar la información de reserva virtual,”](#) página 256.

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.

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.

Prerequisitos

[“Especificar los recursos y valores de configuración de red de una reserva virtual,”](#) página 257.

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 Escriba una o más direcciones de correo electrónico o nombres de grupo para recibir notificaciones de alerta en el cuadro de texto **Destinatarios**.
Pulse Intro 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.
- 13 Especifique la frecuencia de recordatorio (días).
- 14 Haga clic en **Guardar**.

La reserva se ha guardado y aparece en la lista Reservas.

Qué hacer a continuación

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tejido**.
- Cree un perfil de red. Consulte [“Crear un perfil de red,”](#) página 210.

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 endpoints de vCloud Air y endpoints de vCloud Director no admiten el uso de perfiles de red para el aprovisionamiento de 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 deshabilitado.

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](#) página 261

Se pueden usar políticas de reserva para agrupar reservas similares.

- 2 [Asignar una política de reserva a una reserva](#) página 262

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.

Prerequisitos

Inicie sesión en la consola de 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.

Prerequisitos

[“Crear una política de reserva,”](#) página 261.

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 deshabilitado.

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](#) página 263

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](#) página 264

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.

Prerequisitos

Inicie sesión en la consola de 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.

Prerequisitos

[“Crear una política de reserva de almacenamiento,”](#) página 263.

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.

Escenario: Configurar recursos de IaaS para Rainpole

Si combina los privilegios de administrador de tenant y administrador de IaaS, puede crear un prefijo para anteponerlo a las máquinas de vSphere creadas en vRealize Automation, organizar los recursos de vSphere en un grupo de tejidos y asignar recursos al grupo personalizado de arquitectos de vRealize Automation.



Procedimiento

- 1 [Escenario: Crear un grupo de tejidos para Rainpole](#) página 265
Use sus privilegios de administrador de IaaS para crear un grupo de tejidos que incluya los recursos informáticos detectados cuando creó el endpoint de vSphere. Asigne el grupo personalizado de arquitectos y desarrolladores de vRealize Automation a la función de administrador de tejidos para este grupo.
- 2 [Escenario: Configurar prefijos de máquinas para Rainpole](#) página 266
Use sus privilegios de administrador de tejidos para crear un prefijo que puede configurar para anteponerlo en las máquinas aprovisionadas por los arquitectos y los desarrolladores de vRealize Automation durante las fases de desarrollo y de pruebas.
- 3 [Escenario: Crear un grupo empresarial para que los arquitectos de Rainpole prueben elementos del catálogo](#) página 266
Use sus privilegios de administrador de tenant para crear un grupo empresarial para el equipo de TI que se encarga de diseñar y probar los blueprints de vRealize Automation.
- 4 [Escenario: Crear una reserva para asignar recursos a los arquitectos de Rainpole](#) página 267
Use sus privilegios de administrador de tejido para crear una reserva para que el grupo empresarial de Rainpole asigne recursos de vSphere.

Escenario: Crear un grupo de tejidos para Rainpole

Use sus privilegios de administrador de IaaS para crear un grupo de tejidos que incluya los recursos informáticos detectados cuando creó el endpoint de vSphere. Asigne el grupo personalizado de arquitectos y desarrolladores de vRealize Automation a la función de administrador de tejidos para este grupo.

No es necesario crear un endpoint de vSphere porque ya creó uno cuando solicitó el elemento del catálogo de contenido inicial.

Procedimiento

- 1 Seleccione **Infraestructura > Grupos de tejidos**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Escriba **Rainpole fabric** en el cuadro de texto Nombre.
- 4 Busque **Arquitectos de Rainpole** en el cuadro de búsqueda **Administradores de tejido** y seleccione su grupo personalizado.
- 5 Seleccione el recurso informático del entorno de vSphere para incluirlo en el grupo de tejidos.
- 6 Haga clic en **Aceptar**.
- 7 Actualice el explorador para ver las nuevas opciones de menú que tiene disponibles como administrador de tejido.

Qué hacer a continuación

Use sus privilegios de administrador de tejido para crear un prefijo de máquina que los arquitectos de Rainpole puedan usar para identificar fácilmente cualquier máquina que aprovisionen durante las fases de desarrollo y pruebas.

Escenario: Configurar prefijos de máquinas para Rainpole

Use sus privilegios de administrador de tejidos para crear un prefijo que puede configurar para anteponerlo en las máquinas aprovisionadas por los arquitectos y los desarrolladores de vRealize Automation durante las fases de desarrollo y de pruebas.

Procedimiento

- 1 Seleccione **Infraestructura > Administración > Prefijos de máquina**.
- 2 Haga clic en **Nuevo**.
- 3 Escriba **Rainpole** en el cuadro de texto **Prefijo de máquina**.
- 4 Escriba **3** en el cuadro de texto **Número de dígitos**.
- 5 Escriba **1** en el cuadro de texto **Siguiente número**.
- 6 Haga clic en el icono **Guardar** (✓).

Qué hacer a continuación

Use sus privilegios de administrador de tenant para crear un grupo empresarial para el equipo de TI que se encarga de diseñar y probar los blueprints de vRealize Automation.

Escenario: Crear un grupo empresarial para que los arquitectos de Rainpole prueben elementos del catálogo

Use sus privilegios de administrador de tenant para crear un grupo empresarial para el equipo de TI que se encarga de diseñar y probar los blueprints de vRealize Automation.

Procedimiento

- 1 Seleccione **Administración > Usuarios y grupos > Grupos empresariales**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Escriba **Rainpole business group** en el cuadro de texto **Nombre**.
- 4 Escriba una o varias direcciones de correo electrónico en el cuadro de texto **Enviar correos electrónicos del administrador a**.

Por ejemplo, escriba su propia dirección de correo electrónico o la de su director de TI.

- 5 Añada una propiedad personalizada para ayudar a los arquitectos en la solución de problemas de sus blueprints.
 - a Haga clic en el icono **Nuevo** (+).
 - b Escriba **_debug_deployment** en el cuadro de texto **Nombre**.
 - c Escriba **true** en el cuadro de texto **Valor**.
 - d Seleccione **Preguntar al usuario** para permitir a los arquitectos activar o desactivar esta función cuando soliciten un elemento del catálogo.

Normalmente, si no se realiza correctamente el aprovisionamiento de un componente de un elemento del catálogo, vRealize Automation revierte todos los recursos incluidos en el elemento del catálogo. Utilice esta propiedad personalizada para reemplazar ese comportamiento, de modo que los arquitectos puedan localizar dónde están fallando los blueprints. Puede añadir esta propiedad personalizada al grupo empresarial, en lugar de a los blueprints, para asegurarse de que los arquitectos siempre elijan reemplazar este comportamiento, pero la opción nunca se ofrece a los usuarios de manera accidental.

- 6 Haga clic en **Siguiente**.

- 7 Busque **Arquitectos de Rainpole** en el cuadro de búsqueda **Función de administrador de grupo** y seleccione su grupo personalizado.
- 8 Busque **test_user** en el cuadro de texto **Función de usuario** y seleccione el usuario local que configuró como inicio de sesión compartido para probar blueprints.
- 9 Haga clic en **Siguiente**.
- 10 Seleccione **Rainpole** como prefijo de máquina predeterminado en el menú desplegable.
- 11 Haga clic en **Finalizar**.

Qué hacer a continuación

Use sus privilegios de administrador de tejidos para asignar recursos de IaaS al grupo empresarial de Rainpole, mediante la creación de una reserva.

Escenario: Crear una reserva para asignar recursos a los arquitectos de Rainpole

Use sus privilegios de administrador de tejido para crear una reserva para que el grupo empresarial de Rainpole asigne recursos de vSphere.

NOTA: Tras crear una reserva, no podrá cambiar el grupo empresarial ni el recurso informático.

Procedimiento

- 1 Seleccione **Infraestructura > Reservas > Reservas**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Seleccione **vSphere** en el menú desplegable.
- 4 Escriba la información de la reserva.

Opción	Entrada
Name	Rainpole reservation
Tenant	vsphere.local
Grupo empresarial	Rainpole business group
Prioridad	1

- 5 Seleccione la pestaña **Recursos**.
- 6 Escriba la información de recursos del entorno de implementación.

Opción	Entrada
Recursos informáticos	Seleccione un clúster de recursos del menú desplegable.
Cuota de máquinas	Especifique el número máximo de máquinas encendidas para esta reserva.
Memoria	Especifique la cantidad máxima de memoria (MB) que puede consumir esta reserva.
Almacenamiento	Seleccione una o varias rutas y reserve espacio (GB) para esta reserva. Asigne prioridades a las rutas de almacenamiento, siendo 1 la de mayor prioridad.

- 7 Seleccione la pestaña **Red**.
- 8 Seleccione al menos una ruta de red de vSphere.
- 9 Haga clic en **Aceptar**.

Ha traído la infraestructura de vSphere bajo la administración de vRealize Automation y ha asignado recursos de vSphere a su equipo.

Qué hacer a continuación

Use sus privilegios de arquitecto de IaaS para crear un blueprint de máquina y clonar máquinas vSphere CentOS.

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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 179.

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.

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,”](#) página 378.

Lista de comprobación para preparar el aprovisionamiento de una implementación de vRealize Automation con un proveedor de IPAM externo

Es posible obtener rangos y direcciones IP de algún proveedor de la solución IPAM externo compatible, como Infoblox, para usar en un perfil de red de vRealize Automation externa y existente. 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 Infoblox IPAM. 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 3-6. Preparar el aprovisionamiento de una implementación de vRealize Automation con la lista de comprobación de Infoblox IPAM

Tarea	Ubicación	Detalles
<input type="checkbox"/> Obtener, importar y configurar el paquete o el complemento del proveedor de la solución IPAM externo.	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. Si VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_groups/cloud-management) 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 de soporte.	Consulte “ Lista de comprobación para preparar la compatibilidad con proveedores de IPAM de terceros ,” página 16.
<input type="checkbox"/> Crear un endpoint del proveedor de la solución IPAM externo.	Cree un nuevo endpoint de IPAM en vRealize Automation.	Consulte “ Crear un endpoint de proveedor de IPAM de terceros ,” página 192.
<input type="checkbox"/> Especificar la configuración de endpoint del proveedor de la solución IPAM externo.	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 ,” página 217.
<input type="checkbox"/> Definir una reserva para usar un perfil de red externa en un nombre de red existente.	Cree una reserva que llame al perfil de red en vRealize Automation.	Consulte “ Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer ,” página 256.
<input type="checkbox"/> Definir un blueprint que use el perfil de red externa.	Cree un blueprint que utilice la reserva en vRealize Automation.	
<input type="checkbox"/> Autorizar el blueprint y agregarlo al catálogo.	Autorice el blueprint y agréguelo al catálogo en vRealize Automation.	
<input type="checkbox"/> 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.	
<input type="checkbox"/> Consultar en qué dirección IP reside la implementación desde la página Mis elementos.	Determine la dirección IP de la red que se usa para la implementación en vRealize Automation.	

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.

Prerequisitos

- Compruebe que tiene acceso a una instancia de Active Directory de Microsoft. Consulte la documentación de Active Directory de Microsoft.
- Inicie sesión en la consola de 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**.

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.

Qué hacer a continuación

- 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,”](#) página 438.
- 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,”](#) página 299.

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.

Prerequisitos

- Inicie sesión en la consola de 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> <ol 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>
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"> a Escriba el nombre de usuario para la sesión compartida en el cuadro de texto Nombre de usuario de autenticación. b Escriba la contraseña para la sesión compartida en el cuadro de texto Contraseña de autenticación.

Opción	Acción
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.

- Haga clic en **Finalizar**.

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.

Prerequisitos

- 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 la consola de vRealize Automation como **administrador de tenants**.

Procedimiento

- Seleccione **Administración > Configuración de vRO > Endpoints**.
- Haga clic en el icono **Nuevo** (+).
- Seleccione **PowerShell** en el menú desplegable **Complemento**.
- Haga clic en **Siguiente**.
- Especifique un nombre y, opcionalmente, una descripción.
- 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. 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. c Seleccione un tipo de autenticación en el menú desplegable Autenticación. 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>.
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**.

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.

Prerequisitos

- 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 la consola de 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.
- Escriba el nombre del host en el cuadro de texto **Nombre**.
 - 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 .

- (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.
 - (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.
- Para utilizar un proxy, seleccione **Sí** en el menú desplegable **Proxy**.
 - Escriba la dirección IP del servidor proxy en el cuadro de texto **Proxy**.
 - 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	Proporciona autenticación de acceso básica. La comunicación con el host se realiza en modo de sesión compartida. <ol 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.
Implícita	Proporciona autenticación de acceso implícita que usa cifrado. La comunicación con el host se realiza en modo de sesión compartida. <ol 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.

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.

- Haga clic en **Finalizar**.

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.

Prerequisitos

- Instale y configure vCenter Server. Consulte *Instalación y configuración de vSphere*.
- Inicie sesión en la consola de vRealize Automation como **administrador de tenants**.

Procedimiento

- Seleccione **Administración > Configuración de vRO > Endpoints**.
- Haga clic en el icono **Nuevo** (+).
- Seleccione **vCenter Server** en el menú desplegable **Complemento**.
- Haga clic en **Siguiente**.
- Especifique un nombre y, opcionalmente, una descripción.
- 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**.

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.

Prerequisitos

- 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.
- La implementación de vRealize Automation debe tener 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
- Inicie sesión en la consola de 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 el 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	

Parámetro	Descripción
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.
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 Haga clic en **Finalizar**.

Qué hacer a continuación

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.

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.

Ver y administrar hosts de contenedores

Puede ver y administrar los hosts que añada. En el contexto de Contenedores, el host es una máquina virtual o una infraestructura que le permite ejecutar contenedores.

La pestaña **Hosts** contiene los controles para añadir nuevos hosts, supervisar el estado de las solicitudes de aprovisionamiento de los hosts existentes, ver los logs de eventos de los contenedores y recopilar datos en los hosts.

Procedimiento

1 Inicie sesión en vRealize Automation como **administrador de contenedores**.

2 Haga clic en la pestaña **Hosts**.

La pestaña **Hosts** muestra controles de adición y administración.

3 Para añadir un host de contenedor existente, haga clic en **Añadir un host**.

a Complete los siguientes ajustes de configuración.

Configuración	Descripción
Dirección	Introduzca la dirección IP del nuevo host.
Zona de colocación	Seleccione una zona de colocación de la lista desplegable. Opcionalmente, puede crear una nueva zona de colocación.
Credencial de inicio de sesión	Seleccione una credencial de la lista desplegable. Opcionalmente, puede crear una nueva credencial.
Política de implementación	Seleccione una política de la lista desplegable. Opcionalmente, puede crear una nueva política.
Etiquetas	Opcionalmente, puede especificar etiquetas para ayudar a identificar el host.
Propiedades personalizadas	Añada las propiedades personalizadas que guste. Si desea añadir varias propiedades, utilice el botón + para incluir campos nuevos.

b (Opcional) Haga clic en **Verificar** para confirmar que la configuración del host es válida.

c Haga clic en **Añadir** para completar el proceso de adición del host.

El host recién añadido aparece en la pestaña **Hosts**.

Después de añadir un host, puede editarlo, deshabilitarlo o eliminarlo en la pestaña **Hosts**.

4 (Opcional) Para ver las solicitudes de aprovisionamiento, haga clic en el icono **Solicitudes** en la parte derecha de la pestaña **Hosts**.

Se abrirá el panel Solicitud de aprovisionamiento, que mostrará las solicitudes actuales y sus estados. Si hace clic en una solicitud, se mostrará el contenedor al que está asignada.

5 (Opcional) Para ver los logs de eventos, haga clic en el icono **Logs de eventos** en la parte derecha de la pestaña **Hosts**.

Se abrirá el panel Logs de eventos.

Añadir un host de contenedor

Para implementar contenedores, debe añadir un host.

Cuando añada o crea hosts en Contenedores, puede hacer clic en uno de los cuatro iconos de la derecha para ampliar las barras de herramientas de modo que muestren opciones adicionales. Puede añadir o administrar zonas de colocación, credenciales, certificados y colocaciones de implementación.

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 **Añadir un host**.

4 Introduzca la dirección IP del host o el nombre del host con el formato **http(s)://<nombre del host>:<puerto>**.

- 5 Seleccione las credenciales de inicio de sesión de la lista.
Contenedores admite la autenticación con credenciales y la autenticación con clave pública o privada.
 - 6 Seleccione una zona de colocación de la lista.
 - 7 Seleccione una política de implementación de la lista.
 - 8 (Opcional) Defina propiedades personalizadas para el host.
 - 9 Haga clic en **Añadir** y acepte el certificado.
 - 10 Haga clic en **Verificar** para confirmar que los parámetros configurados son válidos.
- Ha añadido correctamente un host a Contenedores.

Usar colocaciones de implementación de contenedores

Puede vincular colocaciones de implementación con definiciones de hosts y de contenedores. Las colocaciones de implementación se utilizan en Contenedores para vRealize Automation para definir una preferencia por hosts y cuotas concretos al implementar un contenedor.

Las colocaciones de implementación que se aplican a colocaciones de contenedor tienen una prioridad mayor que las colocaciones que se aplican a hosts de contenedor.

Crear y administrar las colocaciones de contenedor y la configuración de colocación

Puede utilizar las colocaciones y la configuración de colocación para limitar y reservar los recursos utilizados por un grupo empresarial. También puede establecer una prioridad para la cantidad reservada de recursos de CPU o memoria.

Para editar o eliminar las colocaciones que ha creado, apunte a ellas y haga clic en el botón correspondiente.

Cuando crea o administra colocaciones, puede hacer clic en uno de los dos iconos de la derecha para expandir las opciones adicionales. Los iconos **Zonas de colocación** y **Colocaciones de implementación** le permiten añadir o administrar zonas de colocación y colocaciones de implementación.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de contenedores**.
- Asegúrese de que los recursos de CPU o memoria especificados estén disponibles.
- 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 **Colocaciones**.
- 3 En la página Colocaciones, haga clic en **Añadir**.
- 4 Escriba un nombre para la colocación.
- 5 Asigne la colocación a un grupo.
- 6 Seleccione una zona de colocación de la lista.
- 7 (Opcional) Seleccione una colocación de implementación de la lista.
- 8 (Opcional) Introduzca un valor de prioridad para la colocación.

Introduzca un número positivo, donde **1** representa la máxima prioridad. Para indicar la prioridad más baja, deje el campo vacío.

- 9 Especifique el número de instancias.
- 10 Seleccione la cantidad máxima de memoria que puede utilizarse.
 Seleccione 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. Escriba 0 para no especificar ningún límite.
- 11 Introduzca el porcentaje de recursos de la CPU que desea asignar a esta colocación.
- 12 Haga clic en el botón de la marca de verificación para crear la colocación.

Establecer una colocación de implementación en un host

Establezca una colocación de implementación para un host específico. Permite definir una preferencia por hosts y cuotas concretos al implementar un contenedor.

Procedimiento

- 1 Cree o edite un host de contenedor.
- 2 En la parte derecha, haga clic en **Colocaciones de implementación** de modo que se muestren opciones adicionales.
- 3 Haga clic en **Añadir** y defina un nombre y una descripción de colocación.
- 4 En la vista **Añadir host** o **Editar host**, seleccione la colocación del menú desplegable **Colocaciones de implementación**.

Establecer una política de implementación para una colocación

Establezca una política de implementación para una configuración de colocación.

Prerequisitos

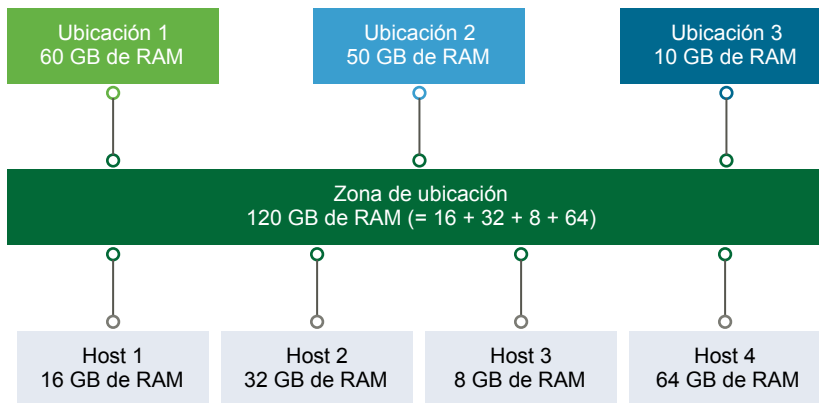
Procedimiento

- 1 Cree o edite una política.
- 2 A la derecha, haga clic en **Colocaciones** para mostrar la página Colocaciones.
- 3 Seleccione una política existente de la lista desplegable **Política de implementación**.
 Esta lista desplegable también incluye controles para buscar políticas, crear políticas nuevas y administrar políticas. También puede hacer clic en el icono **Política de implementación** en el lado derecho de la página Colocaciones para acceder a los controles de configuración de políticas.
- 4 Para completar el proceso, haga clic en el icono de marca de verificación.

Usar zonas de colocación de contenedores

Una zona de colocación es un conjunto de hosts y los recursos disponibles en una zona de colocación son la suma de todos los recursos de los hosts que existen en ella. Cada colocación se asigna a una zona de colocación de Contenedores para vRealize Automation. Más de una colocación puede administrar una única zona de colocación.

Las colocaciones que administran una zona de colocación no pueden reservar en conjunto más recursos que los que están disponibles en el grupo.



Cuando se aprovisiona un contenedor, las colocaciones se filtran en función del grupo empresarial, los recursos disponibles y la prioridad.

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.

Prerequisitos

- 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 Haga clic en **Plantillas** en el panel izquierdo.
- 4 Edite la plantilla o imagen.

- 5 Para editar una plantilla
 - a Haga clic en **Editar** en la parte superior derecha de la plantilla que desea abrir.
 - b Si la plantilla contiene varias plantillas, apunte a la plantilla que desea editar y haga clic en **Editar** en la parte superior derecha de la plantilla que desea abrir.
- 6 Para editar una imagen.
 - a Haga clic en la flecha situada junto al botón **Aprovisionar** de la imagen y, a continuación, haga clic en **Introducir información adicional**.

Se abrirá la página Aprovisionar un contenedor o la página Editar definición de contenedor, que permiten acceder a conjuntos clasificados de propiedades y configuraciones que se pueden editar.

- 7 Haga clic en la pestaña **Configuración de estado**.
- 8 Seleccione un modo de estado.

Tabla 3-7. 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 utilizará. 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.

- 9 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 para el 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.
-

Prerequisitos

- 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 Haga clic en la pestaña **Contenedores**.
- 3 Haga clic en **Plantillas** en el panel izquierdo.
- 4 Edite la plantilla o imagen.
- 5 Para editar una plantilla
 - a Haga clic en **Editar** en la parte superior derecha de la plantilla que desea abrir.
 - b Si la plantilla contiene varias plantillas, apunte a la plantilla que desea editar y haga clic en **Editar** en la parte superior derecha de la plantilla que desea abrir.
- 6 Para editar una imagen.
 - a Haga clic en la flecha situada junto al botón **Aprovisionar** de la imagen y, a continuación, haga clic en **Introducir información adicional**.

Se abrirá la página Aprovisionar un contenedor o la página Editar definición de contenedor, que permiten acceder a conjuntos clasificados de propiedades y configuraciones que se pueden editar.

- 7 Haga clic en la pestaña **Básica**.
- 8 En el cuadro de texto **Servicios**, escriba una lista de servicios separados por comas de los que depende el contenedor.
- 9 En el cuadro de texto **Alias**, escriba un nombre descriptivo del servicio o de la lista de servicios separados por comas.
- 10 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.

Prerequisitos

- 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 Haga clic en **Plantillas** en el panel izquierdo.
- 4 Edite la plantilla o imagen.
- 5 Haga clic en la pestaña **Red**.
- 6 Edite la plantilla o imagen.
- 7 Para editar una plantilla
 - a Haga clic en **Editar** en la parte superior derecha de la plantilla que desea abrir.
 - b Si la plantilla contiene varias plantillas, apunte a la plantilla que desea editar y haga clic en **Editar** en la parte superior derecha de la plantilla que desea abrir.
- 8 Para editar una imagen.
 - a Haga clic en la flecha situada junto al botón **Aprovisionar** de la imagen y, a continuación, haga clic en **Introducir información adicional**.

Se abrirá la página Aprovisionar un contenedor o la página Editar definición de contenedor, que permiten acceder a conjuntos clasificados de propiedades y configuraciones que se pueden editar.

- 9 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.
- 10 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.
- 11 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.

Prerequisitos

- 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 Haga clic en **Plantillas** en el panel izquierdo.
- 4 Edite la plantilla o imagen.
- 5 Haga clic en la pestaña **Colocación**.
- 6 Edite la plantilla o imagen.
- 7 Para editar una plantilla
 - a Haga clic en **Editar** en la parte superior derecha de la plantilla que desea abrir.
 - b Si la plantilla contiene varias plantillas, apunte a la plantilla que desea editar y haga clic en **Editar** en la parte superior derecha de la plantilla que desea abrir.
- 8 Para editar una imagen.
 - a Haga clic en la flecha situada junto al botón **Aprovisionar** de la imagen y, a continuación, haga clic en **Introducir información adicional**.

Se abrirá la página Aprovisionar un contenedor o la página Editar definición de contenedor, que permiten acceder a conjuntos clasificados de propiedades y configuraciones que se pueden editar.

- 9 Defina el tamaño del clúster del contenedor.

10 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,”](#) página 290.

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,”](#) página 291.

Prerequisitos

- 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 Haga clic en **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 Seleccione una plantilla existente o importe un archivo de plantilla YAML.
- 5 Seleccione una plantilla del panel **Vistas**.
 - a Haga clic en **Plantillas** para abrir la vista Plantilla.
 - b Haga clic en **Editar** en la parte superior derecha de la plantilla que desea personalizar.

- 6 Importe una plantilla YAML.
 - a Haga clic en el icono **Importar plantilla o Docker Compose**.
Se abrirá la página Importar plantilla.
 - b 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 .

- c Haga clic en **Importar**.

NOTA: También puede utilizar el campo **Buscar** proporcionado para buscar e importar plantillas.

Qué hacer a continuación

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.

Prerequisitos

- Compruebe que Contenedores para vRealize Automation esté activado en su implementación de vRealize Automation compatible.
- Inicie sesión en la consola de vRealize Automation como **administrador de contenedores**.

Para obtener información sobre el formato YAML utilizado por las API de REST de servicio de vRealize Automation, consulte *Referencia de la API de vRealize Automation*.

Procedimiento

- 1 Haga clic en la pestaña **Contenedores**.
- 2 Haga clic en **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.

Prerequisitos

- Compruebe que Contenedores para vRealize Automation esté activado en su implementación de vRealize Automation compatible.
- Inicie sesión en la consola de vRealize Automation como **administrador de contenedores**.

Procedimiento

- 1 Haga clic en la pestaña **Contenedores**.

- 2 Haga clic en **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 Aprovechone 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.

Prerequisitos

- Compruebe que Contenedores para vRealize Automation esté activado en su implementación de vRealize Automation compatible.
- Inicie sesión en la consola de vRealize Automation como **administrador de contenedores**.

Para obtener información sobre el formato YAML utilizado por las API de REST de servicio de vRealize Automation, consulte *Referencia de la API de vRealize Automation*.

Procedimiento

- 1 Haga clic en la pestaña **Contenedores**.
- 2 Haga clic en **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 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"`. 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 activado de manera predeterminada para todos los tenants y no está presente en la lista de registros, pero se puede deshabilitar 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 deshabilita 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 a partir de los que se cargan o descargan imágenes. Puede desactivar, editar o eliminar los registros que haya creado. Las imágenes que se muestran en la pestaña **Contenedores > Plantillas** se basan en los registros que usted define.

Al crear o administrar registros en la página Registros existentes, puede hacer clic en los iconos **Credenciales** o **Certificado** para añadir o administrar credenciales y certificados.

Prerequisitos

- Inicie sesión en la consola de 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 Plantillas
- 3 Haga clic en **Administrar registro**.
Se abrirá la página Registros existentes.
- 4 Haga clic en **Añadir**.
- 5 Escriba una IP o un nombre de host para el registro.
- 6 (Opcional) Escriba un nombre para el registro.
- 7 Seleccione las credenciales de inicio de sesión de la lista desplegable.
- 8 (Opcional) Haga clic en **Verificar** para confirmar que los parámetros configurados son válidos.
- 9 Haga clic en el icono de marca de verificación para crear 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 el contenedor o aprovisiona una aplicación de varios contenedores a partir de una plantilla de un blueprint de vRealize Automation que contiene el componente de contenedor, la configuración de red se integra y está 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.

Prerequisitos

- 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 **Recursos > 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 la 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 En el campo **Nombre**, escriba cualquier valor de cadena.

Cuando termine de crear la nueva configuración, se adjuntará un identificador único al valor de nombre.

- 5 (Opcional) Para añadir ajustes de configuración más detallados, haga clic en la casilla de verificación **Avanzado**.

Aparecen opciones de configuración de red adicionales en el panel Añadir red.

6 Finalice la configuración de la red.

Opción	Descripción	
Configuración de IPAM	Subred	Proporcione valores 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.
Propiedades personalizadas		Opcionalmente, especifique propiedades personalizadas para la nueva configuración de red.
	containers.ipam.driver	<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 infoblox o calico.</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>
	containers.network.driver	<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 bridge, overlay y macvlan, mientras que los controladores de red proporcionados por el host de contenedor virtual (Virtual Container Host, VCH) incluyen el controlador bridge. También puede que estén disponibles controladores de red de terceros, como weave y calico, 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>
Hosts	Especifique los hosts de red, según corresponda.	

NOTA: Si crea la red sin usar la configuración avanzada, vRealize Automation proporciona la configuración automáticamente.

7 Haga clic en **Crear red**.

El panel Añadir 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 conector de red en el borde inferior de los iconos del contenedor.

- 8 (Opcional) Para conectar un contenedor a la red recién añadida, arrastre el icono del conector de red desde el contenedor hasta cualquier punto del icono horizontal que representa a la red.

Añadir una red a una plantilla de contenedor

Puede añadir una configuración de red a una plantilla de contenedor para conectar los contenedores que integran la plantilla. 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.

Prerequisitos

- 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, incluido un icono en blanco con el signo más.
- 6 Coloque el cursor sobre el icono en blanco hasta que aparezca el icono **Añadir red**.
- 7 Haga clic en el icono **Añadir red**.
Se abrirá el panel Añadir red. Puede agregar una red existente, o bien configurar y añadir una red nueva.
- 8 (Opcional) Añada una red existente.
 - a Haga clic en la casilla de verificación **Existente**.
 - b Haga clic en cualquier lugar dentro del campo **Nombre** para mostrar una lista desplegable con las redes existentes.
 - c Seleccione la red y haga clic en **Guardar**.
El panel Añadir 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 conector de red en el borde inferior de los iconos del contenedor.
- 9 (Opcional) Configure y añada una nueva red.
 - a En el campo **Nombre**, escriba cualquier valor de cadena.
Al guardar la nueva configuración, se adjuntará un identificador único al valor de nombre.
 - b Haga clic en la casilla de verificación **Avanzado**.
Aparecen opciones de configuración de red adicionales en el panel Añadir red.

- c Finalice la configuración de la red.

Opción	Descripción	
Configuración de IPAM	Subred	Proporcione valores 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.
Propiedades personalizadas	Opcionalmente, especifique propiedades personalizadas para la nueva configuración de red. Estos nombres de propiedades distinguen mayúsculas de minúsculas.	
	<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 infoblox o calico.
	<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 bridge, overlay y macvlan, mientras que los controladores de red proporcionados por el host de contenedor virtual (Virtual Container Host, VCH) incluyen el controlador bridge. También puede que estén disponibles controladores de red de terceros, como weave y calico, en función de los complementos de red que estén instalados en el host de contenedor.
Hosts	Especifique los hosts de red, según corresponda.	

- d Haga clic en **Crear red**.

El panel Añadir 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 conector de red en el borde inferior de los iconos del contenedor.

- 10 Para conectar un contenedor a la red recién añadida, arrastre el icono del conector de red desde el contenedor hasta cualquier punto del icono horizontal que representa a la red.

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 preparar la compatibilidad con proveedores de IPAM de terceros](#),” página 16.

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](#) página 300

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](#) página 301

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.

Prerequisitos

- Compruebe que ha creado un endpoint de Active Directory. Consulte [“Configurar el complemento Active Directory como un endpoint,”](#) página 270.
- Si usa un servidor de vRealize Orchestrator externo, verifique que esté configurado correctamente. Consulte [“Configurar un servidor de vRealize Orchestrator externo,”](#) página 181.
- Inicie sesión en la consola de 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	Introduzca el valor permanente. El valor no puede incluir espacios ni caracteres especiales. No podrá cambiar este valor más adelante. Solo podrá recrear la política con otro identificador.
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	Introduzca el nombre distintivo de la unidad organizativa para esta política. Se debe introducir la jerarquía como una lista separada por comas. Por ejemplo, ou=development,dc=corp,dc=domain,dc=com.

- 4 Haga clic en **Aceptar**.

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.

Qué hacer a continuación

- 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,”](#) página 155. 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,”](#) página 301.

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,”](#) página 299.

Prerequisitos

- Compruebe que tiene al menos una política de Active Directory. Consulte [“Crear una política de Active Directory,”](#) página 300. 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,”](#) página 155. 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**.

El blueprint de prueba incluye la propiedad personalizada, pero los usuarios no ven esta propiedad en el formulario de solicitud.

Qué hacer a continuación

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.

Proporcionar servicios a petición a los usuarios

4

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 cubre los siguientes temas:

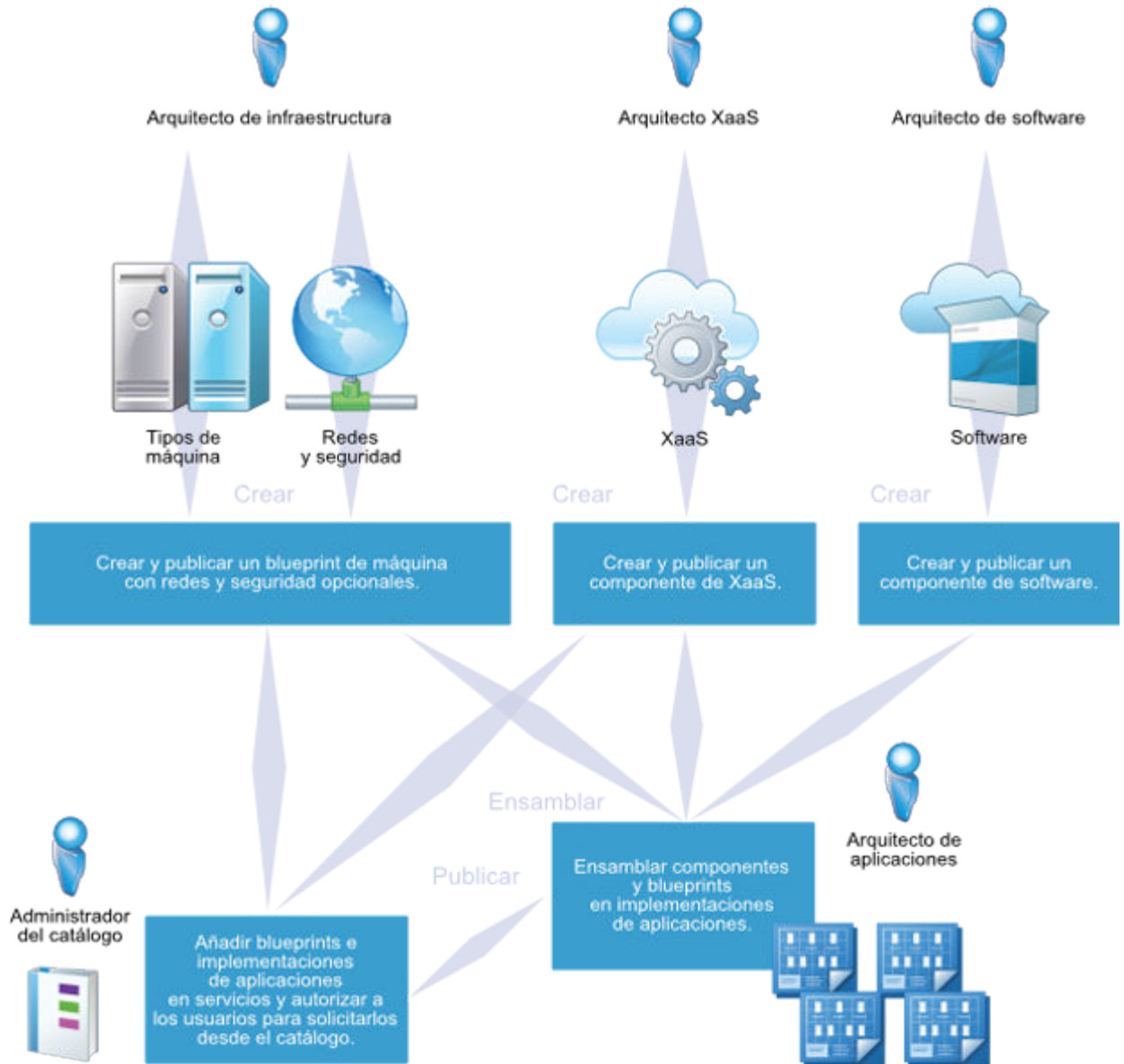
- [“Diseñar blueprints,”](#) página 303
- [“Exportar e importar blueprints,”](#) página 305
- [“Crear la biblioteca de diseño,”](#) página 310
- [“Ensamblar blueprints compuestos,”](#) página 453
- [“Administrar el catálogo de servicios,”](#) página 462

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.

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.

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

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 blueprints de XaaS publicados para crear blueprints de aplicaciones, pero solo en combinación con al menos un componente de máquina.

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 para 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.

Exportar e importar blueprints

Puede exportar 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 contenidos de vRealize Automation:

- Blueprints de aplicaciones y todos sus componentes
- Blueprints de máquinas de IaaS
- Componentes de Software
- Blueprints de XaaS
- 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 4-1. Elegir la herramienta de importación y exportación

Herramienta	Más información
vRealize CloudClient	Consulte el sitio para desarrolladores de VMware en https://developercenter.vmware.com/tool/cloudclient .
API de REST de vRealize Automation	Consulte <i>Guía de programación</i> en el centro de información de vRealize Automation en https://www.vmware.com/support/pubs/vcac-pubs.html .

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 satisficieran las necesidades de su organización.

Prerequisitos

- 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,” página 80.
- 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,” página 217.
- Asigne el perfil de red externa a la reserva de vSphere. Consulte “Crear una reserva para Hyper-V, KVM, SCVMM, vSphere o XenServer,” página 256. 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](#) página 307
 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](#)
página 308

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.

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 en el dispositivo de vRealize Automation mediante SSH.
- 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 la versión 4.x de Cloud Client desde <http://developercenter.vmware.com/tool/cloudclient> en /tmp.
- 4 Descomprima el paquete cloudclient-4x-dist.zip.
- 5 Ejecute Cloud Client en el directorio /bin.

```
$>./bin/cloudclient.sh
```

- 6 Si se le solicita, acepte el contrato de licencia.
- 7 Use Cloud Client para iniciar sesión en el dispositivo de vRealize Automation como usuario con privilegios de **arquitecto de software** y **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
```

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
```

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**.

Ha configurado el blueprint de aplicación de prueba de Dukes Bank para el entorno y ha publicado el blueprint completado.

Qué hacer a continuación

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,”](#) página 463.

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,”](#) página 309.

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.

Prerequisitos

- 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,”](#) página 306.
- 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,”](#) página 463.
- 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 el 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 el 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**.

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.

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.

Tabla 4-2. 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,” página 314
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 de máquina con red y seguridad,” página 339
Software en máquinas	Arquitecto de software	Cree y publique los componentes de Software en la pestaña Software y, a continuación, combínelos con blueprints de máquina en la pestaña Blueprints.	<p>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.</p> <p>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.</p>	“Crear un componente de Software,” página 384

Tabla 4-2. Crear la biblioteca de diseño (Continúa)

Elemento del catálogo	Función	Componentes	Descripción	Detalles
Servicios de TI personalizados	Arquitectos XaaS	Cree y publique blueprints de XaaS en la pestaña XaaS.	<p>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.</p> <p>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.</p>	“Diseñar acciones personalizadas y blueprints XaaS,” página 396
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 	<p>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.</p>	<p>Puede reutilizar componentes y blueprints publicados, combinándolos de nuevas formas para crear paquetes de servicios de TI que proporcionen funciones complejas a los usuarios.</p>	“Ensamblar blueprints compuestos,” página 453

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 Net App 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 [“Crear un endpoint de NetApp ONTAP,”](#) página 197.
- 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.
- 4 Un arquitecto de infraestructura u otro usuario autorizado crea un blueprint para el aprovisionamiento de FlexClone.

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.

Prerequisitos

- Inicie sesión en la consola de 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. [Capítulo 2, “Configurar las opciones de tenant,”](#) página 85.
- Configure los recursos de IaaS. [“Lista de comprobación para la configuración de recursos de IaaS,”](#) página 185.
- 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**.

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.

Qué hacer a continuación

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,”](#) página 453.

Configuración de blueprint de máquina

Conozca las configuraciones y las opciones que se pueden configurar cuando se crean blueprints de máquinas.

Configuración de propiedades de blueprint y de nuevo blueprint

Conozca los ajustes y las opciones que puede configurar en el cuadro de diálogo Nuevo blueprint. Después de crear el blueprint, edite estas opciones en el cuadro de diálogo Propiedades de blueprint.

Pestaña General

Aplice las opciones de configuración en todo el blueprint, incluidos todos los componentes que desea añadir en este momento o posteriormente.

Tabla 4-3. 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.
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.
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.

Pestaña Configuración de NSX

Si ha configurado VMware NSX y ha instalado el complemento NSX para vRealize Automation, puede especificar la configuración de la zona de transporte, política de reserva de puerta de enlace enrutada y de Edge, y 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 Nuevo blueprint y Propiedades de blueprint.

Para obtener información sobre la configuración de NSX, consulte [“Configuración de propiedades de blueprint y de nuevo blueprint con NSX,”](#) página 339.

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 4-4. 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.	
	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.	
	Nombre	Para ver una lista de los nombres de las propiedades personalizadas y sus comportamientos, 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 4-5. 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.
Prefijo de máquina	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. 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.
Instancias: Mínimo y Máximo	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 ingresar el mismo valor en los campos Mínimo y Máximo para configurar exactamente cuántas instancias aprovisionar y deshabilitar las acciones de escalado en ese componente de máquina. 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 deshabilitar las acciones de escalado. Para ello, debe configurar el número exacto de instancias que desea permitir en cada componente de máquina.

Pestaña Información de creación

Configure los ajustes de información de compilación para un componente de máquina de vSphere.

Tabla 4-6. 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 <p>Cree la especificación de componente de máquina sin usar una opción de clonación.</p> ■ Clonar <p>Realice copias de una máquina virtual a partir de una plantilla y un objeto de personalización.</p> ■ Clon vinculado <p>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.</p> <p>El snapshot de máquina virtual identificado en el blueprint debe apagarse antes de aprovisionar las máquinas virtuales de clon vinculado.</p> ■ NetApp FlexClone <p>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.</p>

Tabla 4-6. Pestaña Información de creación (Continua)

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 Aprovisione una máquina sin sistema operativo invitado. ■ ExternalProvisioningWorkflow Cree una máquina iniciándola desde una instancia de máquina virtual o una imagen de nube. ■ LinuxKickstartWorkflow 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. ■ VirtualSccmProvisioningWorkflow 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. ■ WIMImageWorkflow 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>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>
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>

Tabla 4-6. Pestaña Información de creación (Continua)

Configuración	Descripción
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 instantánea) puede generar confusiones. Si selecciona un snapshot existente, esta opción crea un nuevo disco 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. 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 4-7. 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	<p>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.</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>

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 4-8. 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.
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 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,”](#) página 345.

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 propiedades de blueprint y de nuevo blueprint con NSX,”](#) página 339.

Tabla 4-9. 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.
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 deshabilitar 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,”](#) página 345.

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 propiedades de blueprint y de nuevo blueprint con NSX,”](#) página 339.

Tabla 4-10. 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 edición de un blueprint, mediante la página Nuevo blueprint o Propiedades de blueprint, respectivamente.

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 4-11. 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.

Tabla 4-11. Configuración de la pestaña **Propiedades > Propiedades personalizadas** (Continúa)

Configuración	Descripción
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 4-12. 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.
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 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 4-13. 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.

Tabla 4-13. Configuración de la pestaña **General** (Continua)

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.</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.</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 ingresar el mismo valor en los campos Mínimo y Máximo para configurar exactamente cuántas instancias aprovisionar y deshabilitar 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 deshabilitar 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 4-14. 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.</p> <p>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>
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> <ul style="list-style-type: none"> ■ CloneWorkflow <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 4-15. 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 4-16. 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.
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 edición de un blueprint, mediante la página Nuevo blueprint o Propiedades de blueprint, respectivamente.

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 4-17. 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.

Tabla 4-17. Configuración de la pestaña **Propiedades > Propiedades personalizadas** (Continúa)

Configuración	Descripción
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 4-18. 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.
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 4-19. 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.

Tabla 4-19. Configuración de la pestaña **General** (Continua)

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.</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.</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 ingresar el mismo valor en los campos Mínimo y Máximo para configurar exactamente cuántas instancias aprovisionar y deshabilitar 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 deshabilitar 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 4-20. 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>
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>

Tabla 4-20. Pestaña Información de creación (Continúa)

Configuración	Descripción
Habilitar opciones de red de Amazon en la máquina	Elija si desea permitir que los usuarios aprovisionen una máquina en una nube privada virtual (VPC) o en una ubicación no de VPC cuando envíen la solicitud.
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,” página 68 y “Añadir un tipo de instancia de Amazon,” página 68.</p>

Pestaña Recursos de máquinas

Especifique la configuración de CPU, memoria, almacenamiento y volumen de EBS para el componente de máquina de Amazon.

Tabla 4-21. 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 edición de un blueprint, mediante la página Nuevo blueprint o Propiedades de blueprint, respectivamente.

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 4-22. 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 <i>Machine.SSH</i> 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 <i>true</i> 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 <i>Mostrar en solicitud</i> , 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 <i>Reemplazable</i> 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 4-23. 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.
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 4-24. 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.
Prefijo de máquina	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. 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.
Instancias: Mínimo y Máximo	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 ingresar el mismo valor en los campos Mínimo y Máximo para configurar exactamente cuántas instancias aprovisionar y deshabilitar las acciones de escalado en ese componente de máquina. 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 deshabilitar las acciones de escalado. Para ello, debe configurar el número exacto de instancias que desea permitir en cada componente de máquina.

Pestaña Información de creación

Configure las opciones de información de compilación para un componente de máquina de OpenStack.

Tabla 4-25. 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 4-25. Pestaña Información de creación (Continúa)

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 4-26. 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	<p>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.</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>

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 edición de un blueprint, mediante la página Nuevo blueprint o Propiedades de blueprint, respectivamente.

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 4-27. 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.

Tabla 4-27. Configuración de la pestaña **Propiedades > Propiedades personalizadas** (Continúa)

Configuración	Descripción
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 4-28. 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.
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.

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.

Origen

Existen varias causas posibles para los problemas habituales de blueprints de clon y clon vinculado.

Tabla 4-29. 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.	<p>Un usuario de su tenant o grupo empresarial debe solicitar una máquina de vSphere. Puede hacerlo usted mismo si cuenta con las funciones adecuadas.</p> <p>En este cuadro de diálogo, también se ven las máquinas no administradas.</p> <p>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.</p>
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.
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).

Tabla 4-29. Causas de los problemas habituales de blueprints de clon y clon vinculado (Continúa)

Problema	Causa	Solución
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 de máquina con red y seguridad

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.

La configuración de NSX solo se aplica a los tipos de componente de máquina de vSphere.

Configuración de propiedades de blueprint y de nuevo blueprint con NSX

Puede especificar la configuración que se aplicará al blueprint completo. Después de crear el blueprint, edite estas opciones en el cuadro de diálogo Propiedades de blueprint.

Pestaña General

Aplice las opciones de configuración en todo el blueprint, incluidos todos los componentes que desea añadir en este momento o posteriormente.

Tabla 4-30. 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.

Tabla 4-30. Configuración de la pestaña **General** (Continua)

Configuración	Descripción
Descripción	Incluya un resumen del blueprint para proporcionar información a otros arquitectos. Además, los usuarios verán esta descripción en el formulario de solicitud.
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.
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.

Pestaña Configuración de NSX

Si ha configurado VMware NSX y ha instalado el complemento NSX para vRealize Automation, puede especificar la configuración de la zona de transporte, política de reserva de puerta de enlace enrutada y de Edge, y 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 Nuevo blueprint y Propiedades de blueprint.

Para obtener información sobre cómo configurar NSX, consulte la *guía de administración de NSX*.

Tabla 4-31. 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.</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 añade 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 4-32. 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.	
	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.	
	Nombre	Para ver una lista de los nombres de las propiedades personalizadas y sus comportamientos, 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.

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 los cuadros de diálogo 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 vSphere con integración de red y seguridad,”](#) página 190.

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. Los Edges no se pueden añadir a grupos de seguridad, ya que están excluidos 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.

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,”](#) página 345.

Añadir propiedades de red y de seguridad a un componente de máquina

Los componentes de máquina que no son de vSphere no tienen una pestaña Red o Seguridad. Es posible añadir opciones de red y seguridad a componentes de máquina no vSphere en el lienzo de diseño de blueprint mediante propiedades personalizadas.

Los componentes **Redes y seguridad** están disponibles para su utilización únicamente con componentes de máquina de vSphere.

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*.

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 la red y seguridad con vRealize Automation, un administrador de IaaS debe instalar los complementos NSX en vRealize Orchestrator y crear endpoints de vRealize Orchestrator y vSphere.

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 redes y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario tener instalado el complemento NSX y 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 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 redes y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario tener instalado el complemento NSX y 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 a un blueprint, además de los grupos de seguridad especificados en la reserva.

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 del proveedor.

Puede añadir un grupo de seguridad de NSX existente o a petición al lienzo de diseño.

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.

Añadir un componente de grupo de seguridad existente

Puede añadir un componente de grupo de seguridad existente 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.

Se pueden añadir varios componentes de redes y seguridad al lienzo de diseño.

Prerequisitos

- Cree y configure un grupo de seguridad en NSX. Consulte *Configuración de vRealize Automation y la guía de administración de NSX*.
- Compruebe que el complemento de NSX para vRealize Automation esté instalado y que el inventario de NSX se haya ejecutado correctamente para su clúster.

Para usar configuraciones de NSX en vRealize Automation, debe instalar el complemento de NSX y ejecutar la recopilación de datos.
- Inicie sesión en la consola de 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.

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 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.

Prerequisitos

- Cree y configure una política de seguridad en NSX. Consulte la *guía de administración de NSX*.
- Compruebe que el complemento de NSX para vRealize Automation esté instalado y que el inventario de NSX se haya ejecutado correctamente para su clúster.

Para usar configuraciones de NSX en vRealize Automation, debe instalar el complemento de NSX y ejecutar la recopilación de datos.
- Inicie sesión en la consola de 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 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.

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 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.

Se pueden añadir varios componentes de redes y seguridad al lienzo de diseño.

Prerequisitos

- Cree y configure etiquetas de seguridad en NSX. Consulte *Configuración de vRealize Automation y la guía de administración de NSX*.
- Compruebe que el complemento de NSX para vRealize Automation esté instalado y que el inventario de NSX se haya ejecutado correctamente para su clúster.

Para usar configuraciones de NSX en vRealize Automation, debe instalar el complemento de NSX y ejecutar la recopilación de datos.
- Compruebe que el complemento de NSX para vRealize Automation esté instalado y que el inventario de NSX se haya ejecutado correctamente para su clúster.

Para usar configuraciones de NSX en vRealize Automation, debe instalar el complemento de NSX y ejecutar la recopilación de datos.
- Inicie sesión en la consola de 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.

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.

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 redes y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario tener instalado el complemento NSX y 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.

Prerequisitos

- Cree y configure los ajustes de red para NSX. Consulte *Configuración de vRealize Automation* y la *guía de administración de NSX*.
- Compruebe que el complemento de NSX para vRealize Automation esté instalado y que el inventario de NSX se haya ejecutado correctamente para su clúster.
Para usar configuraciones de NSX en vRealize Automation, debe instalar el complemento de NSX y ejecutar la recopilación de datos.
- Cree un perfil de red.
- Inicie sesión en la consola de 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.

Qué hacer a continuación

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.

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.

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.

Prerequisitos

- Cree y configure los ajustes de red para NSX. Consulte *Configuración de vRealize Automation* y la *guía de administración de NSX*.
- Compruebe que el complemento de NSX para vRealize Automation esté instalado y que el inventario de NSX se haya ejecutado correctamente para su clúster.
Para usar configuraciones de NSX en vRealize Automation, debe instalar el complemento de NSX y ejecutar la recopilación de datos.
- Cree un perfil de red.
Por ejemplo, si añade un componente de red con enrutamiento a petición NAT, cree un perfil de red para NAT.

- Inicie sesión en la consola de 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 uno de los componentes de red a petición al lienzo de diseño, en función de si desea configurar un componente de red NAT a petición o un componente de red enrutada a petición.
- 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 añade un componente **Red NAT a petición**, seleccione un perfil de red NAT.

Los siguientes ajustes de red se rellenan en función del perfil de red que elija. 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 (Opcional) Para un componente de red NAT a petición, haga clic en la pestaña **DHCP** para especificar el rango de direcciones IP y los valores de duración de la concesión.

Puede editar los valores de direcciones IP iniciales y finales del rango de DHCP. Cuando la máquina virtual está aprovisionada con DHCP, el adaptador de red asigna una dirección IP a la máquina que está dentro del rango. Es un adaptador de red estático de manera predeterminada. Los valores de dirección IP no pueden coincidir con las direcciones de red o difusión que se usan en la subred asociada. No es posible superponer rangos de IP estáticos.

El DHCP solo está disponible para componentes de red NAT a petición uno a muchos.

- 9 (Opcional) Introduzca un valor de dirección IP inicial en el cuadro de texto **Inicio de rango de IP**.
- 10 (Opcional) Introduzca un valor de dirección IP final en el cuadro de texto **Final de rango de IP**.
- 11 En el cuadro de texto **Tiempo de concesión (segundos)**, especifique una duración de concesión de DHCP en segundos, o bien déjelo en blanco si desea que no exista un límite a la duración de la concesión. Para las redes NAT, también puede cambiar los rangos de IP.

12 (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.

13 Haga clic en **Finalizar** para guardar el blueprint como un borrador o seguir con la configuración del blueprint.

Qué hacer a continuación

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 redes y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario tener instalado el complemento NSX y 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 de equilibradores de carga y la configuración de red VIP del blueprint:

- Si el perfil de red de grupos es NAT, el perfil de red VIP puede ser el mismo perfil de red NAT del mismo 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.

También se crea un recurso de NSX Edge y los detalles del equilibrador de carga, tales como el nivel con carga equilibrada y los servicios configurados, se guardan como propiedades del recurso de Edge.

Añadir un componente de equilibrador de carga a petición

Puede usar un componente de equilibrador de carga a petición para añadir un equilibrador de carga 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.

La configuración de equilibrador de carga distribuye el procesamiento de tareas entre las máquinas aprovisionadas en una red.

Si desea obtener más información sobre cómo crear perfiles de aplicación de NSX para definir el comportamiento de un tipo de tráfico de red específico, consulte la *guía de administración de NSX*.

Prerequisitos

- 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 complemento de NSX para vRealize Automation esté instalado y que el inventario de NSX se haya ejecutado correctamente para su clúster.

Para usar configuraciones de NSX en vRealize Automation, debe instalar el complemento de NSX y ejecutar la recopilación de datos.
- Cree un perfil de red.
- Inicie sesión en la consola de 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 haya, al menos, un componente de máquina de vSphere en el lienzo de 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 **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 máquina en el menú desplegable **Máquina**.
La lista solo contiene los componentes de máquina de vSphere en el blueprint activo.
- 5 Seleccione una NIC y una máquina de vSphere para equilibrar la carga en el menú desplegable **Adaptador de red**.
La lista contiene los NIC que están definidos en el componente de máquina de vSphere seleccionado.
- 6 Seleccione una red VIP en el menú desplegable **Red VIP**.
- 7 (Opcional) Indique la dirección VIP para el NIC a partir de la **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 para VIP desde el perfil de red. Solo puede especificar una dirección IP cuando se crea VIP en una red NAT.
- 8 En la sección Servidores virtuales, active la casilla de verificación situada junto a cada servicio cuya carga desee equilibrar.
Las opciones de servicio son HTTP, HTTPS y TCP.
- 9 (Opcional) Acepte o edite el puerto, el algoritmo, el intervalo de comprobación de estado, el tiempo de espera de respuesta y la URL del supervisor de servicios de cada servicio seleccionado.
- 10 Escriba la dirección del servicio seleccionado en el cuadro de texto **URL de servicio HTTP**.
Solo se dispone de una dirección URL para el control de servicio HTTP de cada equilibrador de carga.
La URL que introduzca se usará para comprobar el estado del servicio. La URL del valor del servicio HTTP no se utiliza para redirigir el tráfico de red.
Escriba la URL de la dirección a la que desea redirigir el tráfico HTTP. Por ejemplo, puede redirigir tráfico de `http://myweb.com` a `https://myweb.com`. El valor que introduzca debe ser igual al valor indicado en la opción **URL de redirección HTTP** de la aplicación NSX.
- 11 Haga clic en **Guardar** para guardar la configuración de blueprint actual o haga clic en **Finalizar** para guardar y salir del blueprint.

Los ajustes configurados están disponibles en la pestaña **Red** del componente de máquina de vSphere asociado.

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.

Prerequisitos

- Inicie sesión en la consola de 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 4-33. 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.

Tabla 4-33. Configuración de la pestaña **Propiedades** para propiedades personalizadas (Continúa)

Configuración	Descripción
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.

Qué hacer a continuación

Puede seguir ajustando la configuración de red de contenedor en la pestaña **Red** de un componente de contenedor 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.

La configuración del componente de redes y seguridad que se añade al lienzo de diseño proviene de la configuración de NSX y, por ello, es necesario tener instalado el complemento NSX y 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*.

Por ejemplo, puede arrastrar un componente de red NAT a petición al lienzo de diseño para que esté disponible en un componente de máquina de vSphere en el 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 4-34. 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 4-35. 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 4-36. 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 4-37. Configuración de la pestaña **Política**

Configuración	Descripción
Política de implementación	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. Es posible añadir una política de implementación mediante la pestaña Contenedores de vRealize Automation.
Tamaño del clúster	Especifique el número de instancias que desea generar como un clúster a partir de este contenedor.
Reiniciar política	
Reinicio máx.	
Recursos de CPU compartidos	Especifique la cantidad de recursos de CPU compartidos 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 que no hay límite.
Intercambio de memoria	
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 4-38. Configuración de la pestaña **Entorno**

Configuración	Descripción
Nombre	
Enlace	
Valor	

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 4-39. 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 4-40. 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 utilizará. 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.

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 4-41. 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 4-42. 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 infoblox o calico.
<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 bridge, overlay y macvlan, mientras que los controladores de red proporcionados por el host de contenedor virtual (Virtual Container Host, VCH) incluyen el controlador bridge. También puede que estén disponibles controladores de red de terceros, como weave y calico, 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 2376.

Tabla 4-42. Propiedades personalizadas de Contenedores (Continúa)

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.

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,”](#) página 359.

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,”](#) página 359.

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](#) página 362

Puede crear blueprints de máquinas virtuales de Microsoft Azure que proporcionen acceso a recursos de máquinas virtuales de Azure.

- [Crear acciones personalizadas de Azure](#) página 368

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.

Prerequisitos

- 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, entre otros campos, los cuadros de texto 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 4-1. Menú del lado derecho del blueprint de Azure

The screenshot shows the configuration interface for an Azure Machine blueprint. The 'Storage' tab is active. Under 'Resource Group', the 'Create New' radio button is selected, and the 'Resource Group Name' is 'RG1-vAficionado'. Under 'Availability Set', the 'None' radio button is selected. A red box highlights the 'Use Existing' option in the 'Resource Group' section, and another red box highlights the 'Value' field in the right panel, which contains 'RG1-vAficionado'. A red arrow points from the 'Use Existing' option to the 'Value' field. The 'Required' dropdown is set to 'No'.

La mayoría de los campos también cuentan con el botón **Opciones avanzadas**. Estas opciones le permiten especificar longitudes de campo e incluso ocultar campos de los usuarios finales.

NOTA: Se deben rellenar los campos obligatorios para 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> <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>

Pestaña	Descripción	Parámetros importantes
		<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>
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> <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	<p>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>	<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> <p>NOTA: Los nombres de cuentas de almacenamiento con guiones bajos u otros caracteres especiales pueden causar errores.</p> <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.
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.

Pestaña	Descripción	Parámetros importantes
		<ul style="list-style-type: none"> ■ Nombre de subred: nombre del dominio de la subred de Azure. ■ Nombre de dirección IP pública: nombre opcional de la construcción de dirección IP pública en Azure que se debe asociar con la interfaz de red aplicable. ■ 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. ■ 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.

- Haga clic en **Finalizar** para guardar la configuración del blueprint y volver a la página Blueprints principal.

Qué hacer a continuación

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.

Prerequisitos

Configure un endpoint de Azure válido para su implementación de vRealize Automation.

Procedimiento

- Seleccione **Diseño > XaaS > Acciones personalizadas**.
- Haga clic en **Nuevo**.
- Acceda a **Orchestrator > Biblioteca > Azure** en la biblioteca de flujos de trabajo de vRealize Orchestrator.
- Seleccione el flujo de trabajo y la carpeta deseados.
- Configure la acción según sus necesidades, al igual que haría con cualquier otra acción personalizada de XaaS.

Escenario: Crear un blueprint de CentOS de vSphere para clonar en Rainpole

Use sus privilegios de arquitecto de IaaS para crear y publicar un blueprint básico para clonar máquinas de CentOS de vSphere.



Después de publicar el blueprint, otros arquitectos podrán usarlo como un componente en nuevos blueprints. Nadie podrá ver el blueprint en el catálogo ni solicitarlo hasta que use sus privilegios de administrador de tenant para hacer que esté disponible para su solicitud.

Procedimiento

- 1 [Escenario: Crear un blueprint para el componente de máquina de Rainpole](#) página 369
Con sus privilegios de arquitecto de IaaS, cree un blueprint y configure el nombre y la descripción de su blueprint de máquina CentOS de vSphere. Se aplica un identificador único al blueprint para que pueda interactuar con los blueprints mediante programación o crear enlaces de propiedades en caso necesario. Como desea que los usuarios tengan cierta flexibilidad con sus concesiones de blueprints, configura el blueprint de tal modo que permita a los usuarios elegir la duración de la concesión, con un valor máximo de un mes.
- 2 [Escenario: Configurar detalles generales para el componente de la máquina Rainpole](#) página 370
Use sus privilegios de arquitecto de IaaS para arrastrar un componente de máquina de vSphere al lienzo de diseño y configurar los detalles generales para las máquinas aprovisionadas mediante el blueprint.
- 3 [Escenario: Especificar la información de compilación del componente de máquina de Rainpole](#) página 370
Use sus privilegios de arquitecto de IaaS para configurar el blueprint para clonar máquinas a partir de la plantilla de CentOS que creó en vSphere.
- 4 [Escenario: Configurar recursos de máquina para máquinas de Rainpole](#) página 371
Use sus privilegios de arquitecto de IaaS para dar a los usuarios unos parámetros mínimos y máximos para la memoria y el número de CPU permitidas. Esto permite conservar recursos a la vez que se adapta a las necesidades de los usuarios.

Escenario: Crear un blueprint para el componente de máquina de Rainpole

Con sus privilegios de arquitecto de IaaS, cree un blueprint y configure el nombre y la descripción de su blueprint de máquina CentOS de vSphere. Se aplica un identificador único al blueprint para que pueda interactuar con los blueprints mediante programación o crear enlaces de propiedades en caso necesario. Como desea que los usuarios tengan cierta flexibilidad con sus concesiones de blueprints, configura el blueprint de tal modo que permita a los usuarios elegir la duración de la concesión, con un valor máximo de un mes.

Procedimiento

- 1 Seleccione **Diseño > Blueprints**.
- 2 Haga clic en el icono **Nuevo** (+).

- 3 Escriba **Centos on vSphere** en el cuadro de texto **Nombre**.
- 4 Revise el identificador único generado.

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.

El campo de identificador se rellena automáticamente en función del nombre que haya introducido.
- 5 Escriba **Golden Standard CentOS machine configuration** en el cuadro de texto **Descripción**.
- 6 Configure un rango de concesión para que los usuarios puedan elegir la duración. Para ello, especifique **1** en el cuadro de texto **Mínimo** y **30** en el cuadro de texto **Máximo**.
- 7 Haga clic en **Aceptar**.

Qué hacer a continuación

Arrastre un componente de máquina de vSphere al lienzo y configúrelo para clonar la plantilla de CentOS que ha creado en vSphere.

Escenario: Configurar detalles generales para el componente de la máquina Rainpole

Use sus privilegios de arquitecto de IaaS para arrastrar un componente de máquina de vSphere al lienzo de diseño y configurar los detalles generales para las máquinas aprovisionadas mediante el blueprint.

Los arquitectos de IaaS son los únicos que tienen permiso para configurar componentes de máquina. Los arquitectos de aplicaciones y Software solo pueden usar componentes de la máquina reutilizando los blueprints de la máquina publicados que usted cree.

Procedimiento

- 1 Haga clic en la categoría **Tipos de máquina** en el panel de navegación izquierdo.

En el panel inferior se muestran tipos de componentes de máquina.
- 2 Arrastre y suelte un componente de máquina de vSphere en el lienzo.
- 3 Escriba **Máquina CentOS estándar maestra** en el cuadro de texto **Descripción**.
- 4 Seleccione **Usar valor predeterminado del grupo** en el menú desplegable **Prefijo de máquina**.

Si tiene previsto importar estos blueprints en los otros entornos, le recomendamos que seleccione el valor predeterminado de grupo en lugar del prefijo de Rainpole específico para evitar configurar el blueprint de modo que funcione con un prefijo de máquina que podría no estar disponible.

Qué hacer a continuación

Configure el componente de máquina para clonar máquinas a partir de la plantilla de CentOS que creó.

Escenario: Especificar la información de compilación del componente de máquina de Rainpole

Use sus privilegios de arquitecto de IaaS para configurar el blueprint para clonar máquinas a partir de la plantilla de CentOS que creó en vSphere.

Configure el componente de máquina para que realice la acción de clonación y seleccione la plantilla que creó como objeto a partir del cual se debe clonar. Establezca la especificación de personalización que creó para evitar los conflictos que puedan surgir si implementa varias máquinas virtuales con configuraciones idénticas.

Procedimiento

- 1 Haga clic en la pestaña **Información de creación**.

- 2 Seleccione si las máquinas aprovisionadas de este blueprint se clasifican como Escritorio o Servidor en el menú desplegable **Tipo de blueprint**.

Esta información solo se usa para mantener un registro y administrar las licencias.

- 3 Seleccione **Clonar** en el menú desplegable **Acción**.
- 4 Seleccione **CloneWorkflow** en el menú desplegable **Flujo de trabajo de aprovisionamiento**.
- 5 Haga clic en el icono **Examinar** al lado del cuadro de texto **Clonar de**.
- 6 Seleccione **Rainpole_centos_63_x86** para clonar máquinas a partir de la plantilla que creó en vSphere.
- 7 Haga clic en **Aceptar**.
- 8 Escriba **Linux** en el cuadro de texto **Especificación de personalización** para usar la especificación de personalización que creó en vSphere.

NOTA: Este valor distingue mayúsculas y minúsculas.

Qué hacer a continuación

Use el blueprint para configurar la memoria de CPU y las opciones de almacenamiento para máquinas aprovisionadas.

Escenario: Configurar recursos de máquina para máquinas de Rainpole

Use sus privilegios de arquitecto de IaaS para dar a los usuarios unos parámetros mínimos y máximos para la memoria y el número de CPU permitidas. Esto permite conservar recursos a la vez que se adapta a las necesidades de los usuarios.

Los arquitectos de software y de aplicaciones no tienen permiso para configurar componentes de máquinas, pero pueden reutilizar blueprints que contengan componentes de máquinas. Cuando termina de editar el componente de máquina, puede publicar el blueprint de su máquina para que otros arquitectos puedan reutilizarlo al diseñar sus propios elementos del catálogo. El blueprint publicado también está disponible para que los administradores del catálogo y los administradores de tenants puedan incluirlo en el catálogo de servicios.

Procedimiento

- 1 Haga clic en la pestaña **Recursos de máquinas**.
- 2 Especifique la configuración de CPU para las máquinas aprovisionadas.
 - a Escriba **1** en el cuadro de texto **Mínimo**.
 - b Escriba **4** en el cuadro de texto **Máximo**.
- 3 Especifique la configuración de memoria para las máquinas aprovisionadas.
 - a Escriba **1024** en el cuadro de texto **Mínimo**.
Este campo se rellena automáticamente según la memoria de la plantilla.
 - b Escriba **4096** en el cuadro de texto **Máximo**.
- 4 Especifique la configuración de almacenamiento para las máquinas aprovisionadas.
Algunos datos de almacenamiento se rellenan en función de la configuración de la plantilla, pero puede añadir almacenamiento adicional.
 - a Haga clic en el icono **Nuevo** (+).
 - b Escriba **10** en el cuadro de texto **Capacidad (GB)**.
 - c Haga clic en **Aceptar**.

- 5 Haga clic en **Finalizar**.
- 6 Seleccione la fila que contiene CentOS en vSphere y haga clic en **Publicar**.

Ha creado un blueprint listo para el catálogo para proporcionar a los usuarios máquinas CentOS de vSphere clonadas y para reutilizarlo en otros blueprints como estándar de máquinas CentOS.

Qué hacer a continuación

Use sus privilegios de administrador de tenant para crear un servicio del catálogo para que los arquitectos validen sus blueprints. Publique el blueprint de máquina CentOS en vSphere como un elemento del catálogo y solicite que verifique su trabajo.

Escenario: Convertir la máquina de Rainpole en base para suministrar componentes de Software

Con sus privilegios de arquitecto de IaaS, cree un blueprint que admita componentes de Software mediante un snapshot de su máquina aprovisionada como máquina de referencia de la que se realizará el clon. Como quiere que se admitan componentes de Software, deberá instalar el agente invitado y el agente de arranque en su máquina aprovisionada antes de tomar el snapshot.



Procedimiento

- 1 [Escenario: Instalar el agente invitado y el agente de arranque de Software en su máquina de Rainpole](#) página 372

Con los privilegios de administrador de grupo empresarial, inicie sesión en la máquina Rainpole001 que aprovisionó como usuario de prueba. Instale el agente invitado y el agente de arranque de Software en su máquina para preparar el aprovisionamiento de Software. Cuando termine, tome un snapshot de la máquina que va a usar como base para clonar las máquinas que va a usar con componentes de Software.

- 2 [Escenario: Crear un blueprint de clon vinculado basado en su instantánea de Rainpole](#) página 373

Con sus privilegios de arquitecto de IaaS, desea proporcionar a los arquitectos de Software copias que hagan un uso eficiente del espacio de la máquina CentOS aprovisionada que ha preparado.

Escenario: Instalar el agente invitado y el agente de arranque de Software en su máquina de Rainpole

Con los privilegios de administrador de grupo empresarial, inicie sesión en la máquina Rainpole001 que aprovisionó como usuario de prueba. Instale el agente invitado y el agente de arranque de Software en su máquina para preparar el aprovisionamiento de Software. Cuando termine, tome un snapshot de la máquina que va a usar como base para clonar las máquinas que va a usar con componentes de Software.

Procedimiento

- 1 Seleccione **Elementos > Máquinas**.
- 2 Haga clic en su CentOS en el elemento vSphere para ver los detalles del elemento.
- 3 Haga clic en **Conectar con la consola remota** en el menú Acciones de la derecha.

- 4 Inicie sesión en la máquina como usuario raíz.
- 5 Descargue el script de instalación desde su 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
```
- 6 Convierta el script `prepare_vra_template.sh` en ejecutable.

```
chmod +x prepare_vra_template.sh
```
- 7 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.
- 8 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.
- 9 Vuelva a la consola de vRealize Automation y cree el snapshot.
 - a Haga clic en **Crear snapshot** en el menú Acciones de la derecha y siga las indicaciones.
 - b Haga clic en la pestaña **Snapshots** para supervisar el proceso.

Ha instalado el agente de arranque del software y el agente invitado, de modo que el snapshot se puede usar como clon base en los blueprints que contengan componentes de software.

Escenario: Crear un blueprint de clon vinculado basado en su instantánea de Rainpole

Con sus privilegios de arquitecto de IaaS, desea proporcionar a los arquitectos de Software copias que hagan un uso eficiente del espacio de la máquina CentOS aprovisionada que ha preparado.

Debe copiar el CentOS existente en el blueprint de vSphere y editar la copia para crear copias de clon vinculado del snapshot que ha preparado. 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 Seleccione **Diseño > Blueprints**.
- 2 Seleccione la fila que contiene CentOS en vSphere y haga clic en **Copiar**.

Ha creado una copia independiente del blueprint de máquina CentOS en vSphere.
- 3 Escriba **CentOS for Software Testing** en el cuadro de texto **Nombre**.
- 4 Escriba **Space-efficient vSphere CentOS for software testing** en el cuadro de texto **Descripción**.
- 5 Haga clic en **Aceptar**.
- 6 Seleccione el componente de máquina en el lienzo para editar los detalles.
- 7 Haga clic en la pestaña **Información de creación**.
- 8 Seleccione **Clon vinculado** en el menú desplegable **Acción**.
- 9 Haga clic en el icono **Examinar** al lado del cuadro de texto **Clonar de**.

- 10 Seleccione la máquina aprovisionada **Rainpole001** en la que instaló los agentes invitados y de arranque de software.
- 11 Seleccione el snapshot en el menú desplegable **Clonar desde snapshot**.
- 12 Haga clic en **Finalizar**.
- 13 Seleccione la fila que contiene CentOS para pruebas de software y haga clic en **Publicar**.

Ha creado un blueprint de clon vinculado que usted y sus arquitectos pueden usar para proporcionar software a máquinas CentOS.

Qué hacer a continuación

Use sus privilegios de arquitecto de software para crear un componente de Software para instalar MySQL.

Añadir soporte para la conexión RDP a los blueprints de máquina de Windows

Si desea permitir que los administradores del catálogo autoricen a los usuarios a la acción Conectar mediante RDP en los blueprints de Windows, debe añadir las propiedades personalizadas de RDP al blueprint de la máquina, y referenciar el archivo RDP personalizado al administrador del sistema 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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 179.
- 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
(Obligatorio) <code>RDP.File.Name</code>	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.
(Obligatorio) <code>VirtualMachine.Rdp.SettingN</code>	Define una configuración de RDP específica. <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 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:3. Use esta propiedad para abrir un vínculo RDP para especificar una configuración. Para ver una lista de las configuraciones disponibles y la sintaxis adecuada, consulte la documentación sobre RDP de Microsoft Windows.
<code>VirtualMachine.Admin.NameCompletion</code>	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 que contiene su blueprint y haga clic en **Publicar**.

Sus administradores del catálogo puede autorizar a los usuarios a 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.

Escenario: 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. Para ello, debe editar el blueprint CentOS de vSphere 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
- Deshabilitar la cuenta de AD
- Cambiar el nombre de la cuenta de AD
- Mover la cuenta de AD a otra unidad organizativa (OU) de AD

Prerequisitos

NOTA: Esta información no se aplica a Amazon Web Services.

- Inicie sesión en la consola de 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, deshabilitar, 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 [“Escenario: Crear un blueprint de CentOS de vSphere para clonar en Rainpole,”](#) página 369.

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 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
Plugin.AdMachineCleanup.UserName	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, deshabilitar y mover cuentas de Active Directory, y cambiarles el nombre. El nombre de usuario debe tener el formato dominio\nombre de usuario.
Plugin.AdMachineCleanup.Password	Escriba la contraseña de la cuenta de Active Directory en el cuadro de texto Valor .
Plugin.AdMachineCleanup.Delete	Establézcala en True para eliminar las cuentas de las máquinas destruidas, en lugar de deshabilitarlas.
Plugin.AdMachineCleanup.MoveToOU	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>).
Plugin.AdMachineCleanup.RenamePrefix	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**.

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **arquitecto de infraestructura**.
- Cree un blueprint de máquina. Consulte [“Escenario: Crear un blueprint de CentOS de vSphere para clonar en Rainpole,”](#) página 369.

Procedimiento

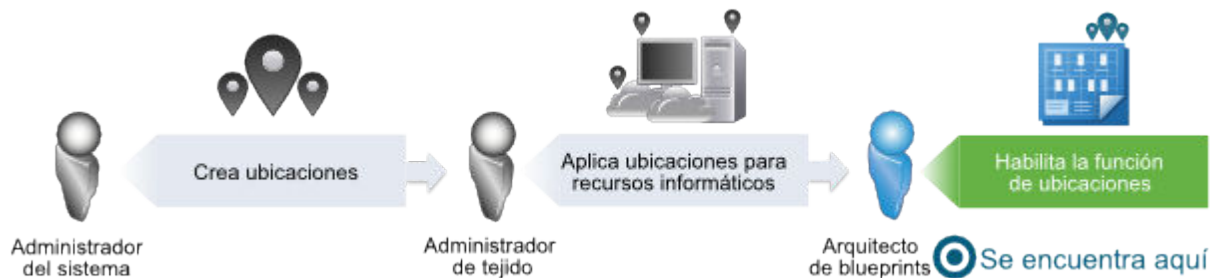
- 1 Seleccione **Diseño > Blueprints**.
- 2 Apunte al blueprint **Centos en vSphere** y haga clic en **Editar**.
- 3 Seleccione el componente de máquina en el lienzo para mostrar la pestaña de detalles.
- 4 Haga clic en la pestaña **Propiedades**.
- 5 Haga clic en **Nueva propiedad**.
- 6 Escriba **Hostname** 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**.

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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 179.
- 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,”](#) página 268.
- Cree un blueprint de máquina. Consulte [“Escenario: Crear un blueprint de CentOS de vSphere para clonar en Rainpole,”](#) página 369.

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**.

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 componentes 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 4-43. 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 Referencia de la API de vRealize Automation*.
- 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 4-44. 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. 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_N% donde N 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 =</code> <code>"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</code> <code>\$cheetah_tgz_url</code>
	Símbolo del sistema de Windows - <code>%cheetah_tgz_url</code> <code>%</code>	<code>start /wait</code> <code>c:\unzip.exe</code> <code>%cheetah_tgz_url</code> <code>%</code>
	Windows PowerShell - <code>\$cheetah_tgz_url</code>	<code>& c:\unzip.exe</code> <code>\$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 4-45. 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 4-46. 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"

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.

Prerequisitos

Inicie sesión en la consola de 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.

a Haga clic en el icono **Añadir** (+).

b Escriba un nombre para la propiedad.

c Escriba una descripción para la propiedad.

Esta descripción se muestra a los arquitectos que usan el componente de Software en los blueprints.

d Seleccione el tipo esperado para el valor de la propiedad.

e 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 4-47. 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	■ return 0 ■ exit 0	■ 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**.

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.

Qué hacer a continuación

Añada su componente de Software publicado a un blueprint de aplicación. Consulte [“Ensamblar blueprints compuestos,”](#) página 453.

Escenario: Crear un componente de Software MySQL para Rainpole

Mediante el uso de sus privilegios de arquitecto de software, cree un componente de Software MySQL para instalar MySQL en máquinas de vSphere CentOS. Cuando diseña el componente de Software MySQL para una máquina virtual de CentOS, configura los parámetros de instalación, configuración e inicio, además de los scripts para los sistemas operativos Linux.

Procedimiento

- 1 Seleccione **Diseño > Componentes de software**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Escriba **MySQL para máquinas virtuales de Linux** en el cuadro de texto **Nombre**.
- 4 Compruebe que se rellene el identificador en función del nombre proporcionado.
Por ejemplo, Software.MySQLparamáquinasvirtualesdeLinux.
- 5 Escriba **Instalación y configuración de MySQL** en el cuadro de texto **Descripción**.
- 6 Seleccione **Máquina** en el menú desplegable **Contenedor**.

Como solo quiere que MySQL se instale directamente en una máquina, impida que los arquitectos coloquen su componente de Software MySQL sobre otros componentes de Software.
- 7 Haga clic en **Siguiente**.
- 8 Haga clic en **Nuevo** y añada y configure cada una de las siguientes propiedades para el script de instalación.

Haga clic en **Aceptar** para guardar cada propiedad.

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.

Nombre	Descripción	Tipo	Valor	Cifrada	Permitir reemplazo	Obligatoria	Computada
db_root_username	Nombre de usuario raíz de la base de datos	Cadena	root	No	Sí	Sí	No
JAVA_HOME	Directorio donde se instala JRE 1.8 o posterior	Cadena	/opt/vmware-jre	No	Sí	Sí	No
global_ftp_proxy	URL del proxy FTP, si lo hay. No es necesaria.	Cadena		No	Sí	No	No
db_port	Puerto de base de datos MySQL	Cadena		No	Sí	Sí	No
db_root_password	Contraseña de usuario raíz de la base de datos	Cadena	contraseña	Sí	Sí	Sí	No

Nombre	Descripción	Tipo	Valor	Cifrada	Permitir reemplazo	Obligatoria	Computada
global_http_proxy	URL del proxy HTTP, si lo hay. No es necesaria.	Cadena		No	Sí	No	No
global_https_proxy	URL del proxy HTTPS, si lo hay. No es necesaria.	Cadena		No	Sí	No	No
max_allowed_packet_size	Tamaño máximo permitido de paquete de servidor	Integer	1024	No	Sí	No	No

9 Haga clic en **Siguiente**.

10 Configure la acción Instalar.

- a Seleccione **Bash** en el menú desplegable **Tipo de script**.
- b Haga clic en **Haga clic aquí para editar**.

- c Pegue el siguiente script.

```
#!/bin/bash

#Setting proxies
export ftp_proxy=${ftp_proxy:-$global_ftp_proxy}
echo "Setting ftp_proxy to $ftp_proxy"

export http_proxy=${http_proxy:-$global_http_proxy}
echo "Setting http_proxy to $http_proxy"

export https_proxy=${https_proxy:-$global_https_proxy}
echo "Setting https_proxy to $https_proxy"

#
# Determine operating system and version
#
export OS=
export OS_VERSION=

if [ -f /etc/redhat-release ]; then
    # For CentOS the result will be 'CentOS'
    # For RHEL the result will be 'Red'
    OS=$(cat /etc/redhat-release | awk '{print $1}')

    if [ -n $OS ] && [ $OS = 'CentOS' ]; then
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $3}')
    else
        # RHEL
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $7}')
    fi

elif [ -f /etc/SuSE-release ]; then
    OS=SuSE

    MAJOR_VERSION=$(cat /etc/SuSE-release | grep VERSION | awk '{print $3}')
    PATCHLEVEL=$(cat /etc/SuSE-release | grep PATCHLEVEL | awk '{print $3}')

    OS_VERSION="$MAJOR_VERSION.$PATCHLEVEL"

elif [ -f /usr/bin/lsb_release ]; then
    # For Ubuntu the result is 'Ubuntu'
    OS=$(lsb_release -a 2> /dev/null | grep Distributor | awk '{print $3}')
    OS_VERSION=$(lsb_release -a 2> /dev/null | grep Release | awk '{print $2}')

fi

echo "Using operating system '$OS' and version '$OS_VERSION'"

if [ "x${global_http_proxy}" == "x" ] || [ "x${global_https_proxy}" == "x" ] ||
    [ "x${global_ftp_proxy}" == "x" ]; then
    echo ""
    echo "#####"
    echo "# One or more PROXY(s) not set. Network downloads may fail #"
    echo "#####"
    echo ""

```

```

fi

export PATH=$PATH:
$JAVA_HOME/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
set -e

# Tested on CentOS
if [ -x /usr/sbin/selinuxenabled ] && /usr/sbin/selinuxenabled; then
    # SELinux can be disabled by setting "/usr/sbin/setenforce Permissive"
    echo 'SELinux is enabled on this VM template. This service requires SELinux to be
disabled to install successfully'
    exit 1
fi

if [ "$OS" != "x" ] && [ "$OS" = 'Ubuntu' ]; then
    # Fix the linux-firmware package
    export DEBIAN_FRONTEND=noninteractive
    apt-get install -y linux-firmware < /dev/console > /dev/console
    # Install MySQL package
    apt-get install -y mysql-server
else
    yum --nogpgcheck --noplugins -y install -x MySQL-server-community mysql-server
fi

# Set Install Path to the default install path (For monitoring)
Install_Path=/usr
echo Install_Path is set to $Install_Path, please modify this script if the install path
is not correct.

```

- d Haga clic en **Aceptar**.
- 11 Configure la acción Configurar.
- a Seleccione **Bash** en el menú desplegable **Tipo de script**.
 - b Haga clic en **Haga clic aquí para editar**.

- c Pegue el siguiente script.

```
#!/bin/bash

#Setting proxies
export ftp_proxy=${ftp_proxy:-$global_ftp_proxy}
echo "Setting ftp_proxy to $ftp_proxy"

export http_proxy=${http_proxy:-$global_http_proxy}
echo "Setting http_proxy to $http_proxy"

export https_proxy=${https_proxy:-$global_https_proxy}
echo "Setting https_proxy to $https_proxy"

#
# Determine operating system and version
#
export OS=
export OS_VERSION=

if [ -f /etc/redhat-release ]; then
    # For CentOS the result will be 'CentOS'
    # For RHEL the result will be 'Red'
    OS=$(cat /etc/redhat-release | awk '{print $1}')

    if [ -n $OS ] && [ $OS = 'CentOS' ]; then
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $3}')
    else
        # RHEL
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $7}')
    fi

elif [ -f /etc/SuSE-release ]; then
    OS=SuSE

    MAJOR_VERSION=$(cat /etc/SuSE-release | grep VERSION | awk '{print $3}')
    PATCHLEVEL=$(cat /etc/SuSE-release | grep PATCHLEVEL | awk '{print $3}')

    OS_VERSION="$MAJOR_VERSION.$PATCHLEVEL"

elif [ -f /usr/bin/lsb_release ]; then
    # For Ubuntu the result is 'Ubuntu'
    OS=$(lsb_release -a 2> /dev/null | grep Distributor | awk '{print $3}')
    OS_VERSION=$(lsb_release -a 2> /dev/null | grep Release | awk '{print $2}')

fi

echo "Using operating system '$OS' and version '$OS_VERSION'"

if [ "x${global_http_proxy}" == "x" ] || [ "x${global_https_proxy}" == "x" ] ||
    [ "x${global_ftp_proxy}" == "x" ]; then
    echo ""
    echo "#####"
    echo "# One or more PROXY(s) not set. Network downloads may fail #"
    echo "#####"
    echo ""

```

```

fi

export PATH=$PATH:
$JAVA_HOME/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
set -e

# Locate the my.cnf file
my_cnf_file=
if [ -f /etc/my.cnf ]; then
    my_cnf_file=/etc/my.cnf
elif [ -f /etc/mysql/my.cnf ]; then
    my_cnf_file=/etc/mysql/my.cnf
fi

if [ "x$my_cnf_file" = "x" ]; then
    echo "Neither /etc/my.cnf nor /etc/mysql/my.cnf can be found, stopping configuration"
    exit 1
fi

# update mysql configuration to handle big packets
sed -ie "s/\[mysqld\]/\[mysqld\]\n\
max_allowed_packet=$max_allowed_packet/g" $my_cnf_file
# update listening port
sed -ie "s/\[mysqld\]/\[mysqld\]\n\
port=$db_port/g" $my_cnf_file

sed -i "s/port.*=[0-9]*/port=$db_port/g" $my_cnf_file

if [ "x$OS" != "x" ] && [ "$OS" = 'Ubuntu' ]; then
    # Make sure that MySQL is started
    service mysql restart
else
    # set up auto-start on booting
    chkconfig mysqld on
    # restart mysqld service
    service mysqld start
fi

# this will assign a password for mysql admin user 'root'
mysqladmin -u $db_root_username password $db_root_password

```

d Haga clic en **Aceptar**.

12 Configure la acción Iniciar.

- a Seleccione **Bash** en el menú desplegable **Tipo de script**.
- b Haga clic en **Haga clic aquí para editar**.
- c Pegue el siguiente script.

```
#!/bin/sh
```

```
echo "The maximum allowed packet size is: "
```

d Coloque el cursor entre los dos puntos y el signo de comillas.

- e Seleccione **max_allowed_packet_size** en el menú desplegable **Seleccione una propiedad para insertar**.

Ahora el script incluye la propiedad.

```
#!/bin/sh
```

```
echo "The maximum allowed packet size is: $max_allowed_packet_size"
```

- f Haga clic en **Aceptar**.
- 13 Haga clic en **Siguiente**.
- 14 Haga clic en **Finalizar**.
- 15 Seleccione la fila que contiene MySQL para máquinas virtuales de Linux y haga clic en **Publicar**.

Su componente de Software MySQL está disponible para otros arquitectos en la página de diseño de blueprint, pero no puede poner a disposición los componentes de Software hasta que los combine con una máquina.

Qué hacer a continuación

Mediante el uso de sus privilegios de arquitecto de software, arquitecto de aplicaciones o arquitecto de IaaS, combine su componente de MySQL con CentOS para blueprint de máquina de Software.

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 4-48. 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 4-48. Configuración general del nuevo Software (Continua)

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 anidarlos en otro componente de Software que haya creado.

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 4-49. 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,” página 380 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,” página 382 y “Crear enlaces de propiedad entre componentes de blueprint,” página 457.

Tabla 4-49. Propiedades de nuevo Software (Continua)

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 <code>echo</code> 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 4-50. 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	■ return 0 ■ exit 0	■ 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.

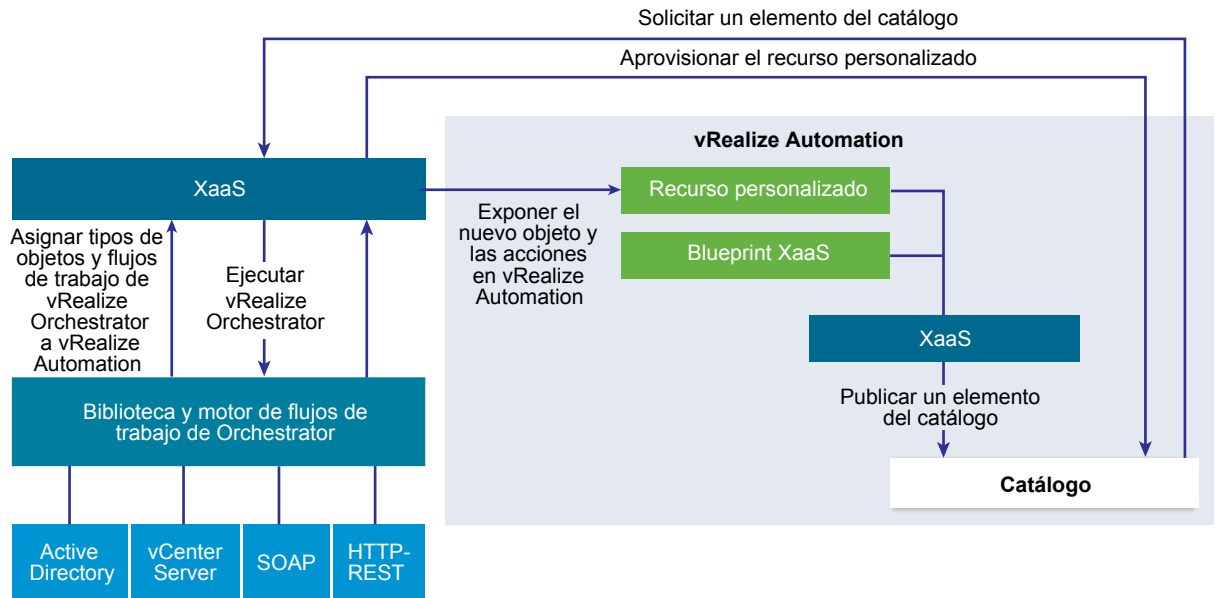
Si utiliza un blueprint como componente de otro blueprint, puede configurarlo de modo que se escale cuando aplique al blueprint implementado un escalado vertical u horizontal.

Integración de vRealize Orchestrator en vRealize Automation

vRealize Orchestrator es el motor de flujos de trabajo integrado en vRealize Automation.

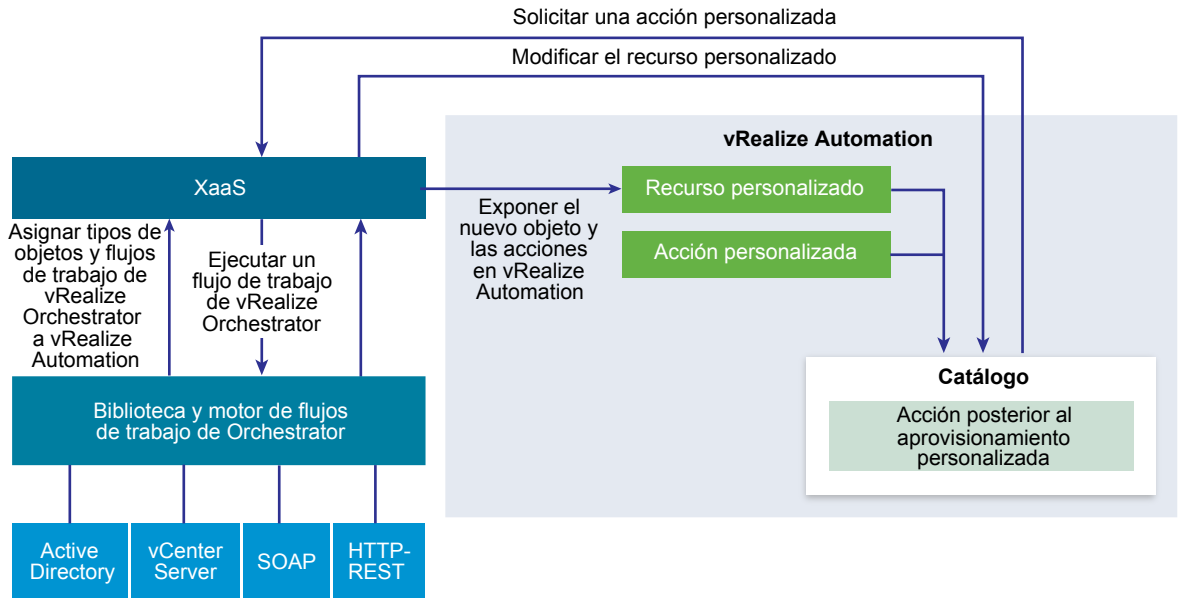
El servidor de vRealize Orchestrator distribuido con vRealize Automation está preconfigurado y, por lo tanto, cuando el administrador del sistema implementa el dispositivo de vRealize Automation, el servidor de vRealize Orchestrator está listo y en ejecución.

Figura 4-2. 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 4-3. 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 4-51. 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.
__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 VMware 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 4-52. 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.

Tabla 4-52. Complementos incluidos de forma predeterminada en vRealize Orchestrator (Continúa)

Complemento	Propósito
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.
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™.

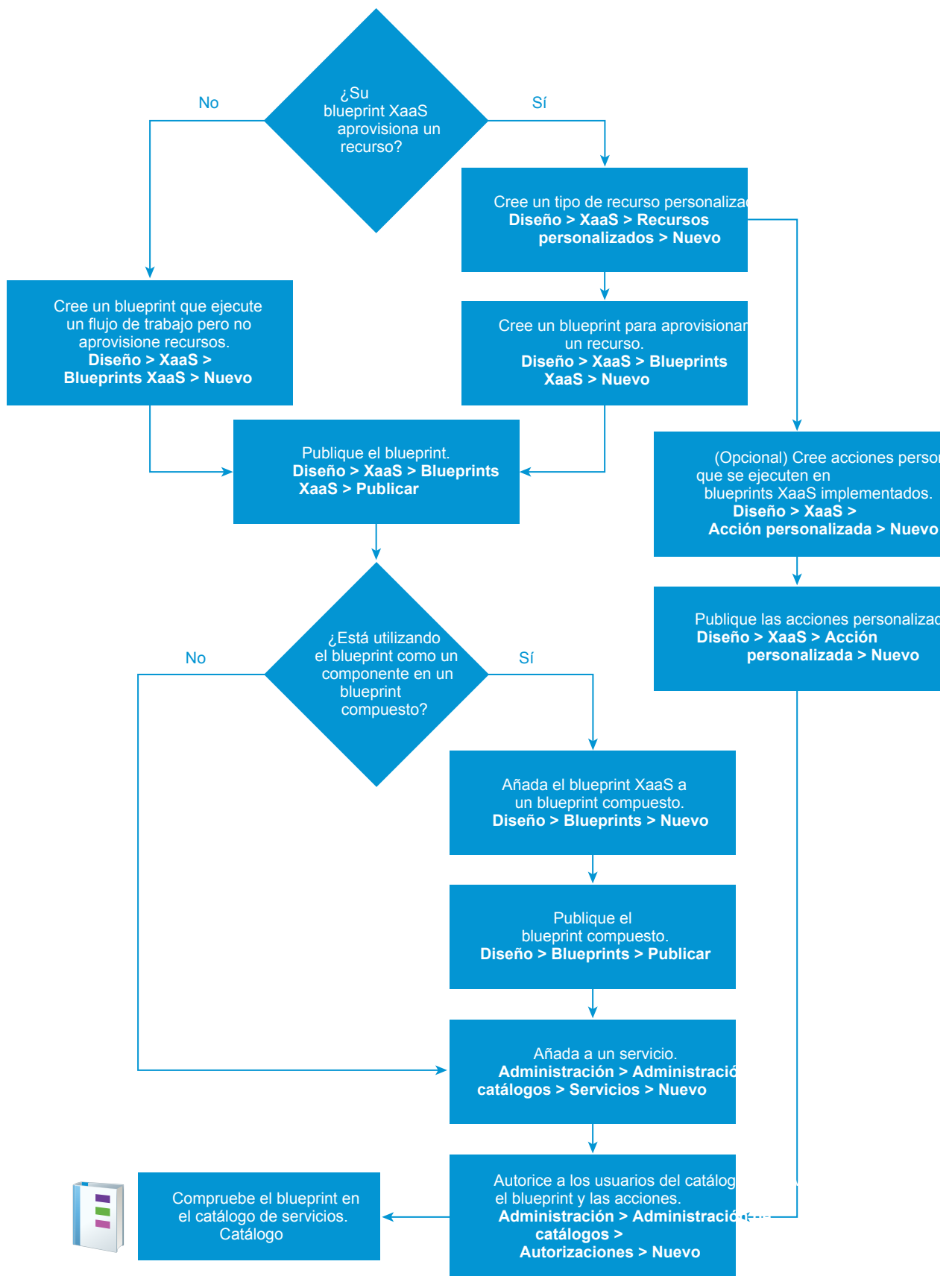
Crear blueprints de XaaS y acciones personalizadas

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	<p>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.</p> <p>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.</p>
Blueprint de no 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, 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.</p> <p>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.</p>
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 aprovisione 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 4-53. 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,”](#) página 426.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 406.

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**.

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.

Qué hacer a continuación

- Cree un blueprint XaaS. Consulte [“Añadir un blueprint XaaS,”](#) página 408.
- Cree una acción personalizada de XaaS. Consulte [“Crear una acción personalizada de XaaS,”](#) página 415.

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 4-54. 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 <code>VC:VirtualMachine</code>.</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 <code>versión_principal.versión_secundaria.revisión_mínima</code>.</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,”](#) página 426.

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 4-55. 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](#) página 408

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](#) página 415

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,”](#) página 438.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 405. 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,”](#) página 429.
- Utilice la información de las opciones detalladas para configurar el blueprint. Consulte [“Opciones del asistente para editar o crear nuevo blueprint XaaS,”](#) página 409.

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**.

Ha creado y publicado un blueprint XaaS.

Qué hacer a continuación

- 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,”](#) página 465.
- Para utilizar este blueprint como un componente en un blueprint compuesto, consulte [“Añadir un blueprint XaaS a un blueprint compuesto,”](#) página 415.

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,”](#) página 408.

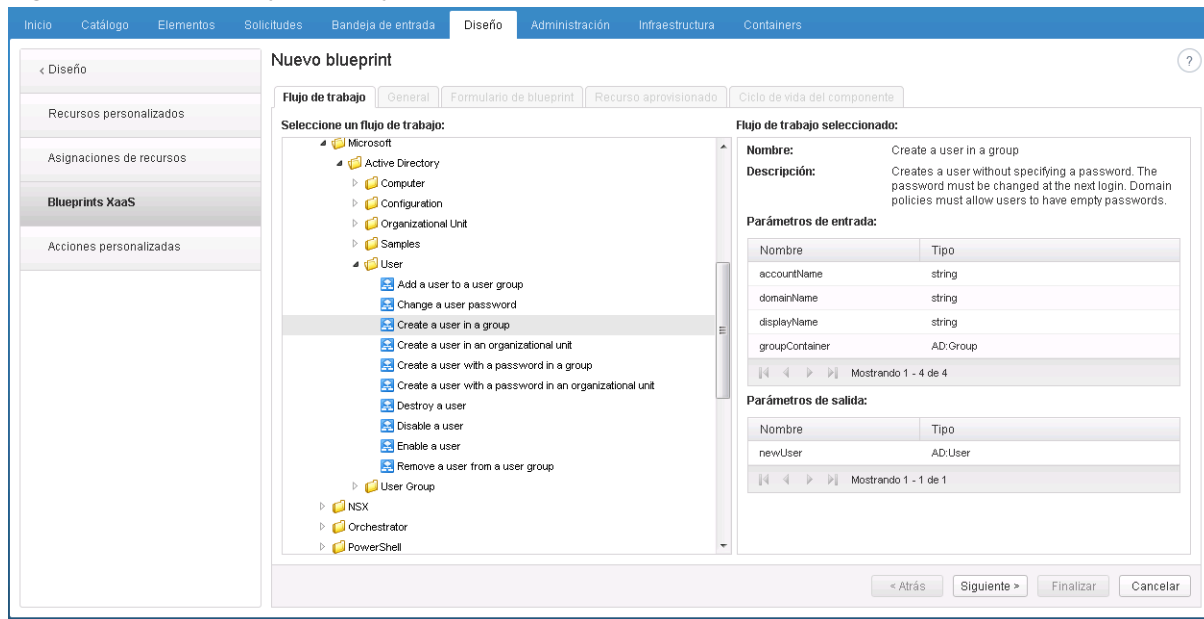
Para utilizar este asistente, seleccione **Diseño > XaaS > Blueprints XaaS**.

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 4-4. 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 4-56. 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	Proporcione una descripción detallada que le permita a diferenciar entre elementos similares.
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.

Tabla 4-56. Opciones de la pestaña General (Continúa)

Opción	Descripción
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,”](#) página 429.

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 4-57. 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 4-58. Opciones de Ciclo de vida del componente

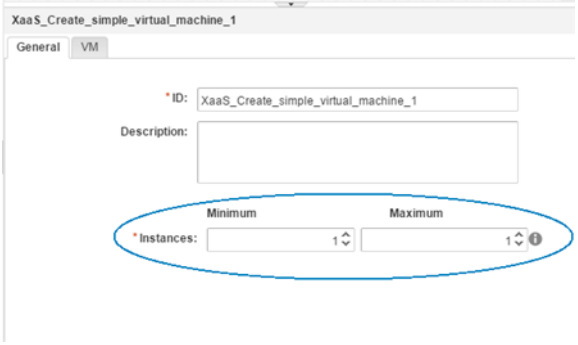
Opción	Descripción
Escalable	<p>Seleccione esta opción para permitir al usuario del catálogo de servicios cambiar el número de instancias de este componente de blueprint después de su implementación como parte de una operación de escalado vertical o escalado horizontal.</p> <p>Esta opción está disponible 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 esta 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>
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>.

Tabla 4-58. Opciones de Ciclo de vida del componente (Continua)

Opción	Descripción
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>.
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 <code>VC:VirtualMachine</code>, el flujo de trabajo de destrucción debe incluir un parámetro de entrada cuyo tipo sea <code>VC:VirtualMachine</code>.</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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **arquitecto de infraestructura**.
- Cree y publique un blueprint XaaS. Consulte [“Crear un blueprint XaaS,”](#) página 407. 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,”](#) página 421.

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**.

El blueprint XaaS ahora forma parte del blueprint compuesto.

Qué hacer a continuación

Añada el blueprint compuesto a un servicio. Consulte [“Administrar el catálogo de servicios,”](#) página 462.

Crear una acción personalizada de XaaS

La acción personalizada se crea para poder administrar los elementos aprovisionados mediante flujos de trabajo de vRealize Orchestrator.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **arquitecto XaaS**.
- Compruebe que dispone de un recurso personalizado que admita la acción. Consulte [“Añadir un recurso personalizado de XaaS,”](#) página 405.

- 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,”](#) página 419.

Procedimiento

1 [Crear una acción personalizada](#) página 416

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](#) página 418

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](#) página 418

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,”](#) página 434.

Prerequisitos

- Inicie sesión en la consola de 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 .

Opción	Acción
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**.

Ha creado una acción personalizada, que ahora aparece recogida en la página Acciones personalizadas.

Qué hacer a continuación

Publicar la acción personalizada. Consulte [“Publicar una acción personalizada,”](#) página 418.

Publicar una acción personalizada

La acción personalizada recién publicada tiene el estado de borrador y se debe publicar.

Prerequisitos

Inicie sesión en la consola de 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**.

El estado de la acción personalizada cambiará a Publicada.

Qué hacer a continuación

Asigne un icono a la acción personalizada. Consulte [“Asignar un icono a una acción de recursos de XaaS,”](#) página 418. 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.

Existe un problema conocido al actualizar el icono de las acciones personalizadas de XaaS. Para obtener detalles, consulte el artículo 2149050 de la base de conocimientos de VMware en <http://kb.vmware.com/kb/2149050>.

Prerequisitos

Inicie sesión en la consola de 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**.

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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 419

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.sekundaria.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 4-59. 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 4-60. 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 escriben una URL.
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

Tabla 4-60. Campos nuevos en el formulario de acción personalizada o de blueprint de XaaS (Continúa)

Campo	Descripción
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 especificadas en el flujo de trabajo de vRealize Orchestrator.

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. Al usar estas condiciones, se pueden crear diversas cláusulas y expresiones y aplicarlas al estado o a las restricciones del elemento.
Externo	Seleccione una acción de script de vRealize Orchestrator para definir el valor.

Tabla 4-61. Restricciones del diseñador de formularios

Restricción	Descripción
Obligatorio	Indica si el elemento es obligatorio.
Solo lectura	Indica si el campo es de solo lectura.
Valor	Permite establecer un valor para el elemento.
Visible	Indica si el consumidor va a poder ver el elemento.
Longitud mínima	Permite establecer un número mínimo de caracteres del elemento de entrada de cadena.

Tabla 4-61. Restricciones del diseñador de formularios (Continúa)

Restricción	Descripción
Longitud máxima	Permite establecer un número máximo permitido de caracteres del elemento de entrada de cadena.
Valor mínimo	Permite establecer un valor mínimo del elemento de entrada de número.
Valor máximo	Permite establecer un valor máximo del elemento de entrada de número.
Incremento	Permite establecer 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	Permite establecer un recuento mínimo de elementos que se puede seleccionar. Por ejemplo, cuando añada o edite una Lista de casillas , puede establecer el número mínimo de casillas que el consumidor debe seleccionar para continuar.
Cantidad máxima	Permite establecer un recuento máximo de elementos que se puede seleccionar. Por ejemplo, cuando añada o edite una Lista de casillas , puede establecer el número máximo de casillas que el consumidor debe seleccionar para continuar.

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 4-62. 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.
Valor	Define un valor personalizado estático con etiquetas.
Valores externos	Seleccione una acción de script de vRealize Orchestrator para definir 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.

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](#) página 427

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](#) página 427

Puede añadir una nueva página para reorganizar el formulario en varias pestañas.

- [Insertar un encabezado de sección en un formulario de recurso personalizado](#) página 428

Puede insertar un encabezado de sección para dividir el formulario en dos secciones.

- [Insertar un elemento de texto en un formulario de recurso personalizado](#) página 428

Puede insertar un cuadro de texto para añadir información descriptiva al formulario.

- [Insertar un campo definido externamente en un formulario de recurso personalizado](#) página 428

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Añadir un recurso personalizado de XaaS,”](#) página 405.

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Añadir un recurso personalizado de XaaS,”](#) página 405.

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**.

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Añadir un recurso personalizado de XaaS,”](#) página 405.

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Añadir un recurso personalizado de XaaS,”](#) página 405.

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Añadir un recurso personalizado de XaaS,”](#) página 405.

- 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 Orchestrator `LdapUser`, 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**.

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](#) página 430
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](#) página 430
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](#) página 432
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](#) página 433
Puede insertar un encabezado de sección para dividir el formulario en dos secciones.

- [Añadir un elemento de texto a un formulario de blueprint XaaS](#) página 433

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Añadir un blueprint XaaS,”](#) página 408.

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**.

Qué hacer a continuación

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Añadir un blueprint XaaS,”](#) página 408.

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> <ol style="list-style-type: none"> Escriba un valor en el cuadro de búsqueda Valores predefinidos para buscar en el inventario de vRealize Orchestrator. Seleccione un valor en los resultados de la búsqueda y presione Entrar.
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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Añadir un blueprint XaaS,”](#) página 408.

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**.

Qué hacer a continuación

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Añadir un blueprint XaaS,”](#) página 408.

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Añadir un blueprint XaaS,”](#) página 408.

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Crear una acción personalizada,”](#) página 416.

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**.

Qué hacer a continuación

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Crear una acción personalizada,”](#) página 416.

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**.

Qué hacer a continuación

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Crear una acción personalizada,”](#) página 416.

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.

Opción	Descripción
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> <p>a Escriba un valor en el cuadro de búsqueda Valores predefinidos para buscar en el inventario de vRealize Orchestrator.</p> <p>b Seleccione un valor en los resultados de la búsqueda y presione Entrar.</p>
Valor	<p>Defina valores personalizados con etiquetas.</p> <p>a Escriba un valor en el cuadro de texto Valor.</p> <p>b Especifique una etiqueta para el valor en el cuadro de texto Etiqueta.</p> <p>c Haga clic en el icono Añadir (+).</p>
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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Crear una acción personalizada,”](#) página 416.

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **arquitecto XaaS**.
- [“Crear una acción personalizada,”](#) página 416.

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.

Prerequisitos

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](#) página 439
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](#) página 440
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](#) página 441
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](#) página 442
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](#) página 442
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.

Prerequisitos

Inicie sesión en la consola de 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**.

Ha creado un recurso personalizado llamado Usuario de prueba, recurso que ahora aparece recogido en la página Recursos personalizados.

Qué hacer a continuación

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.

Prerequisitos

- 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,”](#) página 439.
- Inicie sesión en la consola de 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**.

Ha generado un blueprint que permite crear un usuario de prueba y ha hecho que el blueprint se pueda añadir a un servicio.

Qué hacer a continuación

Cree una acción para ejecutarla en la cuenta de usuario aprovisionada. Consulte [“Crear una acción personalizada para cambiar una contraseña de usuario,”](#) página 441.

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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 439.

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**.

Ha creado una acción personalizada para cambiar la contraseña de un usuario y ha hecho que se pueda añadir a una autorización.

Qué hacer a continuación

Añada a un servicio el blueprint Crear un usuario de prueba. Consulte [“Crear un servicio y añadirle un blueprint Crear un usuario de prueba,”](#) página 442.

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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 440.

Inicie sesión en la consola de 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**.

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.

Qué hacer a continuación

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,”](#) página 442.

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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **administrador de grupo empresarial**.
- Compruebe que el blueprint Crear un usuario se añade a un servicio. Consulte [“Crear un servicio y añadirle un blueprint Crear un usuario de prueba,”](#) página 442.

- Compruebe que exista la acción personalizada Cambiar una contraseña de usuario. Consulte [“Crear una acción personalizada para cambiar una contraseña de usuario,”](#) página 441.

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**.

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.

Qué hacer a continuación

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.

Prerequisitos

Inicie sesión en la consola de vRealize Automation como **arquitecto XaaS**.

Procedimiento

- 1 [Crear una acción personalizada para migrar una máquina virtual de vSphere](#) página 444
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](#) página 444

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**.

Ha creado una acción personalizada para migrar una máquina virtual, acción que ahora aparece recogida en la página Acciones personalizadas.

Qué hacer a continuación

[“Publicar la acción para migrar una máquina virtual de vSphere,”](#) página 444

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**.

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,”](#) página 418.

Qué hacer a continuación

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,”](#) página 472.

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.

Prerequisitos

Inicie sesión en la consola de vRealize Automation como **arquitecto XaaS**.

Procedimiento

- 1 [Crear una acción para migrar una máquina virtual de vSphere con vMotion](#) página 445
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](#) página 446
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](#) página 447
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](#) página 447
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**.

Qué hacer a continuación

[“Editar el formulario de acción personalizada,”](#) página 446.

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**.

Cuando los consumidores soliciten la acción personalizada, verán un menú desplegable con tres opciones: **apagado**, **encendido** y **suspendido**.

Ha editado la presentación del flujo de trabajo Migrar una máquina virtual con vMotion.



Qué hacer a continuación

[“Añadir un formulario de detalles de la acción enviados y guardar la acción,”](#) página 447.

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
Envío 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**.

Ha creado una acción personalizada para migrar una máquina virtual con vMotion y puede ver que aparece en la página Acciones personalizadas.

Qué hacer a continuación

[“Publicar la acción para migrar una máquina virtual con vMotion,”](#) página 447.

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**.

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,”](#) página 418.

También ha editado la presentación del flujo de trabajo y ha definido el aspecto de la acción.

Qué hacer a continuación

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,”](#) página 313.

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.

Prerequisitos

Inicie sesión en la consola de vRealize Automation como **arquitecto XaaS**.

Procedimiento

- 1 [Crear una acción para tomar un snapshot de una máquina virtual de vSphere](#) página 448
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](#) página 449
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**.

Ha creado una acción personalizada para tomar un snapshot de una máquina virtual, acción que ahora aparece recogida en la página Acciones personalizadas.

Qué hacer a continuación

[“Publicar la acción para guardar un snapshot,”](#) página 449.

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**.

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,”](#) página 418.

Qué hacer a continuación

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,”](#) página 313.

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.

Prerequisitos

- 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](#) página 450
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](#) página 450
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](#) página 451
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.

Prerequisitos

- Inicie sesión en la consola de 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**.

Puede usar la asignación de recursos de Amazon para crear acciones personalizadas relativas a las máquinas de Amazon aprovisionadas mediante IaaS.

Qué hacer a continuación

[“Crear una acción personalizada para iniciar una máquina virtual de Amazon,”](#) página 450.

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.

Prerequisitos

Inicie sesión en la consola de 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**.

Ha creado una acción personalizada para iniciar máquinas virtuales de Amazon, acción que ahora aparece recogida en la página Acciones personalizadas.

Qué hacer a continuación

[“Publicar la acción para iniciar instancias de Amazon,”](#) página 451.

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.

Prerequisitos

Inicie sesión en la consola de 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**.

El estado de la acción personalizada Iniciar instancias cambiará a Publicada.

Qué hacer a continuación

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,”](#) página 472.

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.

Origen

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 deshabilitado.

```
com.vmware.o11n.webview.htmlspecialchars.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.

Prerequisitos

- Inicie sesión en la consola de 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**.

El blueprint se publicará como un elemento del catálogo, pero antes deberá autorizarlo para ponerlo a disposición de los usuarios del catálogo de servicios.

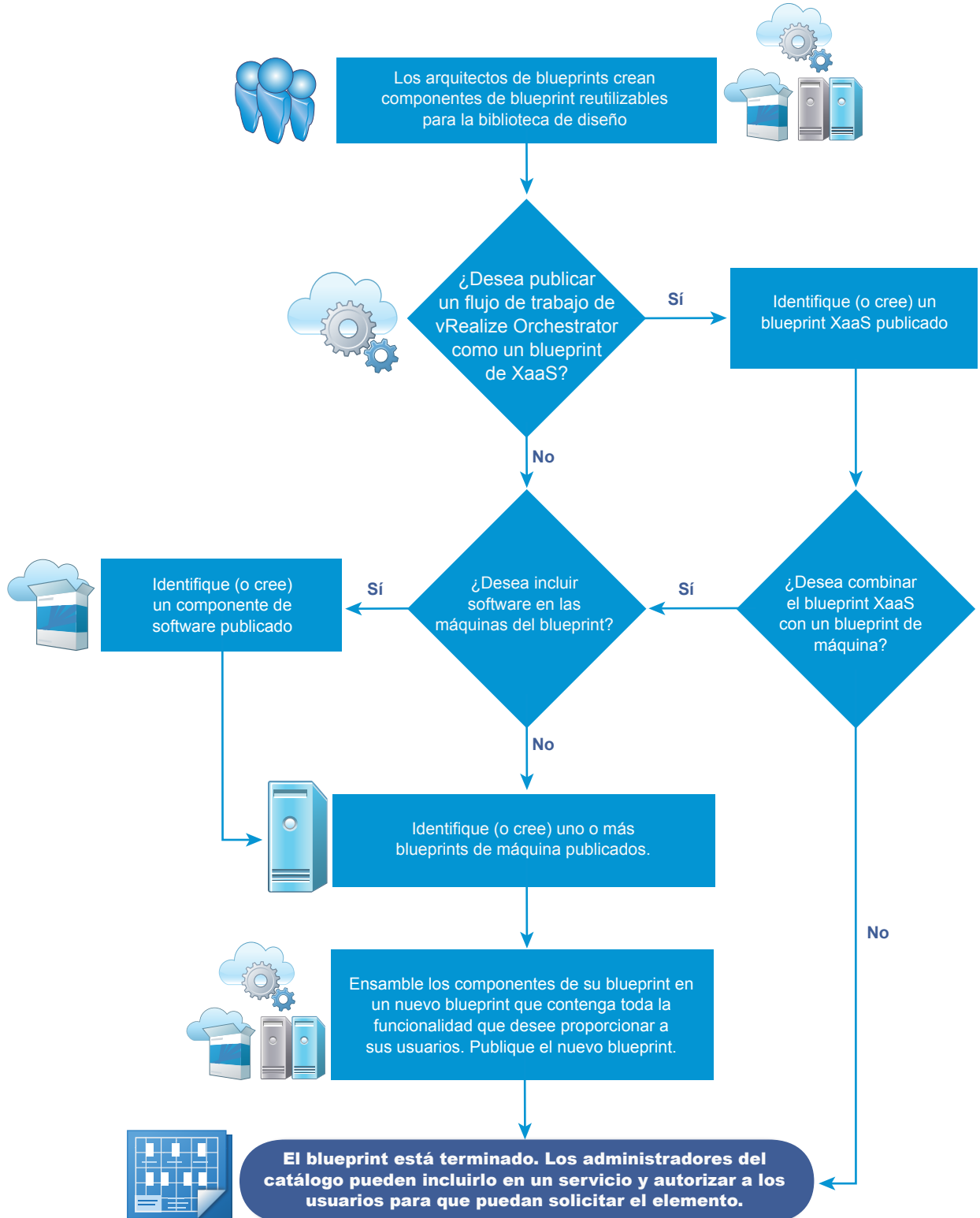
Qué hacer a continuación

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.

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.

Figura 4-5. Flujo de trabajo para ensamblar blueprints compuestos



- [Información sobre el comportamiento de blueprint anidado](#) página 454

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.

- [Seleccionar un componente de máquina compatible con componentes de Software](#) página 456

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](#) página 457

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 explícitas y controlar el orden de aprovisionamiento](#) página 458

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 siempre actualizaciones dependientes durante una operación de escalado horizontal o vertical.

- [Escenario: Ensamblar y probar un blueprint para suministrar MySQL en máquinas de clones vinculados de Rainpole](#) página 459

Con sus privilegios de arquitecto de IaaS, software o aplicaciones, cree un blueprint para combinar el componente de MySQL con el blueprint de clones vinculados CentOS de vSphere que ha creado.

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.

Consideraciones y reglas relativas a redes y seguridad para blueprints anidados

- Todos los componentes de red y seguridad en los blueprints externos se pueden asociar con máquinas que se definen en 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 ajustes de red a petición ni ajustes 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.

Consideraciones relativas a componentes de software para blueprints anidados

En los blueprints que puedan escalar, 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.

Seleccionar un componente de máquina compatible con componentes de Software

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. Como los agentes de Software no son compatibles con la versión de Protocolo de Internet 6 (IPv6), asegúrese de que los blueprints de máquina, las reservas y los componentes de redes y de seguridad que esté usando estén configurados para usar IPv4 y no IPv6. Si diseña blueprints que puedan escalar, 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.

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. 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.

Tabla 4-63. Métodos de aprovisionamiento compatibles con Software

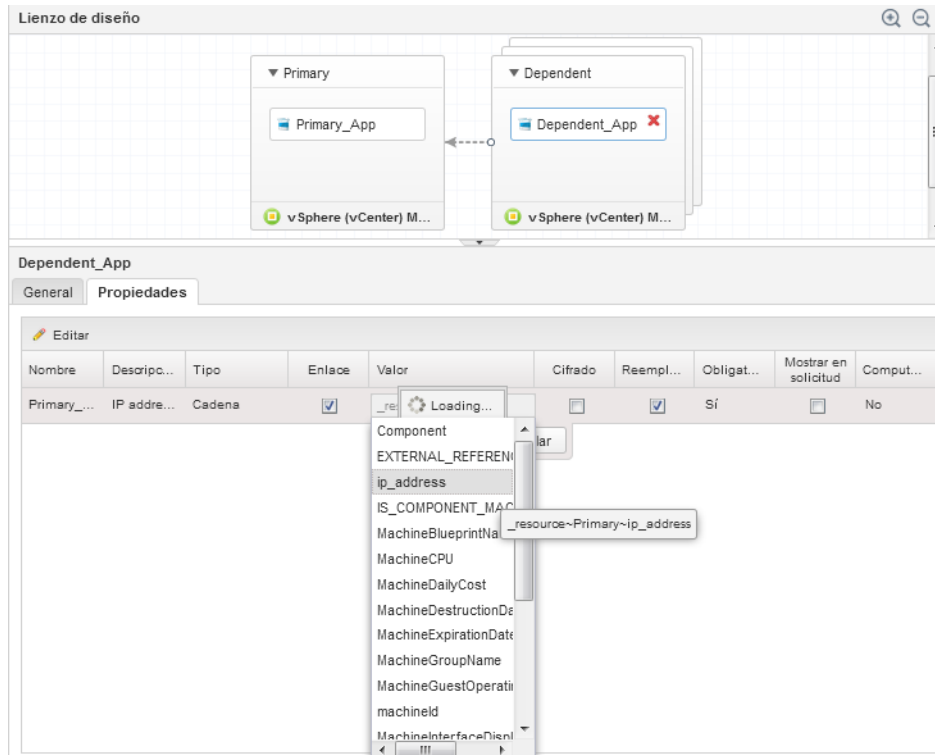
Tipo de máquina	Método de aprovisionamiento
vSphere	Clonar
vSphere	Clon vinculado
vCloud Director	Clonar
vCloud Air	Clonar
Amazon AWS	Imagen de máquina de Amazon

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 4-6. Enlazar una propiedad de software a la dirección IP de una máquina

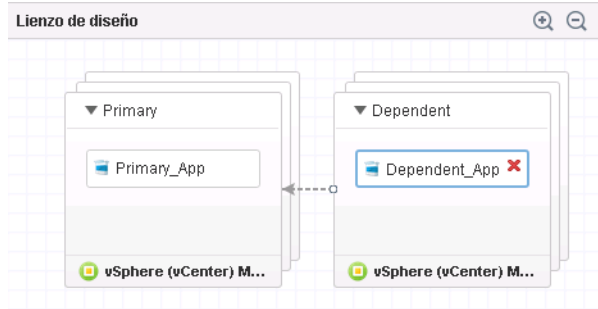
Crear dependencias explícitas y controlar el orden de aprovisionamiento

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 siempre actualizaciones dependientes durante una operación de escalado horizontal o vertical.

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.

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 4-7. 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.

Escenario: Ensamblar y probar un blueprint para suministrar MySQL en máquinas de clones vinculados de Rainpole

Con sus privilegios de arquitecto de IaaS, software o aplicaciones, cree un blueprint para combinar el componente de MySQL con el blueprint de clones vinculados CentOS de vSphere que ha creado.



Prerequisitos

- Cree un componente de Software para instalar MySQL en máquinas Linux. Consulte [“Escenario: Crear un componente de Software MySQL para Rainpole,”](#) página 387.
- Inicie sesión en la consola de vRealize Automation como miembro del grupo personalizado de arquitectos de Rainpole. Consulte [“Escenario: Crear un grupo personalizado para los arquitectos de Rainpole,”](#) página 161.

Procedimiento

- 1 [Escenario: Crear un contenedor para el blueprint de MySQL en CentOS Rainpole](#) página 460
Con sus privilegios de arquitecto de IaaS, software o aplicaciones, cree un contenedor de blueprints y configure el nombre, la descripción y el identificador único de su blueprint de MySQL en CentOS vSphere.

- 2 [Escenario: Añadir software y una máquina a MySQL en el blueprint de CentOS para Rainpole](#) página 460
Con sus privilegios de arquitecto de IaaS, software o aplicaciones, arrastre el blueprint publicado de máquina de Pruebas de software con CentOS al lienzo para volver a utilizar el blueprint como su máquina. Arrastre el componente de software publicado a la máquina virtual y configure las propiedades de Software especificadas en el componente de Software.
- 3 [Escenario: Añadir su elemento del catálogo CentOS con MySQL al servicio de Rainpole](#) página 461
Utilizando sus privilegios de administrador de tenant, añada su nuevo blueprint al servicio del catálogo de Rainpole para que pueda comprobar el trabajo.
- 4 [Escenario: Aprovisionar CentOS con el elemento del catálogo MySQL para Rainpole](#) página 461
Con la cuenta de usuario de prueba, solicite el elemento del catálogo de servicios para aprovisionar una máquina CentOS con MySQL.

Escenario: Crear un contenedor para el blueprint de MySQL en CentOS Rainpole

Con sus privilegios de arquitecto de IaaS, software o aplicaciones, cree un contenedor de blueprints y configure el nombre, la descripción y el identificador único de su blueprint de MySQL en CentOS vSphere.

Procedimiento

- 1 Seleccione **Diseño > Blueprints**.
- 2 Haga clic en el icono **Nuevo (+)**.
- 3 Escriba **MySQL en CentOS** en el cuadro de texto **Nombre**.
- 4 Revise el identificador único generado.

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.
- 5 Escriba **Software MySQL en máquina de vSphere CentOS** en el cuadro de texto **Descripción**.
- 6 Configure un rango de concesión para que los usuarios puedan elegir la duración. Para ello, especifique **1** en el cuadro de texto **Mínimo** y **7** en el cuadro de texto **Máximo**.

Los usuarios pueden elegir que la concesión de las máquinas solicitadas dure hasta un siete días. Transcurrido ese tiempo, deberán renovar las concesiones o dejar que se destruyan las máquinas.
- 7 Haga clic en **Aceptar**.

Qué hacer a continuación

Arrastre al lienzo su componente de MySQL y su blueprint de máquina de CentOS para Software publicado.

Escenario: Añadir software y una máquina a MySQL en el blueprint de CentOS para Rainpole

Con sus privilegios de arquitecto de IaaS, software o aplicaciones, arrastre el blueprint publicado de máquina de Pruebas de software con CentOS al lienzo para volver a utilizar el blueprint como su máquina. Arrastre el componente de software publicado a la máquina virtual y configure las propiedades de Software especificadas en el componente de Software.

Procedimiento

- 1 En la lista Categorías, haga clic en Blueprints.
- 2 Arrastre **Pruebas de software con CentOS** al lienzo.

- 3 En la lista Categorías, haga clic en **Componentes de software**.
- 4 Arrastre **MySQL para máquinas virtuales de Linux** a la máquina vSphere.
- 5 Haga clic en la pestaña **Propiedades**.
- 6 Actualice la propiedad db_port de este blueprint.
 - a Seleccione la propiedad db_port y haga clic en **Editar**.
 - b En el cuadro de texto **Valor**, escriba **3308**.
Cuando un usuario del catálogo de servicios solicita el elemento, el valor predeterminado es 3308.
 - c Haga clic en **Aceptar**.
- 7 Haga clic en **Finalizar**.
- 8 Seleccione la fila que contiene CentOS con MySQL y haga clic en **Publicar**.

Ha publicado un blueprint que incluye la máquina CentOS y el componente de software MySQL.

Escenario: Añadir su elemento del catálogo CentOS con MySQL al servicio de Rainpole

Utilizando sus privilegios de administrador de tenant, añada su nuevo blueprint al servicio del catálogo de Rainpole para que pueda comprobar el trabajo.

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Servicios**.
- 2 Seleccione la fila del servicio del catálogo de Rainpole 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**.

Su elemento del catálogo CentOS con MySQL ya está listo para que lo solicite. No necesita autorizar el nuevo elemento del catálogo porque ya ha autorizado el grupo empresarial de Rainpole a todo el servicio de Rainpole.

Qué hacer a continuación

Solicite el elemento del catálogo CentOS con MySQL para comprobar su trabajo.

Escenario: Aprovisionar CentOS con el elemento del catálogo MySQL para Rainpole

Con la cuenta de usuario de prueba, solicite el elemento del catálogo de servicios para aprovisionar una máquina CentOS con MySQL.

Procedimiento

- 1 Cierre la sesión la consola de vRealize Automation.

- 2 Vuelva a iniciar sesión con el nombre de usuario **test_user** y la contraseña **VMware1!**.
- 3 Haga clic en la pestaña **Catálogo**.
- 4 Haga clic en el botón **Solicitar** para solicitar un elemento del catálogo.
- 5 Escriba **verifying functionality** en el cuadro de texto **Descripción**.
- 6 Haga clic en **Enviar** para solicitar el elemento del catálogo.
- 7 Haga clic en la pestaña **Solicitudes** para ver el estado de la solicitud.

Cuando la máquina se aprovisiona correctamente, aparecerá el mensaje de estado **Correcto**.

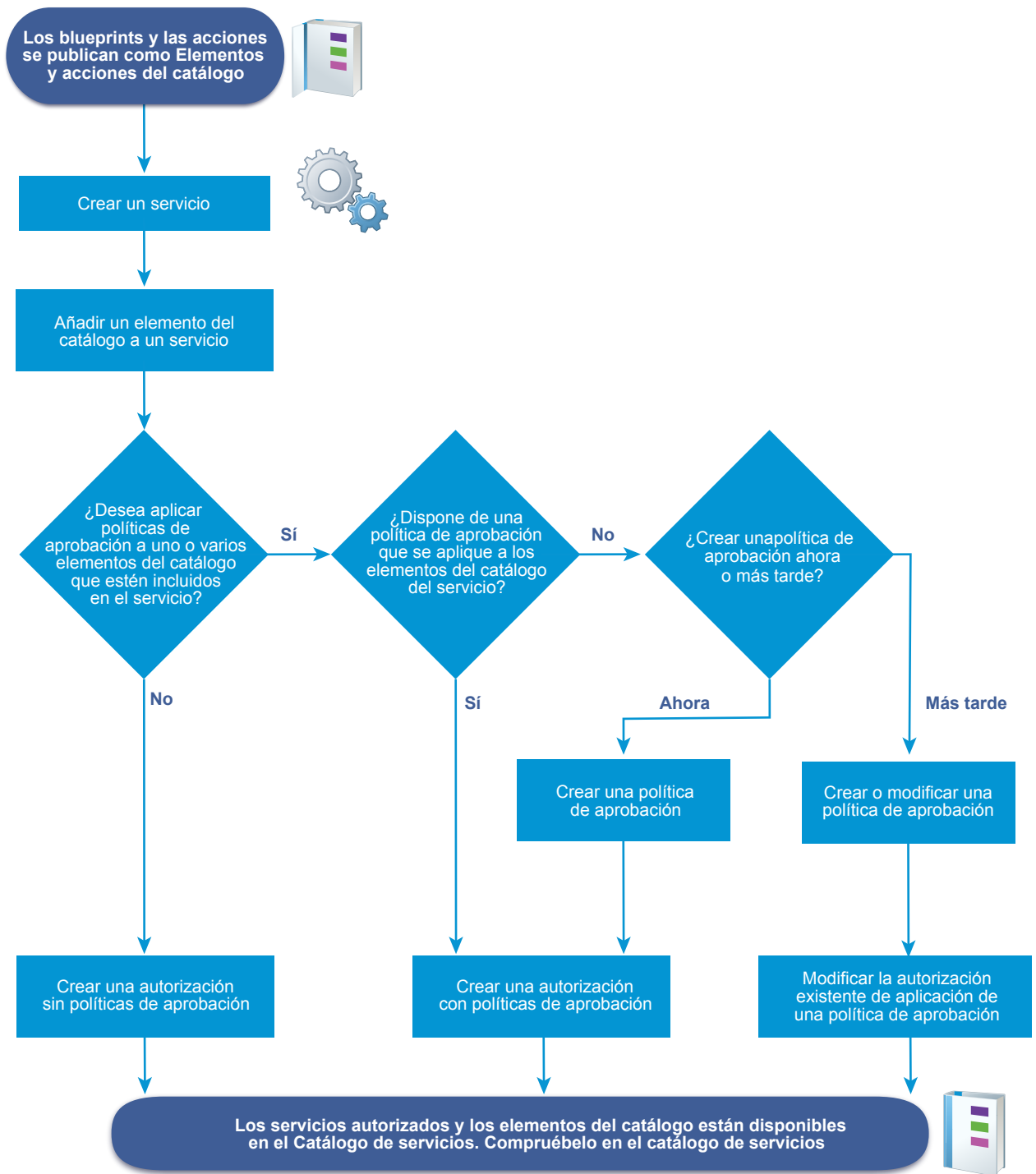
Qué hacer a continuación

- Planifique la instalación de un entorno de producción. Consulte *Arquitectura de referencia*.
- Obtenga más información acerca de las opciones para configurar vRealize Automation, diseñar y exportar blueprints y dirigir el catálogo de servicios. Consulte *Configuración de vRealize Automation*.

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 4-64. Lista de comprobación para configurar el catálogo de servicios

Tarea	Función necesaria	Detalles
<input type="checkbox"/> Añadir un servicio.	Administrador de tenants o administrador del catálogo	Consulte “Añadir un servicio,” página 465.
<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,” página 466.
<input type="checkbox"/> Configurar el elemento del catálogo en el servicio.	Administrador de tenants o administrador del catálogo	Consulte “Configurar un elemento del catálogo,” página 467.
<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,” página 472.
<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,” página 483.

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.

Prerequisitos

Inicie sesión en la consola de 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.

Opción	Descripción
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 periodo	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**.

Qué hacer a continuación

Asocie elementos del catálogo con un servicio, para que se puedan autorizar usuarios en los elementos. Consulte [“Añadir elementos del catálogo a un servicio,”](#) página 466.

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.

Prerrequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **administrador del catálogo**.
- Compruebe que haya un servicio. Consulte [“Añadir un servicio,”](#) página 465.
- Compruebe haya uno o varios elementos del catálogo publicados. Consulte [“Configurar un elemento del catálogo,”](#) página 467.

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**.

Qué hacer a continuación

- 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,”](#) página 467.
- Autorice a los usuarios a los servicios o elementos del catálogo para que puedan solicitarlos en el catálogo de servicios. Consulte [“Crear autorizaciones,”](#) página 469.

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 distinto, deshabilitarlo si desea quitarlo temporalmente del catálogo de servicios y añadir 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 están disponibles para el elemento aprovisionado en la pestaña **Elementos** del usuario del catálogo de servicios en función de si son aplicables al elemento y al estado actual del elemento.

Puede añadir un icono personalizado a la acción que aparezca en la pestaña **Elementos**.

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.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 452.

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	Entre los posibles valores se incluyen Activo , Inactivo , y Almacenamiento provisional . <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.
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.
Nuevo y destacado	El elemento del catálogo aparece en el área Nuevo y destacado de la página principal.

- 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**.

Qué hacer a continuación

- 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,”](#) página 469.
- 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,”](#) página 475.

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**.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **administrador del catálogo**.
- Compruebe que tiene al menos una acción publicada. Consulte [“Publicar un blueprint,”](#) página 452 y [“Publicar una acción personalizada,”](#) página 418.

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**.

Qué hacer a continuación

[“Autorizar usuarios a servicios, elementos de catálogo y acciones,”](#) página 472.

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](#) página 470
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](#) página 470
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](#) página 471

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](#) página 472

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,”](#) página 469.

Prerequisitos

- Inicie sesión en la consola de 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,”](#) página 466.
- 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,”](#) página 155.
- Si tiene intención de añadir aprobaciones al crear esta autorización, compruebe que existen las políticas de aprobación correspondientes. Consulte [“Crear una política de aprobación,”](#) página 483. 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	Entre los posibles valores se incluyen Activo, Inactivo y Eliminado. <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. 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>
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.

Si el estado de la autorización es activo, el servicio y los elementos se añaden al catálogo de servicios.

Qué hacer a continuación

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 Connie, un miembro de dicho grupo.

Tabla 4-65. Autorizaciones de ejemplo

Autorización 1	Autorización 2
Grupo empresarial: Finanzas	Grupo empresarial: Finanzas
Usuarios y grupos: grupo Contabilidad	Usuarios y grupos: Connie
Elemento de catálogo 1: Política A	Elemento de catálogo 1: Política C

Connie solicita el Elemento de catálogo 1 del catálogo de servicios. En función del orden de prioridad de las autorizaciones del grupo empresarial Finanzas, se aplicará una política diferente a la solicitud de Connie.


Tabla 4-66. 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. Connie es miembro del grupo de usuarios Contabilidad. La búsqueda de Connie como usuario con autorización se detiene en Autorización 1 y se aplica la política de aprobación.	Se ha aplicado la Política C. La búsqueda de Connie como usuario con autorización se detiene en Autorización 2 y se aplica la política de aprobación.

Prerequisitos

Inicie sesión en la consola de 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 ventana 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 aprovisiona 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 4-67. 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 4-67. Ejemplos de políticas de aprobación y resultados (Continúa)

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 recursos de infraestructuras virtuales y controlar los costes, puede añadir dos tipos de niveles de aprobación previa: una aprobación es para los recursos de máquina y la otra es para los costes 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.
			Nivel 2 Seleccione Se requiere según condiciones. Configure la condición Coste > 15,00 al día.	Seleccione Usuarios y grupos específicos. Seleccione el grupo de usuarios personalizados del departamento financiero. Seleccione Cualquiera puede aprobar.		

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 Destruir - máquina virtual	Política de aprobación A 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
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 4-68. Configuraciones de autorizaciones

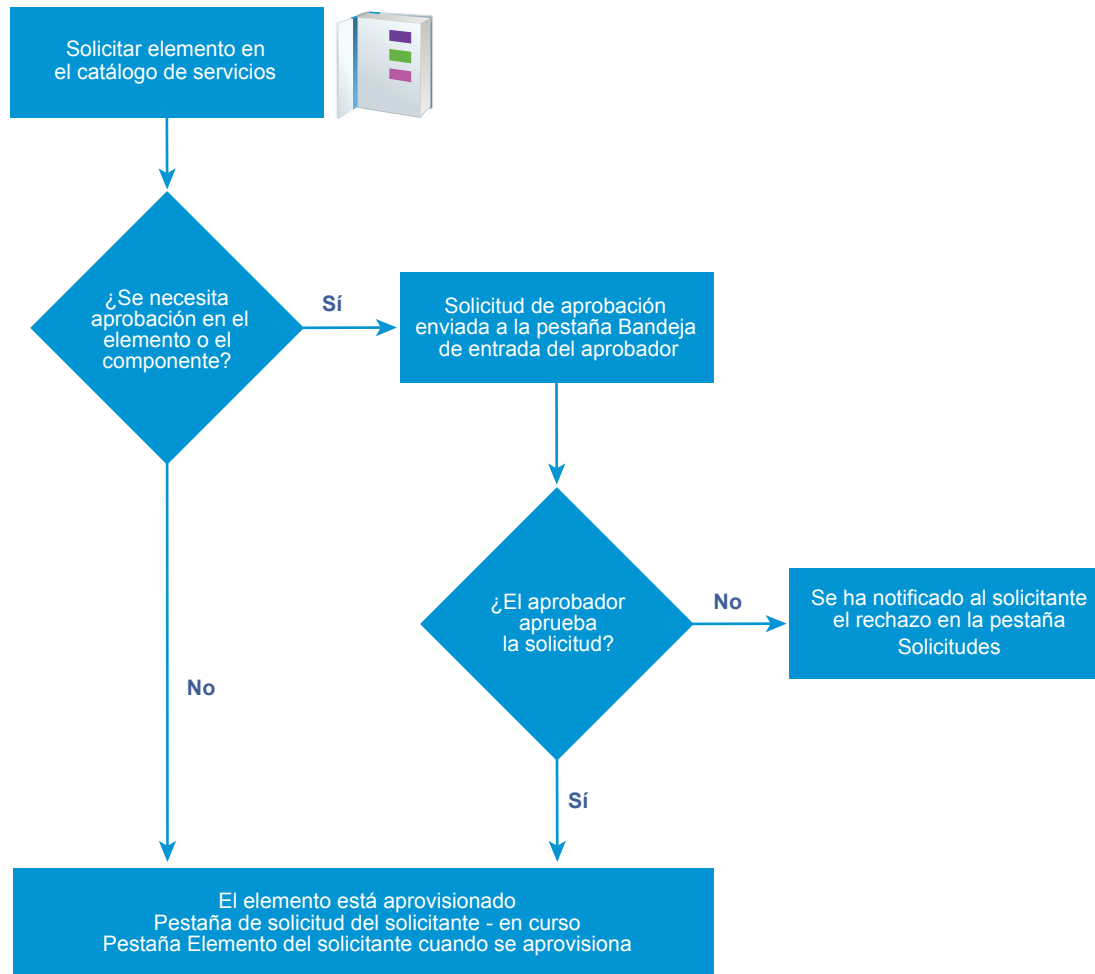
Nombre de autorización	Grupo empresarial	Servicio autorizado	Elemento autorizado
Autorización 1	Calidad	Pruebas	Solicitud de elemento del catálogo - Máquina virtual aplicada a componente de máquina virtual
Autorización 2	Calidad	Formación	

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.

Prerequisitos

Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **administrador de aprobaciones**.

Procedimiento

- 1 [Especificar información sobre políticas de aprobación](#) página 484
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](#) página 485
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](#) página 487
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, la concesión o la memoria, antes de completar una solicitud de aprobación.
- 4 [Configuración de políticas de aprobación](#) página 488
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.

Prerequisitos

Inicie sesión en la consola de 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.

Qué hacer a continuación

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,”](#) página 476.

Prerequisitos

[“Especificar información sobre políticas de aprobación,”](#) página 484.

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**.

Qué hacer a continuación

Para añadir propiedades al formulario de aprobación, consulte [“Configurar el formulario de aprobación para incluir propiedades personalizadas y del sistema,”](#) página 487.

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, la concesión 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.

Prerequisitos

- Inicie sesión en la consola de vRealize Automation como **administrador de tenants** o **administrador de aprobaciones**.
- [“Crear un nivel de aprobación,”](#) página 485.

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**.

Qué hacer a continuación

- 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](#) página 488
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](#) página 489
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](#) página 491
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](#) página 493
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](#) página 493
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 4-69. 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 4-70. 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 4-70. Opciones de política de aprobación (Continua)

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. 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. 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 4-71. 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 4-71. Opciones de información de nivel (Continua)

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>
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>

Tabla 4-71. Opciones de información de nivel (Continua)

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> <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 4-72. 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 4-73. 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.

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,”](#) página 485.

Prerequisitos

Inicie sesión en la consola de 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**.

Ha creado una nueva política de aprobación basada en una política de aprobación existente.

Qué hacer a continuación

Aplice la nueva política de aprobación en una autorización. Consulte [“Autorizar usuarios a servicios, elementos de catálogo y acciones,”](#) página 472.

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.

Prerequisitos

Inicie sesión en la consola de 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**.

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.

Qué hacer a continuación

Si ya no necesita la política de aprobación, puede eliminarla. Consulte [“Eliminar una política de aprobación,”](#) página 496.

Eliminar una política de aprobación

Si tiene políticas de aprobación que ha desactivado y ya no necesita, puede eliminarlas de vRealize Automation.

Prerequisitos

- Desvincule y desactive políticas de aprobación. Consulte [“Desactivar una política de aprobación,”](#) página 495.
- Inicie sesión en la consola de 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**.

La política de aprobación se elimina.

Escenario: Configurar el catálogo para que los arquitectos de Rainpole prueben los blueprints

Utilizando sus privilegios de administrador de tenants, cree un servicio de catálogo especial que contenga muy poco control en el que los arquitectos de Rainpole puedan probar eficazmente su trabajo antes de exportar los blueprints al entorno de producción. Debe crear un servicio de pruebas de blueprints, añadir el blueprint CentOS de vSphere al servicio y autorizar a los arquitectos de Rainpole en todos los elementos del catálogo y en las acciones asociadas al servicio para que los arquitectos puedan comprobar su trabajo mediante el aprovisionamiento de elementos del catálogo.



Procedimiento

- 1 [Escenario: Crear un servicio del catálogo para prueba de blueprint de Rainpole](#) página 497
Con sus privilegios de administrador de tenants, cree un servicio del catálogo llamado servicio Rainpole. Asígnese a usted mismo como propietario y contacto de soporte para este servicio, para que sus arquitectos de Rainpole puedan ponerse en contacto con usted por cualquier problema.
- 2 [Escenario: Agregar su elemento del catálogo de vSphere CentOS al servicio de Rainpole](#) página 497
Mediante el uso de sus privilegios de administrador de tenants, usted agrega el blueprint de la máquina de vSphere CentOS publicado a su servicio de Rainpole.
- 3 [Escenario: Autorizar los arquitectos de Rainpole para solicitar elementos del catálogo](#) página 498
Utilizando sus privilegios de administrador de tenant, autorice a sus arquitectos de Rainpole en todas las acciones y elementos que pertenezcan al servicio de Rainpole.

Escenario: Crear un servicio del catálogo para prueba de blueprint de Rainpole

Con sus privilegios de administrador de tenants, cree un servicio del catálogo llamado servicio Rainpole. Asígnese a usted mismo como propietario y contacto de soporte para este servicio, para que sus arquitectos de Rainpole puedan ponerse en contacto con usted por cualquier problema.

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Servicios**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Escriba el nombre **Rainpole service**.
- 4 En el menú desplegable Estado, seleccione **Activo**.
- 5 Como administrador de tenants que crea el servicio, use la opción de búsqueda para añadirse como Propietario y Equipo de soporte.
- 6 Haga clic en **Aceptar**.

Qué hacer a continuación

Mediante el uso de sus privilegios de administrador de tenants, agregue el blueprint de la máquina de vSphere CentOS publicado a su servicio de Rainpole.

Escenario: Agregar su elemento del catálogo de vSphere CentOS al servicio de Rainpole

Mediante el uso de sus privilegios de administrador de tenants, usted agrega el blueprint de la máquina de vSphere CentOS publicado a su servicio de Rainpole.

Todos los blueprints publicados que quiera aprovisionar deben formar parte de un servicio que sea un elemento del catálogo, pero cada blueprint solo puede ser un elemento del catálogo de un servicio a la vez. Si necesita publicar en varios servicios de catálogo al mismo tiempo, cree copias de su blueprint.

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Servicios**.
- 2 En la lista Servicios, seleccione la fila de pruebas de blueprint y haga clic en **Administrar elementos del catálogo**.
- 3 Haga clic en el icono **Nuevo** (+).
- 4 Active la casilla de **CentOS en vSphere**.

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**.

Qué hacer a continuación

Mediante el uso de sus privilegios de administrador de tenants, autorice a sus arquitectos de Rainpole a solicitar elementos del catálogo desde el servicio de Rainpole.

Escenario: Autorizar los arquitectos de Rainpole para solicitar elementos del catálogo

Utilizando sus privilegios de administrador de tenant, autorice a sus arquitectos de Rainpole en todas las acciones y elementos que pertenezcan al servicio de Rainpole.

Al autorizar a sus arquitectos de Rainpole en todas las acciones y elementos del servicio, hace que les resulte más fácil añadir nuevos elementos del catálogo al servicio para probarlos. En un entorno de producción, es posible que utilice las autorizaciones de un modo distinto y que configure un control más estricto. Sería conveniente administrar qué elementos del catálogo puede solicitar cada usuario y qué acciones pueden realizar con elementos del catálogo específicos que poseen.

Procedimiento

- 1 Seleccione **Administración > Administración de catálogos > Autorizaciones**.
- 2 Haga clic en el icono **Nuevo** (+).
- 3 Configure los detalles.
 - a Especifique el nombre **Autorización de arquitecto de Rainpole**
 - b Seleccione **Activo** en el menú desplegable **Estado**.
 - c Seleccione el grupo empresarial de Rainpole en el menú desplegable **Grupo empresarial**.
 - d Añada los arquitectos de Rainpole mediante el cuadro de búsqueda **Usuarios y grupos**.
 - e Haga clic en **Siguiente**.
- 4 Autorice el servicio del catálogo de Rainpole.
 - a Haga clic en el icono **Añadir servicios** (+) junto al encabezado Servicios autorizados.
 - b Seleccione **Servicio de Rainpole**.
 - c Haga clic en **Aceptar**.

Todos los usuarios que haya incluido en la autorización ahora están autorizados en todos los elementos del catálogo de servicios de Rainpole.

- 5 Autorice todas las acciones de usuario.
 - a Haga clic en el icono **Añadir acciones** (+) junto al encabezado Acciones autorizadas.
 - b Active la casilla del encabezado de columna para autorizar todas las acciones.
 - c Active la casilla **Las acciones solo se aplican a los elementos definidos en esta autorización** para que más adelante pueda aplicar un gobierno más estricto a estos usuarios en otros servicios del catálogo.
 - d Haga clic en **Aceptar**.

Sus arquitectos están autorizados para realizar cualquier acción aplicable en los elementos del catálogo que aprovisionen desde el servicio de Rainpole. No están autorizados para realizar esas acciones en ningún elemento que puedan aprovisionar desde otro servicio o mediante otra autorización.

- 6 Haga clic en **Finalizar**.

Todos los arquitectos ahora pueden ver y solicitar el blueprint de máquina CentOS de vSphere y cualquier nuevo elemento del catálogo que se añada al servicio.

Qué hacer a continuación

Con la cuenta de usuario de prueba local, solicite el aprovisionamiento del elemento del catálogo CentOS de vSphere para probar el blueprint y la configuración del catálogo.

Escenario: Probar la máquina CentOS de Rainpole

Con la cuenta de usuario de prueba local que ha creado, solicite el aprovisionamiento de su máquina CentOS de vSphere. Inicie sesión en la máquina aprovisionada y compruebe que funciona del modo esperado.



Procedimiento

- 1 [Escenario: Solicitar la máquina virtual de Rainpole](#) página 499
Con la cuenta de usuario de prueba, solicite el elemento del catálogo de servicios para aprovisionar CentOS en una máquina virtual de vSphere.
- 2 [Escenario: Iniciar sesión en la máquina aprovisionada de Rainpole](#) página 500
Con la cuenta de usuario de prueba, inicie sesión en la máquina CentOS de vSphere aprovisionada.

Escenario: Solicitar la máquina virtual de Rainpole

Con la cuenta de usuario de prueba, solicite el elemento del catálogo de servicios para aprovisionar CentOS en una máquina virtual de vSphere.

Procedimiento

- 1 Cierre la sesión la consola de vRealize Automation.
 - 2 Vuelva a iniciar sesión con el nombre de usuario **test_user** y la contraseña **VMware1!**.
 - 3 Haga clic en la pestaña **Catálogo**.
 - 4 Haga clic en el botón **Solicitar** para solicitar un elemento del catálogo.
 - 5 Escriba **verifying functionality** en el cuadro de texto **Descripción**.
 - 6 Haga clic en **Enviar** para solicitar el elemento del catálogo.
 - 7 Haga clic en la pestaña **Solicitudes** para ver el estado de la solicitud.
- Cuando la máquina se aprovisiona correctamente, aparecerá el mensaje de estado **Correcto**.

Qué hacer a continuación

Inicie sesión en su máquina aprovisionada.

Escenario: Iniciar sesión en la máquina aprovisionada de Rainpole

Con la cuenta de usuario de prueba, inicie sesión en la máquina CentOS de vSphere aprovisionada.

Procedimiento

- 1 Seleccione **Elementos > Máquinas**.
- 2 Seleccione la flecha al lado de CentOS en el elemento de vSphere.
La máquina aprovisionada aparece en el elemento expandido.
- 3 Haga clic en la máquina aprovisionada.
- 4 Haga clic en **Inicio de sesión remoto en la máquina** en el panel derecho.
- 5 Inicie sesión en la máquina.

Ha instalado vRealize Automation en una implementación mínima, ha configurado una prueba de concepto y ha configurado su entorno para el desarrollo continuo de blueprints.

Qué hacer a continuación

- Si ha adquirido una licencia de empresa de vRealize Automation, puede seguir leyendo para ver la información sobre el aprovisionamiento de máquinas con componentes de software.
- Planifique la instalación de un entorno de producción. Consulte *Arquitectura de referencia*.
- Obtenga información sobre las opciones adicionales para configurar vRealize Automation, diseñar y exportar blueprints, y controlar el catálogo de servicios. Consulte *Configuración de vRealize Automation*.

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.

Prerequisitos

- Inicie sesión en la consola de 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 [“Escenario: Ensamblar y probar un blueprint para suministrar MySQL en máquinas de clones vinculados de Rainpole,”](#) página 459.
- Si crea blueprints en un entorno de desarrollo, importe el blueprint en su entorno de producción. Consulte [“Exportar e importar blueprints,”](#) página 305.
- 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,”](#) página 256.

Procedimiento

- 1 [Escenario: Crear un servicio del catálogo de ingeniería de desarrollo y calidad](#) página 501
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](#) página 502
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](#) página 502
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**.

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**.

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 añada 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**.

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.

Qué hacer a continuación

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,”](#) página 504.

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.

Prerequisitos

- 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,”](#) página 500.

Procedimiento

- 1 [Escenario: Crear una política de aprobación de la máquina virtual CentOS con MySQL](#) página 504
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.
- 2 [Escenario: Crear una política de aprobación de un componente de Software MySQL](#) página 506
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.
- 3 [Escenario: Aplicar políticas de aprobación a componentes de CentOS con MySQL](#) página 507
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.

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**.

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**.

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**.

Esta autorización te permite requerir diferentes aprobaciones en componentes de blueprint distintos.

Qué hacer a continuación

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.

Índice

A

- acción, autorización **469, 471**
- acción personalizada de ejemplo, editar el formulario **446**
- acción personalizada para iniciar una máquina virtual de Amazon **449**
- acciones de destrucción, políticas de aprobación **479**
- acciones de script, asignar como valores externos **424**
- acciones de XaaS **400**
- acciones personalizadas
 - añadir un formulario de ejemplo **447**
 - añadir un nuevo campo **432, 435**
 - añadir un nuevo formulario **434**
 - asignar un icono **418**
 - Azure **368**
 - cambiar contraseña de usuario **441**
 - campos nuevos **421**
 - crear **416**
 - editar campos **436**
 - editar el formulario **434**
 - ejemplo **441**
 - guardar una acción de ejemplo **447**
 - migrar máquina virtual **444, 445**
 - publicar **418**
 - tomar un snapshot **448**
- acciones personalizadas de XaaS
 - asignar **419**
 - crear **415**
- activación, configurar el servicio para los usuarios **18**
- active directory
 - conector **88**
 - directorio **88**
 - trabajo **88**
- Active Directory
 - asignación de atributos **105, 131**
 - complemento de limpieza **375**
 - crear política **299**
 - integrar **89**
 - política **299**
 - reemplazar política **301**
- Active Directory de un único bosque **89**
- active directory, añadir usuarios **104**
- active directory, conceptos importantes **88**
- Active Directory, configurar un vínculo **90**
- AD, Véase Active Directory
- administración de directorios
 - actualización del conector **139, 142**
 - alta disponibilidad **99**
 - autenticación de Kerberos **133**
 - autenticación de RSA SecurID **120**
 - autenticación mediante certificado **126**
 - autenticación RADIUS **122**
 - Conexión OpenLDAP **94**
 - configurar Active Directory de dominio único a través de LDAP **160**
 - entorno con varios bosques **152**
 - federación de SAML **102**
 - servidor RADIUS **122**
 - vínculo de Active Directory **90**
- Administración de directorios, actualización del conector **137**
- administración de directorios, archivo OVA del conector **147**
- administración de directorios, autenticación de usuario **118**
- administración de directorios, conector externo **151**
- administración de directorios, configurar **144**
- administración de directorios, entorno con varios dominios **152**
- administración de directorios, opciones de configuración **86**
- administración de directorios, proveedor de identidades **128**
- administración de directorios, proveedor de identidades de área de trabajo **151**
- administración de identidades, configurar Active Directory de dominio único a través de LDAP **160**
- administradores de IaaS, asignar **165**
- administradores de tejido, asignar administradores a grupos de tejidos **207**
- administradores de tenants
 - asignar **165**
 - crear **158**
- administrar
 - conectores **108**
 - política de acceso de usuarios **117**
 - rangos de redes **129**

- administrar atributos de usuario **107**
- administrar directorios, asignar memoria **106**
- agente de arranque, plataformas de aprovisionamiento compatibles **71**
- agente de arranque de software
 - instalar **78**
 - instalar para Dukes Bank **81**
- agente invitado
 - añadir el certificado cert.pem para clonación **35**
 - certificados SSL **34**
 - descripción general **31**
 - insertar en WinPE **63–66**
 - instalar para Linux **35**
 - instalar para SCCM **57**
 - instalar para Windows **37**
 - preparar el entorno de Amazon **21**
- agente invitado de Linux, instalar **35**
- agente invitado de Windows, instalar **37**
- agentes, usar para crear un endpoint **196, 198, 199**
- agrupar en clústeres, xenon **19**
- aislamiento de aplicaciones
 - permitir en blueprints de máquina **343**
 - usar una política de seguridad de aislamiento de aplicaciones **345**
- almacenamiento, uso eficiente del espacio **313**
- almacenamiento en bloque flexible, crear para implementaciones de Amazon **23**
- almacenes de datos
 - asignar políticas de reserva de almacenamiento **264**
 - usar políticas de reserva de almacenamiento **262**
- alta disponibilidad, administración de directorios **99**
- Amazon
 - añadir compatibilidad con túneles SSH a las reservas **251**
 - crear endpoints **199**
 - crear una reserva **231**
 - credenciales necesarias **20**
 - preparar el aprovisionamiento de software (capítulo) **73**
 - preparar la implementación **20**
 - preparar una máquina Windows de referencia para el aprovisionamiento de software **73**
 - requisitos de conectividad de agentes invitados y software **21**
- Amazon AWS, preparar el aprovisionamiento (capítulo) **67**
- Amazon EC2, configurar conectividad de red a VPC de Amazon **24**
- añadir, política de Active Directory **299, 300**
- añadir blueprints al catálogo de servicios **500**
- añadir host **281**
- añadir un nuevo formulario
 - acciones personalizadas **434**
 - blueprints XaaS **430**
- añadir una nueva página de formulario **427**
- añadir usuarios, active directory **104**
- aplicación de muestra
 - crear plantillas para Dukes Bank **80**
 - importar aplicación de muestra de Dukes Bank **306**
 - solicitar aplicación de muestra de Dukes Bank **309**
- aplicaciones de tenant, personalización de marca **167**
- aprobaciones, crear políticas de aprobación para componentes de elementos del catálogo **504**
- aprovisionamiento de WIM
 - crear WinPE de PEBuilder **62**
 - incluyendo controladores VirtIO **61**
 - insertar el agente invitado **63–66**
 - instalar PEBuilder **60**
 - preparar **57**
 - requisitos de máquina de referencia **59**
 - Sysprep de la máquina de referencia **59**
- aprovisionamiento fino, acerca de **313**
- aprovisionamiento KVM (RHEV), incluyendo controladores VirtIO **61**
- aprovisionar
 - preparar el aprovisionamiento de WIM **57**
 - prepararse para SCVMM **26**
 - preparativos **27**
 - usar direcciones IP **210**
- aprovisionar, configurar recursos **185**
- archivar, configuración del nuevo blueprint **315, 339**
- archivo domain_krb properties **112**
- archivo OVA del conector **147**
- archivos RDP personalizados, crear **179**
- asignaciones de recursos
 - crear **420**
 - vCenter **420**
 - vCloud Director **420**
 - vSphere **420**
- asignar, acciones personalizadas de XaaS **419**
- asignar recursos **450**
- atributos, asignar **105, 131**
- atributos de usuario
 - administrar **107**
 - configurar **87**
- autenticación, RADIUS **121**
- autenticación de tarjeta inteligente **124**
- autenticación de usuario alternativa **118**

autenticación de usuarios, configurar Active Directory de dominio único a través de LDAP **160**

autenticación de Windows **106**

autenticación RADIUS **121**

autenticación:tarjeta inteligente **146**

autorización

acción **469, 471**

componente **469, 470**

elemento del catálogo **469, 470**

política de aprobación **472**

servicio **470**

autorizaciones

añadir servicios **472**

aplicar políticas de aprobación **507**

autorizar a usuarios en elementos del catálogo **500**

crear **469**

crear autorizaciones de bajo control **498**

priorizar **475**

servicios **469**

autorizar

acción personalizada de ejemplo **442**

autorizar servicio a un usuario **442**

autorizar a usuarios en elementos del catálogo **502**

autoYaST

archivo de configuración **54**

especificar scripts personalizados **55**

preparar para aprovisionamiento **53**

Azure

configuración de endpoints **201, 277**

crear una reserva **247**

reserva **247**

Azure, acciones personalizadas **368**

Azure, crear blueprint **362**

Azure, reserva **248**

B

blueprint

añadir blueprint XaaS al blueprint de una aplicación **415**

Azure **362**

XaaS **404**

blueprint de clon vinculado, crear **372, 373**

blueprint XaaS, diseño **404**

Blueprint XaaS, añadir al blueprint de una aplicación **415**

blueprints

añadir componentes de red **349**

añadir componentes de red y seguridad **345**

añadir componentes de seguridad **345**

añadir componentes de software **460**

añadir propiedades personalizadas **339**

añadir ubicaciones de centro de datos **378**

añadir un componente de red

Contenedores **353**

añadir un equilibrador de carga a petición **352**

añadir un grupo de seguridad a petición **347**

añadir un grupo de seguridad existente **347**

añadir una etiqueta de seguridad **348**

añadir una red enrutada a petición **350**

añadir una red existente **349**

añadir una red NAT a petición **350**

aprovisionar hosts Docker **362**

asociar un servicio **467**

comportamiento de blueprint anidado **454**

configuración del cuadro de diálogo Nuevo blueprint **315, 339**

configurar recursos de máquinas **371**

crear blueprints de máquinas **313**

crear componentes de máquina **314**

crear componentes de software **384**

crear con NSX **339**

crear para clon de CentOS de vSphere **369**

definir la seguridad y la red de NSX **339**

descripción general **303**

descripciones de configuración (capítulo) **315**

diagrama de flujo de trabajo para crear **310**

ensamblar blueprints de aplicación **453**

ensamblar máquina y software **459**

especificar un tipo de instancia de Amazon **68, 200**

especificar una imagen de máquina de Amazon **67, 68, 200**

exportar **305**

hojas de trabajo de clonación **41**

importar **305**

importar Dukes Bank **307**

permitir a usuarios especificar nombre del host **377**

preparar la creación de un clon vinculado y software **372**

proceso de compilación escalonado **458**

publicar **371, 452**

usar una política de aislamiento de aplicaciones de NSX **343**

usar una política de reserva de puerta de enlace enrutada de NSX **343**

usar una zona de transporte de NSX **343**

blueprints anidados, dependencias **454, 458**

blueprints combinados, Véase blueprint compuesto

blueprints compuestos, Véase también blueprint de aplicación

blueprints de clon, solucionar problemas **337**

- blueprints de clon vinculado, solucionar problemas **337**
- blueprints de máquinas, creación para Rainpole **369**
- blueprints XaaS
 - añadir un nuevo campo **432, 435**
 - añadir un nuevo formulario **430**
 - campos nuevos **421**
 - crear **407, 408**
 - crear usuario en un grupo **440**
 - editar campos **430**
 - editar el formulario **429**
 - ejemplos y escenarios **438**
- blueprints, añadir propiedades personalizadas a componentes de máquina **344**
- buscar la ubicación de servicio DNS **106**

C

- cadenas, propiedades **380**
- capítulo sobre preparaciones externas para el aprovisionamiento **11**
- catálogo
 - añadir elementos a un servicio **502**
 - crear servicio del catálogo con gobierno **501**
- catálogo de servicios
 - acciones **467, 468**
 - añadir blueprints **500**
 - añadir elementos a un servicio **502**
 - añadir elementos del catálogo **461**
 - configurar **463**
 - crear un servicio **464**
 - elementos del catálogo **467**
- catálogo global de Active Directory **89**
- Chrome **136**
- clon vinculado, máquinas para clonar que faltan **337**
- clonar
 - crear blueprint de vSphere para Rainpole **370**
 - crear plantillas (escenario) **77**
 - crear plantillas de Linux **70**
 - crear un blueprint CentOS de vSphere **369**
 - crear un blueprint de CentOS de vSphere **369**
 - hojas de trabajo **41**
 - instalar agente invitado de Linux **35, 37**
 - preparar el aprovisionamiento **38, 52**
- clonar máquina, solucionar problemas de error de aprovisionamiento **337**
- colocación de implementación, configuración **283**
- colocaciones
 - administrar para contenedores **282**
 - crear para contenedores **282**
- complemento, instalar **13**
- complemento Active Directory, añadir endpoint **270**

- complemento de HTTP-REST, añadir endpoints **271**
- complemento de IPAM, instalar y configurar **298**
- complemento de NSX, instalar **13**
- complemento de Orchestrator
 - HTTP-REST **271**
 - PowerShell **273**
 - SOAP **274**
 - vCenter Server **276**
- complemento de PowerShell, añadir endpoint **273**
- complemento de SOAP, añadir endpoints **274**
- complemento de vCenter Server, añadir endpoints **276**
- complemento Orchestrator, Active Directory **270**
- complementos, instalar **298**
- complementos de Orchestrator, añadir como endpoint **270**
- complementos de Orchestrator, descripción general **399**
- componente, autorización **469, 470**
- componente de máquina, especificar configuración de compilación de blueprint **370**
- componentes
 - desarrollar **379**
 - prácticas recomendadas **384**
- componentes de IaaS, configurar para Rainpole **264**
- componentes de software
 - añadir a blueprints **460**
 - aprovisionar **461**
 - conocer la configuración **393**
 - crear **384, 387**
 - crear políticas de aprobación **506**
 - desarrollar **379**
- comprobación de revocación, tarjeta inteligente **125**
- computadas, propiedades **380**
- concesión, configuración del nuevo blueprint **315, 339**
- conector
 - actualizar **141**
 - externo **151**
 - reemplazar la selección de subred predeterminada **112**
- Conector **129**
- conector externo
 - actualización en línea **138**
 - actualización sin conexión **139, 142**
- conector externo, configuración del servidor proxy **138**
- conector externo, opciones posactualización **141**
- conector, actualización **137, 138**
- conector, actualización sin conexión **139**

- conector, configurar ajustes **148**
 - conector, solución de problemas **142**
 - conector, unir a un dominio **109**
 - conectores, código de activación **87**
 - conectores, administrar **108**
 - conexión de Active Directory, asignar memoria **106**
 - conexión de escritorio remoto, configurar conexión mediante RDP **374**
 - conexiones remotas, configurar conexión mediante RDP **374**
 - configuración de administración de identidad y acceso **87**
 - configuración de componente de máquina
 - Amazon **328**
 - OpenStack **333**
 - vCloud Air **324**
 - vSphere **317**
 - configuración de sincronización **105, 131**
 - configuración de tenant, configurar **85**
 - configuración del contenedor, configurar opciones adicionales **284**
 - configurar
 - administración de directorios **144**
 - plantilla de Linux **75**
 - configurar administración de directorios **86**
 - configurar red, para contenedores **295**
 - configurar un vínculo de Active Directory **90**
 - configurar usuarios locales **164**
 - configurar, autenticación de Kerberos **133**
 - configurar, autenticación de RADIUS **122**
 - configurar, autenticación de RSA SecurID **120**
 - configurar, relación de confianza bidireccional **100**
 - conjuntos de directivas de acceso, predeterminados **113**
 - conjuntos de políticas de acceso
 - específico de aplicaciones web **116**
 - portal **114**
 - predeterminados **114, 131**
 - contenedores
 - añadir componentes de red de contenedor a un blueprint **354**
 - añadir configuración de red en la aplicación de contenedor **297**
 - añadir una red en la aplicación de contenedor **295**
 - aprovisionar desde blueprints **362**
 - colocaciones de implementación **282**
 - configurar el registro de imágenes **294**
 - configurar redes en la aplicación contenedor **295**
 - usar componentes de contenedor en un blueprint **355**
 - usar comprobaciones de estado **284**
 - usar configuración de tamaño de clúster y de escalado **288**
 - usar grupos de propiedades en blueprints **359**
 - usar plantillas de contenedores en blueprints **361**
 - usar una configuración de servicio expuesto **287**
 - usar vínculos **286**
 - usar zonas de colocación **283**
 - Contenedores
 - configurar en la interfaz de dispositivo **19**
 - usar la aplicación integrada **280**
 - contenido, propiedades **380**
 - correos electrónicos
 - configurar plantillas de notificaciones de IaaS **178**
 - suscribirse a notificaciones **178**
 - crear
 - acciones personalizadas de XaaS **415**
 - blueprints XaaS **407**
 - plantilla de Linux **75**
 - XaaS **396**
 - crear acciones de script y flujos de trabajo **419**
 - crear host **281**
 - crear opciones de blueprint XaaS **409**
 - crear una acción personalizada para iniciar una máquina virtual de Amazon **450**
 - crear una asignación de recursos para instancias de Amazon **450**
 - credenciales, almacenamiento **186**
 - credenciales de usuario, almacenamiento **186**
 - cuadros de texto, añadir **428, 433, 438**
- ## D
- DataCenterLocations.xml, especificar ubicaciones de centro de datos **179**
 - definiciones, XaaS **403**
 - definiciones de valores externos
 - añadir **428**
 - asignar en el diseñador de formularios **424**
 - dependencias, asignación en blueprints **458**
 - descargar servicio de arranque del agente **75**
 - descripción general, Configuración de administración de identidad y acceso **87**
 - descripción general de complementos de Orchestrator **399**
 - diseñador de formularios **425**
 - descripción general del complemento Active Directory **399**
 - descripción general del complemento HTTP-REST **399**
 - descripción general del complemento PowerShell **399**

- descripción general del complemento SOAP **399**
- direcciones IP estáticas, usar **211**
- direcciones IP flexibles, crear para implementaciones de Amazon **23**
- directivas de acceso
 - red **113**
 - resultado mínimo de la autenticación **113**
- directorios, añadir **87**
- diseñador de formularios
 - campos nuevos **421**
 - descripción general **425**
 - editar recursos personalizados **426**
 - restricciones que implementar **423**
- domain_krb.properties, solución de problemas **113**
- Dukes Bank
 - configurar en el entorno de vSphere **308**
 - convertir la máquina de referencia en una plantilla **81**
 - crear plantillas **80**
 - importar **307**
 - importar la aplicación de muestra **306**
 - solicitar la aplicación de muestra **309**

E

- editar un formulario, ejemplos **446**
- ejemplo
 - acción personalizada para migrar máquina virtual **443**
 - acción personalizada para migrar máquina virtual con vMotion **445**
 - acción personalizada para tomar un snapshot **448**
 - autorizar servicio a un consumidor **442**
 - cambiar contraseña de usuario **441**
 - crear servicios **442**
 - crear un recurso personalizado **439**
 - crear usuario en un grupo **440**
 - migrar máquina virtual **444, 445**
 - publicar una acción personalizada **444, 447, 449**
 - tomar un snapshot de una máquina virtual **448**
 - XaaS para crear y modificar un usuario **438**
- ejemplo de política de aprobación, varias autorizaciones **481**
- elemento del catálogo, autorización **469, 470**
- elementos de recurso personalizado, editar **427**
- elementos del catálogo
 - añadir a un servicio **461, 466**
 - asociar un servicio **467**
 - diseñar blueprints para elementos del catálogo **303**
 - iniciar sesión en máquinas **500**

- publicación y autorización de un blueprint **452**
- quitar de un servicio **466**
- solicitar **461**
- solicitar para Rainpole **499**
- elementos del catálogo de servicios, quitar **466**
- eliminar
 - política de aprobación **496**
 - tenant **165**
- encabezados de sección, añadir **428, 433, 437**
- encadenamiento de autenticación **114**
- endpoint, integración de red **190**
- endpoint de Microsoft Azure **201, 277**
- endpoint de XaaS, crear **270**
- endpoints
 - crear **188**
 - crear Hyper-V (SCVMM) **196**
 - crear KVM (RHEV) **197**
 - crear NetApp ONTAP **197**
 - crear para Amazon AWS **199**
 - crear para grupo de Xen **198**
 - crear para Hyper-V **196**
 - crear para vCloud Air **193**
 - crear para vCloud Director **193, 194**
 - crear para vSphere **188**
 - crear un endpoint de vCloud **193, 194**
 - crear vSphere **190**
 - crear XenServer independiente **199**
 - importar **204**
 - importar un archivo CSV **205**
 - IPAM externo **192**
 - OpenStack **203**
 - PowerVC **203**
 - suscripción de vCloud Air **193**
 - vCloud Air OnDemand **193**
 - vSphere **15**
- endpoints de vCloud Air, solucionar problemas de URL de administración **206**
- enlazar, propiedades **382, 457**
- entidad de certificación de tarjeta inteligente **125**
- entidad de certificación pública **149**
- equilibrio de carga, añadir un equilibrador de carga a petición a un blueprint **352**
- escalado, blueprints XaaS **404**
- escalado horizontal/escalado vertical, aprovisionar **458**
- escalado XaaS **404**
- especificación de personalización
 - crear con vSphere Web Client **79, 82**
 - crear en vSphere Web Client **71**
- ESX, Véase VMware ESX
- ESXi, Véase VMware ESXi
- etiquetas de seguridad, añadir un grupo a petición al blueprint **348**

F

federación de SAML, administración de directorios y SSO2 **102**

Firefox **136**

FlexClone, crear endpoints de NetApp ONTAP **197**

flujo de trabajo, solicitud del catálogo de servicios con una política de aprobación **483**

flujos de trabajo por tenant, configurar carpeta predeterminada **181**

formulario de aprobación configurar **487**

propiedad del sistema **487**

propiedad personalizada **487**

formulario de detalles de la acción enviados, añadir **447**

formularios dinámicos, XaaS **421**

funciones

- asignar a grupos personalizados **154, 161**
- asignar funciones de usuario **154**
- configurar funciones de usuario **154**

G

glosario **7**

grupo de Xen, crear endpoint de grupo de Xen independiente **198**

grupos

- configurar grupos personalizados **154**
- crear grupos personalizados **154**

grupos de propiedades

- configuración del nuevo blueprint **315, 339**
- propiedades de contenedores **359**

grupos de seguridad

- con OpenStack **25**
- especificar un grupo de seguridad de Amazon **21, 231**
- usar activación de aislamiento de aplicaciones **343**
- usar política de aislamiento de aplicaciones **345**

grupos de seguridad, añadir un grupo a petición al blueprint **347**

grupos de tejidos, crear **207, 265**

grupos empresariales

- configurar grupos empresariales **154**
- crear **155, 266**
- rendimiento lento **157**
- resolución de problemas **157**

grupos personalizados

- crear **161**
- resolución de problemas **157**

H

herramientas de Amazon

- usar almacenamiento en bloque flexible **23**

- usar direcciones IP flexibles **23**
- usar nube privada virtual **22**
- usar regiones de servicios web **21**
- usar un equilibrador de carga flexible **22**

Hyper-V, crear endpoint de Hyper-V independiente **196**

I

IaaS, descripción general de la configuración **185**

imágenes de máquina virtual, descripción general **66**

información actualizada **9**

información de compilación, especificar configuración de blueprint **370**

iniciar la interfaz de configuración de Orchestrator **182**

iniciar sesión en

- cliente de Orchestrator **183**
- iniciar **182**
- interfaz de configuración de Orchestrator **182**

inicio de sesión de tenant, personalización de marca **166**

instalar servicio de arranque del agente **75**

instancia de Orchestrator integrada **397**

instancias de proveedor de identidades, selección **129**

integración, preparar el entorno **11**

integrar con Active Directory **89**

interfaz de configuración de Orchestrator, inicio de sesión **182**

Internet Explorer **134**

IPAM

- configurar perfiles de red **210**
- configurar perfiles de red externa **214, 217**

IPAM, preparación y configuración para proveedores externos **16, 17, 269**

IPv6, no compatible con componentes de software **456**

K

Kerberos **133, 134, 136**

kickstart, especificar scripts personalizados **55**

Kickstart

- archivo de configuración **54**
- preparar para aprovisionamiento **53**

Kickstart de Linux, especificar scripts personalizados **55**

L

Linux

- archivo de configuración **54**
- preparar para aprovisionamiento **53**

M

Manager Service, configurar para agente invitado **35**
 máquina de referencia, convertir a plantilla para la clonación **70**
 máquina de referencia de Linux, convertir a plantilla para la clonación **70**
 máquina virtual de Linux, actualizar plantillas **76**
 máquina virtual de Windows, actualizar plantillas existentes **76**
 máquinas, configurar opciones de Amazon opcionales **21**
 matriz, propiedades **380**
 métodos de aprovisionamiento, elegir **27**
 métodos de autenticación
 añadir a política **132**
 relación con las directivas de acceso **113**
 relación con las políticas de acceso **114**
 Microsoft azure, reserva **248**
 mostrar ubicación al solicitar, habilitar selección de ubicación de centro de datos **378**

N

Net App FlexClone, acerca del aprovisionamiento **313**
 NetApp FlexClone, crear endpoints **197**
 nivel de aprobación, añadir **491**
 niveles, políticas de aprobación **489**
 niveles de aprobación posterior, crear **485**
 niveles de aprobación previa, crear **485**
 nodo único, enlazar **382, 457**
 nombres de host, permitir a usuarios especificar **377**
 notificación de correo electrónico de caducidad de máquina, personalizar **177**
 notificaciones
 añadir servidores de correo electrónico entrante **174**
 añadir servidores de correo electrónico saliente **173, 175**
 configurar **168, 171**
 configurar escenarios **177**
 configurar plantillas de correos electrónicos de IaaS **178**
 crear servidor entrante global **171**
 crear servidor saliente global **172**
 habilitar **177**
 reemplazar servidor entrante predeterminado **176**
 reemplazar servidor saliente predeterminado **176**
 revertir a los servidores predeterminados **177**
 suscribirse **178**
 NSX
 aprovisionamiento en un entorno de VC cruzado **15**

crear blueprints **339**

crear endpoints **188**

nube privada virtual, configurar para usar con Amazon **22**

O

Opciones de blueprint XaaS **409**
 opciones de configuración de NSX
 usar aislamiento de aplicaciones **339**
 usar una política de reserva de puerta de enlace enrutada y de Edge **339**
 usar una puerta de enlace enrutada **339**
 usar una zona de transporte **339**
 opciones de política de aprobación **488**
 opciones de recursos personalizados de XaaS **406**
 OpenLDAP, administración de directorios **94**
 OpenLDAP, limitaciones **98**
 OpenStack
 aprovisionar imágenes de máquina virtual **66**
 asignar una dirección IP flotante **25**
 compatibilidad con grupos de seguridad **25**
 imágenes de máquina virtual **66**
 tipos **67**
 usar funciones opcionales **25**
 Orchestrator
 carpeta raíz predeterminada **181**
 integración **397**
 orden de método de autenticación **132**

P

pares de claves
 cargar una clave privada **209**
 crear **209**
 descripción general **208**
 exportar una clave privada **209**
 PEBuilder
 usar scripts personalizados **61**
 Véase también VMware PEBuilder
 perfiles de red
 asignar a una reserva **260**
 configurar rangos de IP **216, 226**
 configurar rangos de IP con el endpoint de IPAM suministrado **222**
 configurar rangos de IP con un endpoint de IPAM de terceros **224**
 configurar rangos de IP desde IPAM externo **219**
 creación de perfil de red enrutada a petición **220**
 crear **210**
 crear rango de redes mediante CSV **212**
 crear un enrutamiento a petición con el endpoint de IPAM suministrado **220**

- crear un perfil de red enrutada a petición con un endpoint de IPAM de terceros **222**
- crear un perfil de red externa **214, 217**
- crear un perfil de red NAT **224**
- especificar información de la red enrutada del endpoint de IPAM suministrado **221**
- especificar información de la red enrutada para el endpoint de IPAM de terceros **223**
- especificar información de red **218**
- especificar información de red externa **215**
- especificar información de red NAT **225**
- preparar y configurar proveedores de IPAM externos **16, 17**
- usar **211, 227**
- personalización de marca **166**
- personalización de marca, aplicaciones de tenant **167**
- personalización de marca, página de inicio de sesión de tenant **166**
- personalizar marcas, configurar para Rainpole **161**
- plantillas
 - aprovisionar una plantilla o una imagen de contenedor **291**
 - convertir máquina de referencia en plantilla de clonación **78**
 - crear especificaciones de personalización para la clonación de Linux **71**
 - crear para clonar máquinas vSphere CentOS **69**
 - crear para la clonación de Linux **70**
 - crear una plantilla de clon de vSphere CentOS **69**
 - crear una plantilla de contenedor personalizada **289**
 - exportar un archivo de Docker Compose **292**
 - exportar un archivo de plantilla **292**
 - importar un archivo de plantilla o un archivo de Docker Compose **290**
 - preparar el aprovisionamiento de software (capítulo) **73**
 - solucionar problemas de plantillas que faltan **337**
 - usar contenedores en vRealize Automation **289**
 - usar plantillas de contenedores en blueprints **361**
- plantillas de MV, actualizar **76**
- política, Active Directory **299**
- política de acceso de usuarios, administrar **117**
- política de Active Directory
 - crear **299, 300**
 - propiedades personalizadas **299**
- política de aprobación
 - autorización **472**
 - copiar **494**
 - desactivar **495**
 - eliminar **496**
 - flujo de trabajo del catálogo de servicios **483**
 - formulario **493**
 - modificar **494**
 - nivel de aprobación **491**
 - propiedad personalizada **493**
 - propiedades del sistema **493**
 - tipo de política **484, 488**
- política de implementación, para colocaciones **283**
- política de seguridad de NSX, habilitar **14**
- políticas, crear políticas de reserva **261**
- políticas de acceso
 - específico de aplicaciones web **116**
 - Intensidad de autenticación **131**
 - puntuación mínima de autenticación **114, 116**
- red **114, 116**
- Red **131**
- relación con los proveedores de identidades **114**
- tipo de cliente **131**
- TTL **114, 116, 131**
- Políticas de Active Directory, reemplazar **301**
- políticas de aprobación
 - acciones **479**
 - aplicar en autorizaciones **507**
 - configuraciones de muestra **477**
 - crear **483, 504**
 - crear para componentes de software **506**
 - información general **484**
 - nivel de aprobación posterior **485**
 - nivel de aprobación previa **485**
 - niveles **489**
- políticas de reserva
 - asignar a una reserva **262**
 - crear **261**
 - crear y aplicar para controlar el aprovisionamiento **260**
 - crear y usar políticas de reserva **228**
- políticas de reserva de almacenamiento
 - asignar a un almacén de datos **264**
 - asignar almacenes de datos **262**
 - crear **263**
 - crear y usar políticas de reserva de almacenamiento **228**
- prefijos de máquina
 - configurar **207**
 - configurar para Rainpole **266**

- preparar el aprovisionamiento
 - clonar **38**
 - vCloud Director y vCloud Air **52**
- preparar plantillas de Linux **81**
- PrePostProvisioningExample.vbs, script de ejemplo **30**
- propiedad del sistema, política de aprobación **493**
- propiedad personalizada, política de aprobación **493**
- propiedades
 - cadena **380**
 - computadas **380**
 - contenido **380**
 - matriz **380**
- propiedades personalizadas
 - añadir al componente de tipo de máquina en el lienzo **344**
 - configuración del nuevo blueprint **315, 339**
 - configurar **87**
 - limpieza de Active Directory **375**
 - ver configuración de las propiedades combinadas **315, 339**
- proteger **87**
- proveedor de identidades
 - Conector **129**
 - terceros **129**
- proveedores de identidades
 - externos **127**
 - relación con las políticas de acceso **114**
- publicar
 - acciones personalizadas **418**
 - ejemplos de acciones personalizadas **444, 447, 449**
- publicar una acción personalizada **451**
- público objetivo **7**
- puerta de enlace enrutada, configurar para **255**

R

- rangos de IP
 - configurar **222, 224, 226**
 - configurar para perfil de red externa **216, 219**
- rangos de redes, relación con las políticas de acceso **114**
- rangos de redes, administrar **129**
- RDP, Véase conexión de escritorio remoto
- recopilación de datos, error en endpoint de vSphere **205**
- recursos de asignación
 - especificar en reservas de vCloud Air **241**
 - especificar en reservas de vCloud Director **245**
- recursos de máquina de Amazon, configurar tipos de instancia **68, 200**
- recursos informáticos, añadir ubicaciones de centro de datos **268**

- recursos personalizados
 - añadir **405**
 - editar el formulario **426**
 - opciones **406**
- red
 - añadir a plantilla de contenedor **297**
 - añadir componentes de red a un blueprint **345, 349**
 - añadir una red enrutada a petición a un blueprint **350**
 - añadir una red existente a un blueprint **349**
 - añadir una red NAT a petición a un blueprint **350**
 - trabajar con **295**
 - usar política de reserva de puerta de enlace enrutada **343**
- red a VPC de Amazon, configurar conectividad para una prueba de concepto **24**
- red y seguridad
 - añadir componentes al lienzo de diseño **355**
 - lista de comprobación de preparación externa **12, 15, 255, 345**
- redes
 - añadir componentes de red de contenedor a un blueprint **354**
 - configurar reservas **255**
 - configurar seguridad **345**
- redes de contenedor, añadir un componente de red Contenedores a un blueprint **353**
- reemplazar global, servidores de correo electrónico **176**
- reemplazar la selección de subred predeterminada **112**
- registros
 - configurar plantillas **294**
 - registro de imágenes **294**
- reglas de política, encadenamiento de autenticación **114**
- relación de confianza bidireccional, configurar **100**
- rendimiento lento, grupos personalizados **157**
- reserva de Azure, información de red **249**
- reserva, Microsoft Azure **247**
- reservas
 - añadir compatibilidad con túneles SSH a una reserva **251**
 - asignar políticas de reserva **262**
 - Azure **249**
 - configurar red **255**
 - creación para Rainpole **267**
 - crear políticas de reserva **261**
 - crear reservas **228**
 - crear reservas de vCloud Air **241**
 - crear reservas de vCloud Director **245**
 - crear reservas para Amazon **21, 231**

- crear una reserva de OpenStack **235**
 - crear una reserva de vCloud Air **239, 240, 242**
 - crear una reserva de vCloud Director **243, 244, 246**
 - crear una reserva virtual **256, 259**
 - crear y usar reservas de nube **229**
 - crear y usar reservas virtuales **253**
 - elegir el tipo de reserva que crear **228**
 - FlexClone **257**
 - información de recursos de Azure **248**
 - NetApp ONTAP **257**
 - tipos **228**
 - usar política de reserva de puerta de enlace enrutada **343**
 - usar reservas de nube **229**
 - usar reservas virtuales **254**
 - reservas de nube, endpoints **229**
 - reservas virtuales **253**
 - resolución de problemas
 - grupos empresariales **157**
 - grupos personalizados **157**
 - restricciones, diseñador de formularios **423**
 - revocación de certificado de tarjeta inteligente **125**
- S**
- SAML, proveedores de identidades externos **127**
 - SCCM, preparar para aprovisionamiento **56, 57**
 - scripts de VB, Véase scripts de Visual Basic
 - scripts de Visual Basic, habilitar en aprovisionamiento **30**
 - scripts personalizados, especificar para Linux Kickstart/autoYaST **55**
 - SCVMM, crear endpoints **196**
 - SecurID **119**
 - seguridad
 - añadir un grupo de seguridad existente a un blueprint **347**
 - aplicar políticas, grupos y etiquetas **345**
 - configurar integración de red y seguridad **345**
 - selección de controladoras de dominio **110**
 - servicio
 - autorización **469, 470**
 - catálogo de servicios **464**
 - servicios
 - añadir **465**
 - asociar blueprints **467**
 - asociar elementos del catálogo **467**
 - servicios del catálogo
 - añadir elementos del catálogo **497**
 - crear un servicio para la prueba y el desarrollo de blueprints **497**
 - crear un servicio para la prueba y el desarrollo de Rainpole **496**
 - servidor de Orchestrator externo, configurar **181**
 - servidor RADIUS **122**
 - servidor RSA SecurID **120**
 - servidores de correo electrónico
 - añadir entrante **174**
 - añadir saliente **173, 175**
 - configurar **168, 171**
 - crear saliente global **172**
 - crear servidores entrantes globales **171**
 - reemplazar global **176**
 - revertir a los servidores predeterminados **177**
 - software
 - conectividad de red a VPC de Amazon **24**
 - instalar el agente invitado y el agente de arranque **372**
 - preparar el aprovisionamiento de software (capítulo) **73**
 - preparar el entorno de Amazon **21**
 - preparar una base para suministrar componentes de software **372**
 - usar en blueprints **456**
 - Software
 - métodos de aprovisionamiento compatibles **71**
 - preparar una máquina Windows de referencia **73**
 - solucionar problemas, cadenas de XaaS incorrectas **451**
 - SRV **106**
 - Sysprep, para el aprovisionamiento de WIM **59**
- T**
- tarjeta inteligente, configurar **126**
 - tarjeta inteligente, entidad de certificación **125**
 - tarjeta inteligente:autenticación **146**
 - tenant predeterminado
 - configurar para Rainpole **158**
 - configurar usuarios locales **158**
 - tenant, configurar usuarios locales **164**
 - tenant, eliminar **165**
 - tenants
 - asignar administradores **165**
 - configurar **163**
 - configurar el tenant predeterminado para Rainpole **158**
 - configurar usuarios locales **158**
 - crear **163, 164**
 - editar acceso a carpeta de flujo de trabajo **181**
 - personalización de marca **166**

tipo de política de aprobación **484**
 token de activación del conector **147**

U

ubicaciones, permitir a los usuarios
 seleccionar **268**
 ubicaciones de centros de datos
 añadir **179**
 añadir a blueprints **378**
 UPN **124**
 usuarios
 atributos de usuario **105, 131**
 autorizar en elementos del catálogo **498, 502**
 conceder acceso a los usuarios **154**
 configurar **154**
 configurar usuarios locales **158**
 crear grupos personalizados **161**

V

valores, diseñador de formularios **423**
 valores de propiedad, analizar **383**
 varios dominios **89**
 vCenter, asignaciones de recursos **420**
 vCenter Orchestrator
 configurar endpoints **191**
 servidor externo **13**
 vCloud, crear endpoints **193, 194**
 vCloud Air
 preparar el aprovisionamiento de software
 (capítulo) **73**
 preparar la integración **20**
 preparar una máquina Windows de referencia
 para el aprovisionamiento de
 software **73**
 vCloud Director
 asignaciones de recursos **419, 420**
 preparar el aprovisionamiento de software
 (capítulo) **73**
 preparar la integración **19**
 preparar una máquina Windows de referencia
 para el aprovisionamiento de
 software **73**
 vDC de organización, endpoints de vCloud
 Air **193**
 vDCs de organización, crear endpoints **193, 194**
 ver y administrar hosts **280**
 VirtIO, uso con KVM (RHEV) **61**
 VirtualMachine.NetworkN.ProfileName
 asignar un perfil de red a una reserva **260**
 usar una dirección IP estática **211**
 VMware ESXi, preparar para
 aprovisionamiento **53**
 VMware PEBuilder
 crear WinPE **62**
 instalar **60**

vRealize Automation
 agente invitado **75**
 gugent **75**
 proporcionar servicios a petición a los
 usuarios (capítulo) **303**
 vRealize Orchestrator
 configuración externa de **180**
 integrar **191**
 vSphere
 asignaciones de recursos **420**
 crear endpoints **188, 190**
 crear plantillas para la clonación
 (escenario) **77**
 crear reservas para Rainpole **267**
 crear un blueprint de clon CentOS **369**
 crear un blueprint de clon de CentOS **369**
 preparar el aprovisionamiento de software
 (capítulo) **73**
 preparar una máquina Windows de referencia
 para el aprovisionamiento de
 software **73**

X

XaaS
 crear **396**
 definiciones **403**
 diseñador de formularios **421**
 XenServer, crear endpoint de XenServer
 independiente **199**

Z

zona de transporte, especificar un valor para
 NSX **345**