

Administrar vRealize Automation

Octubre de 2022
vRealize Automation 8.7

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

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

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

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

Copyright © 2022 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

- 1 Administrar vRealize Automation 5**
- 2 Administrar usuarios 6**
 - Cómo habilitar grupos de Active Directory para proyectos 7
 - Cómo eliminar usuarios en vRealize Automation 8
 - Cómo editar funciones de usuario en vRealize Automation 9
 - Cómo editar las asignaciones de funciones de grupo en vRealize Automation 9
 - ¿Cuáles son las funciones de usuario de vRealize Automation? 10
 - Habilitar aviso del Departamento de Defensa y banner de consentimiento 28
- 3 Mantener el dispositivo 30**
 - Iniciar y detener vRealize Automation 30
 - Escalar horizontalmente vRealize Automation de uno a tres nodos 32
 - Configurar una regla de antiafinidad y un grupo de máquinas virtuales para una instancia de Workspace ONE Access agrupada en clúster 33
 - Reemplazar un nodo de un dispositivo 34
 - Aumentar el espacio de disco del dispositivo de vRealize Automation 36
 - Actualizar la asignación de DNS para vRealize Automation 36
 - Cambiar la dirección IP de un nodo o clúster 37
 - Cómo habilitar la sincronización de hora 38
 - Cómo se restablece la contraseña raíz 40
- 4 Usar configuraciones de tenant de varias organizaciones en vRealize Automation 42**
 - Configurar tenants de varias organizaciones para vRealize Automation 45
 - Administrar certificados y la configuración de DNS en implementaciones de varias organizaciones de un solo nodo 47
 - Administrar la configuración de certificados y DNS en implementaciones de vRealize Automation agrupadas en clúster 49
 - Iniciar sesión en tenants y agregar usuarios en vRealize Automation 52
 - Usar vRealize Orchestrator con implementaciones de varias organizaciones de vRealize Automation 53
- 5 Trabajar con logs 55**
 - Cómo se trabaja con logs y paquetes de logs 55
 - Cómo se configura el reenvío de logs a vRealize Log Insight 59
 - Cómo crear o actualizar una integración de syslog 64
 - Cómo eliminar una integración de syslog para el registro 66
 - Cómo trabajar con paquetes de contenido 66

6 Participar en el programa de mejora de la experiencia de cliente 69

Cómo hay que unirse al programa o se abandona 69

Cómo se configura la hora de la recopilación de datos para el programa 70

7 Activación del formulario de comentarios en el producto 71

Administrar vRealize Automation

1

En esta guía se describe cómo supervisar y administrar aspectos críticos de la infraestructura y la administración de usuarios de una implementación de vRealize Automation.

Las tareas que se describen aquí son esenciales para que una implementación de vRealize Automation siga funcionando correctamente. Estas tareas incluyen la administración de usuarios y grupos, y la supervisión de logs del sistema.

Además, describe cómo configurar y administrar implementaciones de varias organizaciones.

Mientras que algunas tareas de administración de vRealize Automation se completan en vRealize Automation, otras requieren el uso de productos relacionados, como vRealize Suite Lifecycle Manager y Workspace ONE Access. Los usuarios deben familiarizarse con estos productos y su funcionalidad antes de completar las tareas aplicables.

Por ejemplo, para obtener información sobre copias de seguridad, restauración y recuperación ante desastres, consulte las secciones **Copia de seguridad y restauración, y Recuperación ante desastres > 2019** de la [documentación del producto de vRealize Suite](#).

Nota La recuperación ante desastres se admite en vRealize Automation 8.0.1 y versiones posteriores.

Para obtener información sobre cómo trabajar con la instalación, la actualización y la administración de vRealize Suite Lifecycle Manager, consulte la [documentación del producto de Lifecycle Manager](#).

Administrar usuarios y grupos en vRealize Automation

2

vRealize Automation utiliza VMware Workspace ONE Access, la aplicación de administración de identidades proporcionada por VMware, para importar y administrar usuarios y grupos. Después de crear o importar los usuarios y los grupos, puede administrar las asignaciones de funciones para las implementaciones de tenant único mediante la página Administración de identidades y acceso.

vRealize Automation se instala mediante VMware Lifecycle Manager (vRSLCM o LCM). Al instalar vRealize Automation, debe importar una instancia de Workspace ONE Access existente o implementar una nueva para que sea compatible con la administración de identidades. Estos dos escenarios definen las opciones de administración.

- Si implementa una instancia nueva de Workspace ONE Access, puede administrar usuarios y grupos a través de LCM. Durante la instalación, puede configurar una conexión de Active Directory mediante Workspace ONE Access. De forma alternativa, puede ver y editar algunos aspectos de los usuarios y los grupos en vRealize Automation mediante la página Administración de identidades y acceso como se describe en este documento.
- Si utiliza una instancia de Workspace ONE Access, debe importarla para usarla con vRealize Automation a través de LCM durante la instalación. En este caso, puede seguir utilizando Workspace ONE Access para administrar usuarios y grupos o bien, puede utilizar las funciones de administración de LCM.

Consulte [Iniciar sesión en tenants y agregar usuarios en vRealize Automation](#) para obtener más información sobre cómo administrar usuarios en una implementación de varias organizaciones.

Se deben asignar funciones a los usuarios de vRealize Automation. Las funciones definen el acceso a las características de la aplicación. Cuando se instala vRealize Automation con una instancia de Workspace ONE Access, se crea una organización predeterminada y se asigna al instalador la función de propietario de la organización. El propietario de la organización asigna todas las demás funciones de vRealize Automation.

Existen tres tipos de funciones en vRealize Automation: funciones de organización, funciones de servicio y funciones de proyecto. Para Cloud Assembly, Service Broker y Code Stream, por lo general, las funciones de nivel de usuario pueden utilizar recursos, mientras que para crear y configurar recursos se necesitan funciones de nivel de administrador. Las funciones de

organización definen los permisos dentro del tenant. Los propietarios de organización tienen permisos de nivel de administrador, mientras que los miembros de la organización tienen permisos de nivel de usuario. Los propietarios de la organización pueden agregar y administrar otros usuarios.

Funciones de organización	Funciones de servicio
■ Propietario de la organización	■ Administrador de Cloud Assembly
■ Miembro de la organización	■ Usuario de Cloud Assembly
	■ Visor de Cloud Assembly
	■ Administrador de Service Broker
	■ Usuario de Service Broker
	■ Visor de Service Broker
	■ Administrador de Code Stream
	■ Usuario de Code Stream
	■ Visor de Code Stream

Además, hay dos funciones principales de nivel de proyecto que no se muestran en la tabla: administrador del proyecto y usuario del proyecto. Estas funciones se asignan ad hoc por proyecto con Cloud Assembly. Estas funciones son algo fluidas. El mismo usuario puede ser un administrador en un proyecto y un usuario en otro. Para obtener más información, consulte [¿Cuáles son las funciones de usuario de vRealize Automation?](#).

Para obtener más información sobre cómo trabajar con vRealize Suite Lifecycle Manager y Workspace ONE Access, consulte lo siguiente.

Este capítulo incluye los siguientes temas:

- [Cómo habilitar los grupos de Active Directory en vRealize Automation para los proyectos](#)
- [Cómo eliminar usuarios en vRealize Automation](#)
- [Cómo editar funciones de usuario en vRealize Automation](#)
- [Cómo editar las asignaciones de funciones de grupo en vRealize Automation](#)
- [¿Cuáles son las funciones de usuario de vRealize Automation?](#)
- [Habilitar aviso del Departamento de Defensa y banner de consentimiento](#)

Cómo habilitar los grupos de Active Directory en vRealize Automation para los proyectos

Si un grupo no está disponible en la página Agregar grupos mientras se agregan usuarios a los proyectos, revise la página Administración de identidades y acceso, y agregue el grupo si está disponible. Si el grupo no aparece en la página Administración de identidades y acceso de vRealize Automation, es posible que el grupo no esté sincronizado en la instancia de Workspace ONE Access. Compruebe si se ha sincronizado y, a continuación, siga este procedimiento para agregar el grupo como se muestra aquí.

Para agregar miembros de un grupo de Active Directory a un proyecto, debe asegurarse de que el grupo esté sincronizado con la instancia de Workspace ONE Access y se haya agregado a la organización.

Requisitos previos

Si los grupos no están sincronizados, no estarán disponibles al intentar agregarlos a un proyecto. Compruebe que sincronizó los grupos de Active Directory con su instancia de Lifecycle Manager.

Procedimiento

- 1 Inicie sesión en vRealize Automation como usuario desde el mismo dominio de Active Directory que desea agregar. Por ejemplo, @miempresa.com
- 2 En Cloud Assembly, haga clic en Administración de identidades y acceso en el panel de navegación derecho de encabezados.
- 3 Haga clic en **Grupos empresariales** y, a continuación, en **Asignar funciones**.
- 4 Utilice la función de búsqueda para buscar el grupo que desea agregar y selecciónelo.
- 5 Asigne una función de organización.

Como mínimo, el grupo debe tener una función de miembro de organización. Consulte [Cuáles son las funciones de usuario de vRealize Automation Cloud Assembly](#) para obtener más información.

- 6 Haga clic en **Agregar acceso a servicios**, agregue uno o varios servicios y seleccione una función para cada uno.
- 7 Haga clic en **Asignar**.

Resultados

Ahora puede agregar el grupo de Active Directory a un proyecto.

Cómo eliminar usuarios en vRealize Automation

Puede eliminar usuarios según sea necesario en vRealize Automation.

De forma predeterminada, todos los usuarios se enumeran y no se pueden agregar usuarios con la página Administración de identidades y acceso. Puede eliminar usuarios.

Procedimiento

- 1 Seleccione la pestaña Usuarios activos en la página Administración de identidades y acceso.
- 2 Busque los usuarios que desea eliminar y selecciónelos.
- 3 Haga clic en **Eliminar usuarios**.

Resultados

Se eliminan los usuarios seleccionados.

Cómo editar funciones de usuario en vRealize Automation

Puede editar las funciones asignadas a los usuarios de Workspace ONE Access que se hayan importado a vRealize Automation.

Requisitos previos

Procedimiento

- 1 En Cloud Assembly, haga clic en Administración de identidades y acceso en el panel de navegación derecho de encabezados.
- 2 Seleccione el usuario deseado de la pestaña Usuarios activos y haga clic en **Editar funciones**.
- 3 Puede editar las funciones de organización y servicio para el usuario.
 - Seleccione la lista desplegable que aparece junto al encabezado Asignar funciones de organización para cambiar la relación del usuario con la organización.
 - Haga clic en Agregar acceso a servicios con el fin de agregar nuevas funciones de servicio para el usuario.
 - Para eliminar funciones de usuario, haga clic en la X que se encuentra junto al servicio correspondiente.
- 4 Haga clic en **Guardar**.

Resultados

Se actualizará la asignación de funciones de usuario según lo especificado.

Cómo editar las asignaciones de funciones de grupo en vRealize Automation

Puede editar las asignaciones de funciones de los grupos en vRealize Automation

Requisitos previos

Se importaron los usuarios y grupos desde una instancia de vIDM válida asociada con la implementación de vRealize Automation.

Procedimiento

- 1 En Cloud Assembly, haga clic en Administración de identidades y acceso en el panel de navegación derecho de encabezados.
- 2 Seleccione la pestaña Grupos empresariales.
- 3 En el campo de búsqueda, escriba el nombre del grupo para el que desea editar la asignaciones de funciones.

- 4 Edite las asignaciones de funciones para el grupo seleccionado. Tiene dos opciones.
 - Asignar funciones de organización
 - Asignar funciones de servicio
- 5 Haga clic en **Asignar**.

Resultados

Las asignaciones de funciones se actualizarán según lo especificado.

¿Cuáles son las funciones de usuario de vRealize Automation?

Como propietario de una organización, puede asignar funciones de organización y de servicio a los usuarios. Las funciones determinan qué pueden hacer o ver los usuarios. Luego, en los servicios, el administrador de servicio puede asignar funciones de proyecto. Para determinar la función que desea asignar, evalúe las tareas en las siguientes tablas.

Funciones de servicio de Cloud Assembly

Las funciones de servicio de Cloud Assembly determinan lo que puede ver y hacer en Cloud Assembly. El propietario de una organización define estas funciones de servicio en la consola.

Tabla 2-1. Descripciones de las funciones de servicio de Cloud Assembly

Función	Descripción
Administrador de Cloud Assembly	Un usuario que tiene acceso de lectura y escritura a toda la interfaz de usuario y a los recursos de la API. Esta es la única función de usuario que puede ver y hacer todo, incluidas la adición de cuentas de nube, la creación de nuevos proyectos y la asignación de un administrador de proyectos.
Usuario de Cloud Assembly	Un usuario que no tiene la función de administrador de Cloud Assembly. En un proyecto de Cloud Assembly, el administrador agrega usuarios a los proyectos como miembros, administradores o visores del proyecto. El administrador también puede agregar un administrador del proyecto.
Visor de Cloud Assembly	Un usuario que tiene acceso de lectura para ver información, pero que no puede crear, actualizar ni eliminar valores. Esta es una función de solo lectura en todos los proyectos. Los usuarios con la función de visor pueden ver toda la información que está disponible para el administrador. No puede realizar ninguna acción a menos que se lo convierta en un administrador del proyecto o en un miembro del proyecto. Si el usuario está afiliado a un proyecto, tiene los permisos relacionados con la función. El visor de proyectos no extenderá sus permisos de la forma en que lo hace el administrador o el miembro.

Además de las funciones de servicio, Cloud Assembly tiene funciones de proyecto. Cualquier proyecto está disponible en todos los servicios.

Las funciones de proyecto se definen en Cloud Assembly y pueden variar de un proyecto a otro.

En las siguientes tablas, se indican lo que las diferentes funciones de servicio y de proyecto pueden ver y hacer. Recuerde que los administradores de servicios tienen permisos completos en todas las áreas de la interfaz de usuario.

Las descripciones de las funciones de proyecto sirven como ayuda para decidir qué permisos otorgar a los usuarios.

- Los administradores de proyectos aprovechan la infraestructura que el administrador de servicios crea para garantizar que los miembros del proyecto dispongan de los recursos que necesitan para realizar su labor de desarrollo.
- Los miembros del proyecto trabajan dentro de sus proyectos para diseñar e implementar plantillas de nube. En la siguiente tabla, sus proyectos solo pueden incluir recursos que sean de su propiedad o que se compartan con otros miembros del proyecto.
- Los visores de proyectos están restringidos al acceso de solo lectura, excepto en algunos casos en los que pueden realizar tareas no destructivas, como descargar plantillas de nube.

- Los supervisores de proyectos son aprobadores en Service Broker para sus proyectos en los que se define una directiva de aprobación con un aprobador de supervisor de proyectos. Si desea proporcionar al supervisor contexto para las aprobaciones, considere también otorgarle la función de miembro o visor del proyecto.

Tabla 2-2. Funciones de servicio y de proyecto de Cloud Assembly

Contexto de interfaz de usuario	Tarea	Administrador de Cloud Assembly	Visor de Cloud Assembly	Usuario de Cloud Assembly			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
Acceder a Cloud Assembly							
Consola	En la consola de vRA, puede ver y abrir Cloud Assembly	Sí	Sí	Sí	Sí	Sí	Sí
Infraestructura							
	Ver y abrir la pestaña Infraestructura	Sí	Sí	Sí	Sí	Sí	Sí
Configurar > Proyectos	Crear proyectos	Sí					
	Actualice o elimine los valores del resumen del proyecto, el aprovisionamiento, Kubernetes, las integraciones y las configuraciones del proyecto de prueba.	Sí					
	Agregar usuarios y grupos, y asignar funciones en proyectos	Sí		Sí. Sus proyectos.			
	Ver proyectos	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos
Configurar > Zonas de nube	Crear, actualizar o eliminar zonas de nube	Sí					
	Ver zonas de nube	Sí	Sí				

Tabla 2-2. Funciones de servicio y de proyecto de Cloud Assembly (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Cloud Assembly	Visor de Cloud Assembly	Usuario de Cloud Assembly			
				El usuario debe ser administrador o miembro del proyecto para ver y realizar tareas relacionadas con el proyecto.			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
	Ver panel de control Información de la zona de nube	Sí	Sí				
	Ver alertas de zonas de nube	Sí	Sí				
Configurar: zonas de Kubernetes	Crear, actualizar o eliminar zonas de Kubernetes	Sí					
	Ver zonas de Kubernetes	Sí	Sí				
Configurar: tipos	Crear, actualizar o eliminar tipos	Sí					
	Ver tipos	Sí	Sí				
Configurar > Asignaciones de imagen	Crear, actualizar o eliminar asignaciones de imagen	Sí					
	Ver asignaciones de imagen	Sí	Sí				
Configurar > Perfiles de red	Crear, actualizar o eliminar perfiles de red	Sí					
	Ver perfiles de red de imagen	Sí	Sí				
Configurar > Perfiles de almacenamiento	Crear, actualizar o eliminar perfiles de almacenamiento	Sí					
	Ver perfiles de almacenamiento de imagen	Sí	Sí				
Configurar: tarjetas de precios	Crear, actualizar o eliminar tarjetas de precios	Sí					
	Ver las tarjetas de precios	Sí	Sí				

Tabla 2-2. Funciones de servicio y de proyecto de Cloud Assembly (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Cloud Assembly	Visor de Cloud Assembly	Usuario de Cloud Assembly			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
Configurar > Etiquetas	Crear, actualizar o eliminar etiquetas	Sí		El usuario debe ser administrador o miembro del proyecto para ver y realizar tareas relacionadas con el proyecto.			
	Ver etiquetas	Sí	Sí				
Recursos > Informáticos	Agregar etiquetas a recursos informáticos detectados	Sí					
	Ver los recursos informáticos detectados	Sí	Sí				
Recursos: redes	Modificar etiquetas de red, rangos de IP y direcciones IP	Sí					
	Ver recursos de red detectados	Sí	Sí				
Recursos: seguridad	Agregar etiquetas a grupos de seguridad detectados	Sí					
	Ver grupos de seguridad detectados	Sí	Sí				
Recursos > Almacenamiento	Agregar etiquetas a almacenamiento detectado	Sí					
	Ver almacenamiento	Sí	Sí				
Recursos: Kubernetes	Implementar o agregar clústeres de Kubernetes, y crear o agregar espacios de nombres	Sí					
	Ver clústeres y espacios de nombres de Kubernetes	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	

Tabla 2-2. Funciones de servicio y de proyecto de Cloud Assembly (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Cloud Assembly	Visor de Cloud Assembly	Usuario de Cloud Assembly			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
Actividad > Solicitudes	Eliminar registros de solicitud de implementación	Sí		El usuario debe ser administrador o miembro del proyecto para ver y realizar tareas relacionadas con el proyecto.			
	Ver registros de solicitud de implementación	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	
Actividad: logs de eventos	Ver logs de eventos	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	
Conexiones > Cuentas de nube	Crear, actualizar o eliminar cuentas de nube	Sí					
	Ver cuentas de nube	Sí	Sí				
Conexiones > Integraciones	Crear, actualizar o eliminar integraciones	Sí					
	Ver integraciones	Sí	Sí				
Incorporación	Crear, actualizar o eliminar planes de incorporación	Sí					
	Ver planes de incorporación	Sí	Sí			Sí. Sus proyectos	
Extensibilidad							
	Consultar y abrir la pestaña Extensibilidad	Sí	Sí			Sí	
Eventos	Ver eventos de extensibilidad	Sí	Sí				
Suscripciones	Crear, actualizar o eliminar suscripciones de extensibilidad	Sí					
	Desactivar suscripciones	Sí					
	Ver suscripciones	Sí	Sí				

Tabla 2-2. Funciones de servicio y de proyecto de Cloud Assembly (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Cloud Assembly	Visor de Cloud Assembly	Usuario de Cloud Assembly			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
El usuario debe ser administrador o miembro del proyecto para ver y realizar tareas relacionadas con el proyecto.							
Biblioteca: temas de eventos	Ver temas de eventos	Sí	Sí				
Biblioteca: acciones	Crear, actualizar o eliminar acciones de extensibilidad	Sí					
	Ver acciones de extensibilidad	Sí	Sí				
Biblioteca: flujos de trabajo	Ver flujos de trabajo de extensibilidad	Sí	Sí				
Actividad: ejecuciones de acciones	Cancelar o eliminar ejecuciones de acciones de extensibilidad	Sí					
	Ver ejecuciones de acciones de extensibilidad	Sí	Sí			Sí. Sus proyectos	
Actividad: ejecuciones de flujos de trabajo	Ver ejecuciones de flujos de trabajo de extensibilidad	Sí	Sí				
Diseño							
Diseño	Abrir la pestaña Diseño	Sí	Sí	Sí.	Sí.	Sí.	Sí
Plantillas de nube	Crear, actualizar y eliminar plantillas de nube	Sí		Sí. Sus proyectos	Sí. Sus proyectos		
	Ver plantillas de nube	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	
	Descargar plantillas de nube	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	
	Cargar plantillas de nube	Sí		Sí. Sus proyectos	Sí. Sus proyectos		
	Implementar plantillas de nube	Sí		Sí. Sus proyectos	Sí. Sus proyectos		

Tabla 2-2. Funciones de servicio y de proyecto de Cloud Assembly (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Cloud Assembly	Visor de Cloud Assembly	Usuario de Cloud Assembly			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
	Asignar una versión y restaurar plantillas de nube	Sí		Sí. Sus proyectos	Sí. Sus proyectos		
	Publicar plantillas de nube en el catálogo	Sí		Sí. Sus proyectos	Sí. Sus proyectos		
Recursos personalizados	Crear, actualizar o eliminar recursos personalizados	Sí					
	Ver recursos personalizados	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	
Acciones personalizadas	Crear, actualizar o eliminar acciones personalizadas	Sí					
	Ver acciones personalizadas	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	
Recursos							
	Consultar y abrir la pestaña Recursos	Sí	Sí	Sí	Sí	Sí	Sí
Implementaciones	Ver implementaciones, incluidos los detalles de la implementación, el historial de implementaciones, y la información de supervisión, alertas, optimización y solución de problemas	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	
	Administrar alertas	Sí		Sí. Sus proyectos	Sí. Sus proyectos		
	Ejecutar acciones del día 2 en implementaciones basadas en directivas	Sí		Sí. Sus proyectos	Sí. Sus proyectos		

Tabla 2-2. Funciones de servicio y de proyecto de Cloud Assembly (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Cloud Assembly	Visor de Cloud Assembly	Usuario de Cloud Assembly			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
				El usuario debe ser administrador o miembro del proyecto para ver y realizar tareas relacionadas con el proyecto.			
Recursos: todos los recursos	Ver todos los recursos detectados	Sí	Sí				
	Ejecute acciones del día 2 en recursos detectados. Acciones disponibles solo en máquinas y limitadas al encendido y apagado para todas las máquinas, y la consola remota para máquinas vSphere.	Sí					
Recursos: todos los recursos	Ver recursos implementados, incorporados y migrados	Sí	Sí	Sí. Sus proyectos.	Sí. Sus proyectos.	Sí. Sus proyectos.	
	Ejecutar acciones del día 2 en recursos implementados, incorporados y migrados en función de las directivas	Sí	Sí	Sí. Sus proyectos.	Sí. Sus proyectos.		
Recursos : máquinas virtuales	Ver máquinas detectadas	Sí	Sí				

Tabla 2-2. Funciones de servicio y de proyecto de Cloud Assembly (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Cloud Assembly	Visor de Cloud Assembly	Usuario de Cloud Assembly			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
	Ejecutar acciones del día 2 en máquinas detectadas. Las acciones se limitan al encendido y apagado, y a la consola remota para las máquinas vSphere.	Sí		El usuario debe ser administrador o miembro del proyecto para ver y realizar tareas relacionadas con el proyecto.			
	Crear nueva máquina virtual	Sí					
	Ve recursos implementados, incorporados y migrados.	Sí		Sí. Sus proyectos.	Sí. Sus proyectos.	Sí. Sus proyectos.	
	Ejecutar acciones del día 2 en recursos implementados, incorporados y migrados en función de las directivas	Sí		Sí. Sus proyectos.	Sí. Sus proyectos.		
Recursos > Volúmenes	Ver volúmenes detectados	Sí	Sí				
	No hay acciones del día 2 disponibles						
	Ver volúmenes implementados, incorporados y migrados	Sí	Sí	Sí. Sus proyectos.	Sí. Sus proyectos.	Sí. Sus proyectos.	

Tabla 2-2. Funciones de servicio y de proyecto de Cloud Assembly (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Cloud Assembly	Visor de Cloud Assembly	Usuario de Cloud Assembly			
				El usuario debe ser administrador o miembro del proyecto para ver y realizar tareas relacionadas con el proyecto.			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
	Ejecutar acciones del día 2 en volúmenes implementados, incorporados y migrados en función de las directivas	Sí		Sí. Sus proyectos.	Sí. Sus proyectos.		
Recursos: redes y seguridad	Ver redes detectadas, equilibradores de carga y grupos de seguridad	Sí	Sí				
	No hay acciones del día 2 disponibles						
	Ver redes implementadas, incorporadas y migradas, equilibradores de carga y grupos de seguridad	Sí	Sí	Sí. Sus proyectos.	Sí. Sus proyectos.	Sí. Sus proyectos.	
	Ejecutar acciones del día 2 en redes implementadas, incorporadas y migradas, equilibradores de carga y grupos de seguridad en función de las directivas	Sí		Sí. Sus proyectos.	Sí. Sus proyectos.		
Alertas							
	Ver y abrir la pestaña Alertas	Sí	Sí	Sí	Sí	Sí	
	Administrar alertas	Sí		Sí. Sus proyectos	Sí. Sus proyectos		
	Ver alertas	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	

Funciones de servicio de Service Broker

Las funciones de servicio de Service Broker determinan lo que puede ver y hacer en Service Broker. El propietario de una organización define estas funciones de servicio en la consola.

Tabla 2-3. Descripciones de funciones de servicio de Service Broker

Función	Descripción
Administrador de Service Broker	Debe tener acceso de lectura y escritura a toda la interfaz de usuario y a los recursos de la API. Esta es la única función de usuario que puede realizar todas las tareas, como crear un proyecto nuevo y asignar un administrador de proyecto.
Usuario de Service Broker	<p>Todo usuario que no tiene la función de administrador de Service Broker.</p> <p>En un proyecto de Service Broker, el administrador agrega usuarios a los proyectos como miembros, administradores o visores del proyecto. El administrador también puede agregar un administrador del proyecto.</p>
Visor de Service Broker	<p>Un usuario que tiene acceso de lectura para ver información, pero que no puede crear, actualizar ni eliminar valores.</p> <p>Los usuarios con la función de visor pueden ver toda la información que está disponible para el administrador. No puede realizar ninguna acción a menos que se lo convierta en un administrador del proyecto o en un miembro del proyecto. Si el usuario está afiliado a un proyecto, tiene los permisos relacionados con la función. El visor de proyectos no extenderá sus permisos de la forma en que lo hace el administrador o el miembro.</p>

Además de las funciones de servicio, Service Broker tiene funciones de proyecto. Cualquier proyecto está disponible en todos los servicios.

Las funciones de proyecto se definen en Service Broker y pueden variar de un proyecto a otro.

En las siguientes tablas, se indican lo que las diferentes funciones de servicio y de proyecto pueden ver y hacer. Recuerde que los administradores de servicios tienen permisos completos en todas las áreas de la interfaz de usuario.

Use las siguientes descripciones de las funciones de proyecto como ayuda para decidir qué permisos otorgará a los usuarios.

- Los administradores de proyectos aprovechan la infraestructura que el administrador de servicios crea para garantizar que los miembros del proyecto dispongan de los recursos que necesitan para realizar su labor de desarrollo.
- Los miembros del proyecto trabajan dentro de sus proyectos para diseñar e implementar plantillas de nube. En la siguiente tabla, los proyectos solo pueden incluir recursos que sean de su propiedad o que se compartan con otros miembros del proyecto.
- Los visores de proyectos están restringidos al acceso de solo lectura.

- Los supervisores de proyectos son aprobadores en Service Broker para sus proyectos en los que se define una directiva de aprobación con un aprobador de supervisor de proyectos. Si desea proporcionar al supervisor contexto para las aprobaciones, considere también otorgarle la función de miembro o visor del proyecto.

Tabla 2-4. Funciones de servicio y funciones de proyecto de Service Broker

Contexto de interfaz de usuario	Tarea	Administrador de Service Broker	Visor de Service Broker	Usuario de Service Broker			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
Acceso a Service Broker							
Consola	En la consola, puede ver y abrir Service Broker	Sí	Sí	Sí	Sí	Sí	Sí
Infraestructura							
	Ver y abrir la pestaña Infraestructura	Sí	Sí				
Configurar > Proyectos	Crear proyectos	Sí					
	Actualice o elimine los valores del resumen del proyecto, el aprovisionamiento, Kubernetes, las integraciones y las configuraciones del proyecto de prueba.	Sí					
	Agregar usuarios y grupos, y asignar funciones en proyectos	Sí		Sí. Sus proyectos.			
	Ver proyectos	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	
Configurar > Zonas de nube	Crear, actualizar o eliminar zonas de nube	Sí					
	Ver zonas de nube	Sí	Sí				
Configurar: zonas de Kubernetes	Crear, actualizar o eliminar zonas de Kubernetes	Sí					

Tabla 2-4. Funciones de servicio y funciones de proyecto de Service Broker (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Service Broker	Visor de Service Broker	Usuario de Service Broker			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
				El usuario debe ser el administrador del proyecto para ver y realizar tareas relacionadas con el proyecto.			
	Ver zonas de Kubernetes	Sí	Sí				
Conexiones > Cuentas de nube	Crear, actualizar o eliminar cuentas de nube	Sí					
	Ver cuentas de nube	Sí	Sí				
Conexiones > Integraciones	Crear, actualizar o eliminar integraciones	Sí					
	Ver integraciones	Sí	Sí				
Actividad > Solicitudes	Eliminar registros de solicitud de implementación	Sí					
	Ver registros de solicitud de implementación	Sí					
Actividad: logs de eventos	Ver logs de eventos	Sí					
Contenido y directivas							
	Consultar y abrir la pestaña Contenido y directivas	Sí	Sí				
Orígenes de contenido	Crear, actualizar o eliminar orígenes de contenido	Sí					
	Ver orígenes de contenido	Sí	Sí				
Uso compartido de contenido	Agregar o eliminar contenido compartido	Sí					
	Ver contenido compartido	Sí	Sí				

Tabla 2-4. Funciones de servicio y funciones de proyecto de Service Broker (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Service Broker	Visor de Service Broker	Usuario de Service Broker			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
				El usuario debe ser el administrador del proyecto para ver y realizar tareas relacionadas con el proyecto.			
Contenido	Personalizar formulario y configurar elemento	Sí					
	Ver contenido	Sí	Sí				
Directivas: definiciones	Crear, actualizar o eliminar definiciones de directivas	Sí					
	Ver definiciones de directivas	Sí	Sí				
Directivas: aplicación	Ver log de aplicación	Sí	Sí				
Notificaciones: servidor de correo electrónico	Configurar un servidor de correo electrónico	Sí					
Catálogo							
	Ver y abrir la pestaña Catálogo	Sí	Sí	Sí	Sí	Sí	Sí
	Ver elementos del catálogo disponibles	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	
	Solicitar un elemento del catálogo	Sí		Sí. Sus proyectos	Sí. Sus proyectos		
Recursos							
	Consultar y abrir la pestaña Recursos	Sí	Sí	Sí.	Sí	Sí	Sí

Tabla 2-4. Funciones de servicio y funciones de proyecto de Service Broker (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Service Broker	Visor de Service Broker	Usuario de Service Broker			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
				El usuario debe ser el administrador del proyecto para ver y realizar tareas relacionadas con el proyecto.			
Implementaciones	Ver implementaciones, incluidos los detalles de la implementación, el historial de implementaciones, el precio, las alertas, y la información de supervisión, optimización y solución de problemas	Sí	Sí	Sí. Sus proyectos	Sí. Sus proyectos	Sí. Sus proyectos	
	Administrar alertas	Sí		Sí. Sus proyectos	Sí. Sus proyectos		
	Ejecutar acciones del día 2 en implementaciones basadas en directivas	Sí		Sí. Sus proyectos	Sí. Sus proyectos		
Recursos: todos los recursos	Ver todos los recursos detectados	Sí	Sí				
	Ejecute acciones del día 2 en recursos detectados. Acciones disponibles solo en máquinas y limitadas al encendido y apagado para todas las máquinas, y la consola remota para máquinas vSphere.	Sí					

Tabla 2-4. Funciones de servicio y funciones de proyecto de Service Broker (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Service Broker	Visor de Service Broker	Usuario de Service Broker			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
				El usuario debe ser el administrador del proyecto para ver y realizar tareas relacionadas con el proyecto.			
Recursos: todos los recursos	Ver recursos implementados, incorporados y migrados	Sí	Sí	Sí. Sus proyectos.	Sí. Sus proyectos.	Sí. Sus proyectos.	
	Ejecutar acciones del día 2 en recursos implementados, incorporados y migrados en función de las directivas	Sí	Sí	Sí. Sus proyectos.	Sí. Sus proyectos.		
Recursos : máquinas virtuales	Ver máquinas detectadas	Sí	Sí				
	Ejecutar acciones del día 2 en máquinas detectadas. Las acciones se limitan al encendido y apagado, y a la consola remota para las máquinas vSphere.	Sí					
	Crear nueva máquina virtual	Sí					
	Ve recursos implementados, incorporados y migrados.	Sí		Sí. Sus proyectos.	Sí. Sus proyectos.	Sí. Sus proyectos.	
	Ejecutar acciones del día 2 en recursos implementados, incorporados y migrados en función de las directivas	Sí		Sí. Sus proyectos.	Sí. Sus proyectos.		

Tabla 2-4. Funciones de servicio y funciones de proyecto de Service Broker (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Service Broker	Visor de Service Broker	Usuario de Service Broker			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
				El usuario debe ser el administrador del proyecto para ver y realizar tareas relacionadas con el proyecto.			
Recursos > Volúmenes	Ver volúmenes detectados	Sí	Sí				
	No hay acciones del día 2 disponibles						
	Ver volúmenes implementados, incorporados y migrados	Sí	Sí	Sí. Sus proyectos.	Sí. Sus proyectos.	Sí. Sus proyectos.	
	Ejecutar acciones del día 2 en volúmenes implementados, incorporados y migrados en función de las directivas	Sí		Sí. Sus proyectos.	Sí. Sus proyectos.		
Recursos: redes y seguridad	Ver redes detectadas, equilibradores de carga y grupos de seguridad	Sí	Sí				
	No hay acciones del día 2 disponibles						
	Ver redes implementadas, incorporadas y migradas, equilibradores de carga y grupos de seguridad	Sí	Sí	Sí. Sus proyectos.	Sí. Sus proyectos.	Sí. Sus proyectos.	

Tabla 2-4. Funciones de servicio y funciones de proyecto de Service Broker (continuación)

Contexto de interfaz de usuario	Tarea	Administrador de Service Broker	Visor de Service Broker	Usuario de Service Broker			
				Administrador del proyecto	Miembro del proyecto	Visor de proyectos	Supervisor de proyectos
				El usuario debe ser el administrador del proyecto para ver y realizar tareas relacionadas con el proyecto.			
	Ejecutar acciones del día 2 en redes implementadas, incorporadas y migradas, equilibradores de carga y grupos de seguridad en función de las directivas	Sí		Sí. Sus proyectos.	Sí. Sus proyectos.		
Aprobaciones							
	Consultar y abrir la pestaña Aprobaciones	Sí	Sí	Sí	Sí	Sí	Sí
	Responder a las solicitudes de aprobación	Sí		Sí. El aprobador de directivas y proyectos es el administrador de proyectos	Solo si es un aprobador designado	Solo si es un aprobador designado	Sí. El aprobador de directivas y proyectos es el supervisor de proyectos

Habilitar aviso del Departamento de Defensa y banner de consentimiento

Para algunos clientes gubernamentales, un administrador debe configurar el aviso estándar del Departamento de Defensa (Department of Defense, DoD) y el banner de consentimiento en Workspace ONE Access para que los usuarios accedan a vRealize Automation.

El texto estándar obligatorio para el aviso del DoD y el banner de consentimiento es el siguiente:

Está accediendo a un sistema de información (Information System, SI) del Gobierno de EE. UU. (U.S. Government, USG) que se proporciona solo para el uso autorizado por el USG. Al usar este SI (que incluye cualquier dispositivo asociado al SI), usted acepta las siguientes condiciones:

- De forma regular, el USG intercepta y supervisa las comunicaciones en este SI para fines de pruebas de penetración, supervisión de COMSEC, operaciones de red y defensa, investigaciones de conductas indebidas en el personal (Personnel Misconduct, PM), de fuerzas policiales (Law Enforcement, LE) y de contrainteligencia (Counterintelligence, CI), entre otros.
- En cualquier momento, el USG puede inspeccionar y confiscar los datos almacenados en el SI.
- Las comunicaciones en las que se utiliza el SI o los datos almacenados en el SI no son privados, están sujetos a tareas de supervisión, interceptación y búsqueda de rutina, y pueden ser divulgados o utilizados con fines autorizados por el USG.

En los siguientes pasos, se describe cómo configurar el banner en Workspace ONE Access. Para obtener más información, consulte la documentación de la consola de administración de Workspace ONE Access.

Procedimiento

- 1 Inicie sesión en la consola de administración de Workspace ONE como administrador.
- 2 En la consola de VMware Identity Manager, haga clic en la pestaña Administración de identidades y acceso.
- 3 Haga clic en Configuración y, a continuación, en la pestaña Conectores.
- 4 Haga clic en el vínculo Trabajador de cada conector que desee configurar.
- 5 Haga clic en la pestaña Adaptadores de autenticación y seleccione `CertificateAuthAdapter`.
- 6 Haga clic en la casilla Habilitar el formulario de consentimiento antes de la autenticación.
- 7 Pegue el texto estándar obligatorio para el aviso del DoD y el banner de consentimiento en el cuadro Contenido del formulario de consentimiento.
- 8 Guarde los cambios.

Resultados

Mantener el dispositivo de vRealize Automation

3

Como administrador del sistema, es posible que deba realizar varias tareas para garantizar el funcionamiento correcto de la aplicación de vRealize Automation instalada.

Si acaba de empezar a utilizar vRealize Automation, estas no son las tareas requeridas. Saber cómo realizar estas tareas resulta útil si necesita resolver problemas de rendimiento o de comportamiento del producto.

Este capítulo incluye los siguientes temas:

- Iniciar y detener vRealize Automation
- Escalar horizontalmente vRealize Automation de uno a tres nodos
- Configurar una regla de antiafinidad y un grupo de máquinas virtuales para una instancia de Workspace ONE Access agrupada en clúster
- Reemplazar un nodo de un dispositivo de vRealize Automation
- Aumentar el espacio de disco del dispositivo de vRealize Automation
- Actualizar la asignación de DNS para vRealize Automation
- Cambiar las direcciones IP de un nodo o un clúster de vRealize Automation
- Cómo habilitar la sincronización de hora de vRealize Automation
- Cómo se restablece la contraseña raíz para vRealize Automation

Iniciar y detener vRealize Automation

Observe los procedimientos adecuados al iniciar o cerrar vRealize Automation.

La forma recomendada de apagar e iniciar los componentes de vRealize Automation es utilizar la funcionalidad APAGAR y ENCENDER que se proporciona en la sección **Operaciones de ciclo de vida > Entornos** de vRealize Suite Lifecycle Manager. Los siguientes procedimientos describen los métodos manuales para apagar e iniciar los componentes de vRealize Automation en caso de que vRealize Suite Lifecycle Manager no esté disponible por alguna razón.

Cerrar vRealize Automation

Para conservar la integridad de los datos, desactive los servicios de vRealize Automation antes de apagar los dispositivos virtuales. Mediante SSH o VMRC, puede apagar o iniciar todos los nodos desde cualquier dispositivo individual.

Nota Si es posible, evite utilizar los comandos `vracli reset vidm`. Este comando restablece todas las configuraciones de Workspace ONE Access e interrumpe la asociación entre los usuarios y los recursos aprovisionados.

- 1 Inicie sesión en la consola de cualquier dispositivo de vRealize Automation mediante SSH o VMRC.
- 2 Para desactivar los servicios de vRealize Automation en todos los nodos del clúster, ejecute el siguiente conjunto de comandos.

Nota Si copia cualquiera de estos comandos para ejecutarlos y se produce un error, péguelos primero en el bloc de notas y, a continuación, cópielos de nuevo antes de ejecutarlos. Este procedimiento elimina los caracteres ocultos y otros artefactos que podrían existir en el origen de la documentación.

```
/opt/scripts/deploy.sh --shutdown
```

- 3 Cierre los dispositivos de vRealize Automation.

La implementación de vRealize Automation está ahora cerrada.

Iniciar vRealize Automation

Después de una desactivación inesperada, una desactivación controlada o un procedimiento de recuperación, los componentes de vRealize Automation se deben reiniciar en un orden específico. vRLCM es un componente no crítico, por lo que se puede iniciar en cualquier momento. Los componentes de VMware Workspace ONE Access, anteriormente conocido como VMware Identity Management, se tienen que iniciar antes de vRealize Automation.

Nota Compruebe que los equilibradores de carga correspondientes se estén ejecutando antes de iniciar los componentes de vRealize Automation.

- 1 Encienda todos los dispositivos de vRealize Automation y espere a que se inicien.
- 2 Inicie sesión en la consola de cualquier dispositivo mediante SSH o VMRC, y ejecute el siguiente comando para restablecer los servicios en todos los nodos.

```
/opt/scripts/deploy.sh
```

- 3 Compruebe que todos los servicios se estén ejecutando con el siguiente comando.

```
kubectl get pods --all-namespaces
```

Nota Debe haber tres instancias de cada servicio con el estado En ejecución o Completado.

vRealize Automation estará listo para usarlo cuando todos los servicios se muestren como En ejecución o Completado.

Reiniciar vRealize Automation

Todos los servicios de vRealize Automation se pueden reiniciar de forma centralizada desde cualquiera de los dispositivos del clúster. Siga las instrucciones anteriores para cerrar vRealize Automation y, a continuación, utilice las instrucciones para iniciar vRealize Automation. Antes de reiniciar vRealize Automation, compruebe que se estén ejecutando todos los componentes de VMware Workspace ONE Access y el equilibrador de carga correspondientes.

vRealize Automation estará listo para usarlo cuando todos los servicios se muestren como En ejecución o Completado.

Ejecute el siguiente comando para comprobar que todos los servicios están en ejecución:

```
kubectl -n prelude get pods
```

Escalar horizontalmente vRealize Automation de uno a tres nodos

A medida que las necesidades aumentan, se puede escalar horizontalmente una implementación de vRealize Automation de uno a tres nodos.

Debe usar funciones de vRealize Suite Lifecycle Manager para completar varios pasos de este procedimiento. Para obtener información sobre cómo trabajar con la instalación, la actualización y la administración de vRealize Suite Lifecycle Manager, consulte la [documentación del producto de Lifecycle Manager](#).

Si utiliza una implementación agrupada en clúster de tres nodos, vRealize Automation puede, por lo general, soportar el error de un nodo y seguir funcionando. El error de dos nodos en un clúster de tres nodos hará que vRealize Automation deje de funcionar.

Requisitos previos

En este procedimiento, se supone que ya existe una implementación de vRealize Automation con un solo nodo en funcionamiento.

Procedimiento

- 1 Apague todos los dispositivos de vRealize Automation.

Para desactivar los servicios de vRealize Automation en todos los nodos del clúster, ejecute el siguiente conjunto de comandos.

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

Ahora puede apagar los dispositivos de vRealize Automation.

- 2 Realice una instantánea de implementación.

Utilice la opción Crear instantánea en vRealize Suite Lifecycle Manager **Operaciones de ciclo de vida > Entornos > vRA > Ver detalles**.

Nota Las instantáneas en línea, que se toman sin cerrar los nodos de vRealize Automation, son compatibles desde la versión 8.0.1. Para los entornos de vRealize Automation 8.0, primero debe detener los nodos de vRealize Automation.

- 3 Encienda el dispositivo de vRealize Automation y ponga en marcha todos los contenedores.
- 4 Mediante la funcionalidad de Locker que se encuentra en **LCM > Locker > Certificados** en vRealize Suite Lifecycle Manager, genere o importe certificados de vRealize Automation para todos los componentes, incluidos los FQDN de los nodos de vRealize Suite Lifecycle Manager y el nombre de dominio completo del equilibrador de carga de vRealize Automation.
Agregue los nombres de los tres dispositivos en los nombres alternativos de asunto.
- 5 Importe el nuevo certificado en vRealize Suite Lifecycle Manager.
- 6 Reemplace el certificado de vRealize Suite Lifecycle Manager existente por el que se generó en el paso anterior con la opción de LCM **Operaciones de ciclo de vida > Entornos > vRA > Ver detalles** Reemplazar certificado.
- 7 Escale horizontalmente vRealize Automation a tres nodos mediante la selección de Agregar componentes en **LCM > Operaciones de ciclo de vida > Entornos > vRA > Ver detalles**.

Resultados

vRealize Automation se ha escalado a una implementación de tres nodos.

Configurar una regla de antiafinidad y un grupo de máquinas virtuales para una instancia de Workspace ONE Access agrupada en clúster

Si el entorno de vRealize Automation utiliza una instancia de Workspace ONE Access agrupada en clúster, cree una regla de antiafinidad y un clúster de máquinas para garantizar un correcto flujo de trabajo de vSphere de alta disponibilidad.

Para proteger los nodos agrupados en clúster de Workspace ONE Access de un error en el nivel del host, configure una regla de antiafinidad para ejecutar las máquinas virtuales que existen en diferentes hosts del clúster de administración de vSphere predeterminado. Después de crear una regla de antiafinidad, configure un grupo de máquinas virtuales para definir el orden de inicio de la máquina deseado. Al utilizar un orden de inicio de máquina definido, puede asegurarse de que vSphere High Availability encienda los nodos de Workspace ONE Access agrupados en clúster en el orden correcto para su entorno.

Para obtener información sobre cómo configurar reglas de antiafinidad y un grupo de máquinas virtuales, consulte [Configurar una regla de antiafinidad y un grupo de máquinas virtuales para la instancia de Workspace ONE Access agrupada en clúster](#) en la documentación del producto de VMware Cloud Foundation.

Consideraciones sobre reglas de afinidad al actualizar de una versión de vRealize Automation a otra

vRealize Suite Lifecycle Manager no admite reglas de antiafinidad para vRealize Automation 8.x. Debido a que vRealize Easy Installer utiliza vRealize Suite Lifecycle Manager durante la actualización de vRealize Automation y no hay ningún orden específico de apagado y encendido de los nodos de vRealize Automation durante la actualización, pueden producirse problemas si el orden utilizado entra en conflicto con las reglas de afinidad que definen el orden en el que se apagan y se encienden las máquinas. Cuando utilice vRealize Suite Lifecycle Manager o vRealize Easy Installer para actualizar de una versión de vRealize Automation a otra, deshabilite las reglas de afinidad antes de iniciar la actualización.

Para obtener información sobre cómo actualizar de una versión de vRealize Automation a otra, consulte [Instalar vRealize Automation con vRealize Easy Installer](#) en la [documentación del producto de vRealize Automation](#).

Reemplazar un nodo de un dispositivo de vRealize Automation

Cuando se produce un error en un dispositivo de vRealize Automation en una configuración de alta disponibilidad (HA) de varios nodos, es posible que deba reemplazar el nodo defectuoso.

Precaución Antes de continuar, VMware recomienda ponerse en contacto con el equipo de soporte técnico para solucionar el problema de HA y comprobar que el problema esté aislado en un nodo.

Si el soporte técnico determina que necesita reemplazar el nodo, siga estos pasos.

- 1 En vCenter, realice instantáneas de copia de seguridad de cada dispositivo en la configuración de HA.
En las instantáneas de copia de seguridad, no incluya la memoria de la máquina virtual.
- 2 Apague el nodo defectuoso.

- 3 Tome nota del número de compilación de software de vRealize Automation y la configuración de red del nodo defectuoso.

Anote el FQDN, la dirección IP, la puerta de enlace, los servidores DNS y, especialmente, la dirección MAC. Posteriormente, asigne los mismos valores al nodo de reemplazo.

- 4 El nodo de base de datos principal debe ser uno de los nodos en buen estado. Siga estos pasos:

- a Inicie sesión como raíz en la línea de comandos de un nodo en buen estado.
- b Busque el nombre del nodo de base de datos principal mediante la ejecución del siguiente comando.

```
vracli status | grep primary -B 1
```

El resultado debe ser similar a este ejemplo, donde postgres-1 es el nodo de base de datos principal.

```
"Conninfo":
"host=postgres-1.postgres.prelude.svc.cluster.local
dbname=repmgr-db user=repmgr-db passfile=/scratch/repmgr-db.cred
connect_timeout=10",
"Role": "primary",
```

- c Verifique que el nodo de la base de datos principal esté en buen estado mediante la ejecución del siguiente comando.

```
kubectl -n prelude get pods -o wide | grep postgres
```

El resultado debe ser similar a este ejemplo, donde postgres-1 se encuentra en la lista como en ejecución y en buen estado.

```
postgres-1 1/1 Running 0 39h 12.123.2.14 vc-vm-224-84.company.com <none> <none>
postgres-2 1/1 Running 0 39h 12.123.1.14 vc-vm-224-85.company.com <none> <none>
```

Importante Si el nodo de base de datos principal es defectuoso, póngase en contacto con el soporte técnico en lugar de continuar.

- 5 En la línea de comandos raíz del nodo en buen estado, elimine el nodo defectuoso.

```
vracli cluster remove faulty-node-FQDN
```

- 6 Utilice vCenter para implementar un nuevo nodo de vRealize Automation de reemplazo.

Implemente el mismo número de compilación de software de vRealize Automation y aplique la configuración de red del nodo defectuoso. Incluya el FQDN, la dirección IP, la puerta de enlace, los servidores DNS y, especialmente, la dirección MAC que anotó anteriormente.

- 7 Encienda el nodo de reemplazo.
- 8 Inicie sesión como raíz en la línea de comandos del nodo de reemplazo.

- 9 Compruebe que la secuencia de arranque inicial haya finalizado mediante la ejecución del siguiente comando.

```
vracli status first-boot
```

Busque un mensaje de `First boot complete` nuevo.

- 10 Desde el nodo de reemplazo, únase al clúster de vRealize Automation de reemplazo.

```
vracli cluster join primary-DB-node-FQDN
```

- 11 Inicie sesión como raíz en la línea de comandos del nodo de base de datos principal.

- 12 Implemente el clúster reparado mediante la ejecución del siguiente script.

```
/opt/scripts/deploy.sh
```

Aumentar el espacio de disco del dispositivo de vRealize Automation

Es posible que necesite aumentar el espacio de disco del dispositivo de vRealize Automation para ciertos fines, como el almacenamiento de archivos de log.

Procedimiento

- 1 Utilice vSphere para expandir el VMDK en el dispositivo de vRealize Automation.
- 2 Inicie sesión en la línea de comandos del dispositivo de vRealize Automation como usuario raíz.
- 3 En el símbolo del sistema, ejecute el siguiente comando de vRealize Automation:

```
vracli disk-mgr resize
```

Si se generan errores al cambiar el tamaño de vRealize Automation, consulte el [artículo 79925 de la base de conocimientos](#).

Actualizar la asignación de DNS para vRealize Automation

Un administrador puede actualizar las asignaciones de DNS para vRealize Automation.

Procedimiento

- 1 Inicie sesión en la consola de cualquier dispositivo de vRealize Automation mediante SSH o VMRC.
- 2 Ejecute el siguiente comando.

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

- 3 Compruebe que los nuevos servidores DNS se aplicaron correctamente a todos los nodos de vRealize Automation con el comando `vracli network dns status`.

- 4 Ejecute el siguiente conjunto de comandos para cerrar los servicios de vRealize Automation en todos los nodos del clúster.

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

- 5 Reinicie los nodos de vRealize Automation y espere a que se inicien por completo.
- 6 Inicie sesión en cada nodo de vRealize Automation con SSH y compruebe que los nuevos servidores DNS aparezcan en `/etc/resolv.conf`.
- 7 En uno de los nodos de vRealize Automation, ejecute el siguiente comando para iniciar los servicios de vRealize Automation: `/opt/scripts/deploy.sh`

Resultados

La configuración de DNS de vRealize Automation se cambiará según lo especificado.

Cambiar las direcciones IP de un nodo o un clúster de vRealize Automation

Puede cambiar la dirección IP de un nodo o un clúster de vRealize Automation.

Por ejemplo, es posible que desee migrar el entorno de vRealize Automation implementado a una instancia de vCenter más conveniente o admitir la conmutación por error de vRealize Automation.

Como administrador de vRealize Automation, puede utilizar el siguiente procedimiento para establecer una nueva dirección IP para el nodo o el clúster de vRealize Automation y, a continuación, volver a implementar los servicios en la nueva dirección IP.

Nota Antes de continuar con el cambio de la dirección IP de un nodo o un clúster de vRealize Automation, debe comprobar que el nodo o el clúster se encuentren en buen estado. Si se intenta ejecutar este procedimiento en un nodo o clúster que no se encuentra en buen estado, pueden surgir problemas muy difíciles de resolver.

En este procedimiento, reiniciará vRealize Automation de forma específica y secuencial. Para obtener información relacionada con el apagado y el reinicio de vRealize Automation, consulte [Iniciar y detener vRealize Automation](#).

- 1 Compruebe que el nodo o el clúster de vRealize Automation se encuentra en buen estado mediante el siguiente comando.

```
vracli service status
```

- 2 Cuando vRealize Automation esté en buen estado, establezca la dirección IP alternativa de los dispositivos del nodo o del clúster mediante el siguiente comando.

```
vracli network alternative-ip set --dns DNSIPaddress1,DNSIPaddress2 IPV4_address
Gateway_IPV4_address
```

Si trabaja con un clúster de, establezca la dirección IP alternativa de cada nodo correspondiente en el clúster.

- 3 Apague los servicios mediante el siguiente comando.

```
/opt/scripts/deploy.sh -shutdown
```

- 4 Si es necesario, realice una operación de conmutación por error o de migración de vRealize Automation. Consulte la información sobre [VMware Site Recovery Manager](#) y sus propios procedimientos y prácticas internos.

- 5 Cambie la dirección IP de vRealize Automation mediante el siguiente comando.

```
vracli network alternative-ip swap
```

Si utiliza un clúster de vRealize Automation, debe cambiar la dirección IP de cada nodo del clúster.

- 6 Reinicie vRealize Automation mediante el siguiente comando.

```
shutdown -r now
```

Si utiliza un clúster de vRealize Automation, debe reiniciar cada nodo del clúster.

- 7 Vuelva a implementar los servicios de vRealize Automation mediante el siguiente comando.

```
/opt/scripts/deploy.sh
```

Después de reiniciar vRealize Automation, y una vez que los servicios reimplementados estén en ejecución, vRealize Automation debería estar disponible en la nueva dirección IP.

Cómo habilitar la sincronización de hora de vRealize Automation

Puede habilitar la sincronización de hora en la implementación de vRealize Automation con la línea de comandos del dispositivo de vRealize Automation.

Puede configurar la sincronización de hora para la implementación de vRealize Automation independiente o agrupada en clúster mediante el protocolo de tiempo de redes (Network Time Protocol, NTP). vRealize Automation admite dos configuraciones de NTP mutuamente excluyentes:

Configuración de NTP	Descripción
ESXi	<p>Esta configuración puede utilizarse cuando el servidor de ESXi que aloja vRealize Automation está sincronizado con un servidor NTP. Si utiliza una implementación agrupada en clúster, todos los hosts ESXi deben estar sincronizados con un servidor NTP. Si desea obtener más información sobre la configuración de NTP para ESXi, consulte el artículo 57147 de la base de conocimientos Configurar el protocolo de tiempo de redes (NTP) en un host ESXi mediante vSphere Web Client.</p> <p>Nota Puede experimentar un desplazamiento del reloj si la implementación de vRealize Automation se migra a un host ESXi que no está sincronizado con un servidor NTP.</p>
systemd	<p>Esta configuración utiliza el daemon de systemd-timesyncd para sincronizar los relojes de la implementación de vRealize Automation.</p> <p>Nota De forma predeterminada, el daemon de systemd-timesyncd está habilitado, pero no tiene servidores NTP configurados. Si el dispositivo de vRealize Automation utiliza una configuración de IP dinámica, el dispositivo puede utilizar cualquier servidor NTP que reciba el protocolo DHCP.</p>

Procedimiento

- 1 Inicie sesión en la línea de comandos del dispositivo de vRealize Automation como **raíz**.
- 2 Habilite NTP con ESXi.

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

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

- 3 Habilite NTP con systemd.

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

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

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

Resultados

Habilitó la sincronización de hora para la implementación del dispositivo de vRealize Automation.

Pasos siguientes

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

Cómo se restablece la contraseña raíz para vRealize Automation

Puede restablecer una contraseña raíz perdida u olvidada de vRealize Automation.

En este procedimiento, se utiliza una ventana de línea de comandos en el dispositivo de vCenter del host para restablecer la contraseña raíz de vRealize Automation de la organización.

Requisitos previos

Este proceso es para los administradores de vRealize Automation y requiere las credenciales necesarias para acceder al dispositivo de vCenter del host.

Procedimiento

- 1 Apague e inicie vRealize Automation mediante el procedimiento descrito en [Iniciar y detener vRealize Automation](#).
- 2 Cuando aparezca la ventana de la línea de comandos del sistema operativo Photon, introduzca `e` y pulse la tecla **Intro** para abrir el editor del menú de arranque de GNU GRUB.
- 3 En el editor de GNU GRUB, introduzca `rw init=/bin/bash` al final de la línea que comienza con `linux "/" $photon_linux root=rootpartition` como se muestra a continuación:

```

vcenter
GNU GRUB version 2.02~beta2

setparams 'Photon'

linux "/"$photon_linux root=$rootpartition net_ifnames=0 $photon_cmd\
line coredump_filter=0x37 consoleblank=0 rw init=/bin/bash_
if [ "$photon_initrd" ]; then
  initrd "/"$photon_initrd
fi

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.

```

- 4 Pulse la tecla **F10** para insertar el cambio y reinicie vRealize Automation.

- 5 Espere a que vRealize Automation se reinicie.
- 6 En la solicitud `root [/]#`, introduzca `passwd` y pulse la tecla **Intro**.
- 7 En la solicitud `New password:`, introduzca la nueva contraseña y pulse la tecla **Intro**.
- 8 En la solicitud `Retype new password:`, vuelva a introducir la nueva contraseña y pulse la tecla **Intro**.
- 9 En la solicitud `root [/]#`, introduzca `reboot -f` y pulse la tecla **Intro** para completar el proceso de restablecimiento de la contraseña raíz.

```
root [ / ]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [ / ]# reboot -f_
```

Pasos siguientes

Como administrador de vRealize Automation, ahora puede iniciar sesión en vRealize Automation con la nueva contraseña raíz.

Usar configuraciones de tenant de varias organizaciones en vRealize Automation

4

vRealize Automation permite que los proveedores de TI configuren varios tenants u organizaciones dentro de cada implementación. Los proveedores pueden configurar organizaciones de varios tenants y asignar infraestructuras dentro de cada implementación. Los proveedores también pueden administrar usuarios para los tenants. Cada tenant administra sus propios proyectos, recursos e implementaciones.

En una configuración de vRealize Automation de varias organizaciones, los proveedores pueden crear varias organizaciones, y la organización de cada tenant utiliza sus propios proyectos, recursos e implementaciones. Si bien los proveedores no pueden administrar la infraestructura de tenant de forma remota, pueden iniciar sesión en los tenants y administrar la infraestructura dentro de ellos.

La estructura de varios tenants se basa en la coordinación y la configuración de tres productos VMware diferentes, como se describe a continuación:

- **Workspace ONE Access:** este producto proporciona compatibilidad de infraestructura para conexiones de dominio de varios tenants y de Active Directory que proporcionan administración de usuarios y grupos dentro de las organizaciones de tenants.
- **vRealize Suite Lifecycle Manager:** este producto admite la creación y configuración de tenants para productos compatibles, como vRealize Automation. Además, proporciona algunas capacidades de administración de certificados.
- **vRealize Automation:** los proveedores y los usuarios inician sesión en vRealize Automation para acceder a los tenants en los que crean y administran las implementaciones.

Al configurar varios tenants, los usuarios deben estar familiarizados con los tres productos y la documentación asociada.

Para obtener más información sobre cómo trabajar con vRealize Suite Lifecycle Manager y Workspace ONE Access, consulte lo siguiente.

- **vRealize Suite Lifecycle Manager:** consulte [documentación del producto Lifecycle Manager](#)
- **Workspace ONE Access:** consulte [Administración de usuarios con VMware Identity Manager y Administración de VMware Workspace ONE Access](#)

Los administradores con privilegios de vRealize Suite Lifecycle Manager crean y administran tenants mediante la página de tenants de Lifecycle Manager que se encuentra en el servicio de administración de identidades y tenants. Los tenants se construyen mediante una conexión LDAP o IWA de Active Directory, y son compatibles con la instancia de VMware Workspace ONE Access asociada que se requiere para las implementaciones de vRealize Automation. Consulte la documentación asociada para obtener información sobre el uso de Lifecycle Manager.

Al configurar varios tenants, empiece con un tenant de base o principal. Este es el tenant predeterminado que se crea al implementar la aplicación Workspace ONE Access subyacente. Otros tenants, conocidos como subtenants, pueden basarse en el tenant principal. Actualmente, vRealize Automation admite hasta 20 organizaciones de tenants con la implementación estándar de tres nodos.

Antes de habilitar vRealize Automation para varios tenants, primero debe instalar la aplicación en la configuración de una sola organización y, a continuación, utilizar Lifecycle Manager para establecer una configuración de varias organizaciones. Una implementación de Workspace ONE Access es compatible con la administración de tenants y las conexiones de dominio de Active Directory asociadas.

Cuando inicialmente configura varios tenants, se designa un administrador de proveedores en Lifecycle Manager. Puede cambiar esta designación o agregar administradores más adelante, si lo desea. En las configuraciones de varias organizaciones, los usuarios y los grupos de vRealize Automation se administran principalmente a través de Workspace ONE Access.

Después de que se creen las organizaciones, los usuarios autorizados podrán iniciar sesión en sus aplicaciones para crear o trabajar con proyectos y recursos, y crear implementaciones. Los administradores pueden administrar las funciones de usuario en vRealize Automation.

Establecer una configuración de varias organizaciones

Puede habilitar una implementación de varias organizaciones después de completar la instalación de vRealize Automation. Al definir los ajustes para una configuración de varias organizaciones, debe configurar la instancia de Workspace ONE Access externa para el uso de varios tenants y, a continuación, utilizar Lifecycle Manager para crear y configurar tenants. Esto se aplica tanto a las implementaciones nuevas como a las existentes. Como paso inicial para configurar los tenants, debe usar Lifecycle Manager para definir un alias para el tenant principal que se creó de forma predeterminada en Workspace ONE Access. Los subtenants que se crean a partir de este tenant principal heredan las configuraciones de dominio de Active Directory de este.

En Lifecycle Manager, los tenants se asignan a un producto, como vRealize Automation, y a un entorno específico. Cuando se configura un tenant, también se debe designar un administrador de tenants. De forma predeterminada, la configuración para varios tenants está habilitada en función del nombre de host del tenant. Los usuarios pueden optar por configurar manualmente el nombre de tenant por nombre de DNS. Durante este procedimiento, debe establecer varias marcas para admitir varios tenants y también debe configurar el equilibrador de carga.

Si utiliza una instancia agrupada en clúster, ambos nombres de host basados en tenant de Workspace ONE Access y vRealize Automation apuntarán al equilibrador de carga.

Si la instancia de Workspace ONE Access agrupada en clúster y los equilibradores de carga de vRealize Automation no utilizan certificados comodín, los usuarios deben agregar nombres de host de tenant como entradas de SAN en los certificados. Para cada tenant nuevo que se crea.

No puede eliminar los tenants en vRealize Automation ni en Lifecycle Manager. Si necesita agregar tenants a una implementación de varios tenants existente, puede hacerlo con Lifecycle Manager, pero necesitará un periodo de inactividad de entre tres y cuatro horas.

Consulte los vínculos de la documentación al principio de este tema para obtener más información sobre el uso de vRealize Suite Lifecycle Manager Workspace ONE Access.

Nombres de host y varios tenants

En versiones anteriores de vRealize Automation, los usuarios accedían a los tenants con URL basadas en la ruta de acceso del directorio. En la implementación de varios tenants actual, los usuarios acceden a los tenants en función del nombre de host.

Asimismo, el formato de nombre de host que utilizarán los usuarios de vRealize Automation para acceder a los tenants es diferente del formato que se utiliza para acceder a los tenants en Workspace ONE Access. Por ejemplo, un nombre de host válido tendría el siguiente aspecto:

`tenant1.example.eng.vmware.com` en lugar de `vidm-node1.eng.vmware.com`.

Configuración para varios tenants y certificados

Debe crear certificados para todos los componentes que participan en una configuración de varias organizaciones. Necesitará uno o más certificados para Workspace ONE Access, Lifecycle Manager y vRealize Automation, según se utilice una configuración de un solo nodo o una configuración agrupada en clúster.

Cuando se configuran certificados, se pueden utilizar comodines con nombres de SAN o nombres dedicados. El uso de comodines simplificará la administración de certificados, ya que estos deben actualizarse cuando se agregan nuevos tenants. Si su equilibrador de carga de Workspace ONE Access y vRealize Automation no utilizan certificados comodín, debe agregar nombres de host de tenant como entradas de SAN en los certificados para cada nuevo tenant que se crea. Además, si utiliza SAN, los certificados deben actualizarse manualmente si agrega o elimina hosts, o si cambia un nombre de host. También debe actualizar las entradas de DNS para los tenants.

Tenga en cuenta que Lifecycle Manager no crea certificados independientes para cada tenant. En su lugar, crea un único certificado con cada nombre de host del tenant que aparece en la lista. Para las configuraciones básicas, el CNAME del tenant utiliza el siguiente formato: `tenantname.vrahostname.domain`. Para las configuraciones de alta disponibilidad, el nombre utiliza el siguiente formato: `tenantname.vraLBhostname.dominio`.

Si utiliza una configuración de Workspace ONE Access agrupada en clúster, tenga en cuenta que Lifecycle Manager no puede actualizar el certificado del equilibrador de carga, por lo que debe actualizarlo manualmente. Además, si necesita volver a registrar productos o servicios que son externos a Lifecycle Manager, debe hacerlo de forma manual.

Este capítulo incluye los siguientes temas:

- [Configurar tenants de varias organizaciones para vRealize Automation](#)
- [Iniciar sesión en tenants y agregar usuarios en vRealize Automation](#)
- [Usar vRealize Orchestrator con implementaciones de varias organizaciones de vRealize Automation](#)

Configurar tenants de varias organizaciones para vRealize Automation

Puede configurar tenants de varias organizaciones para vRealize Automation mediante vRealize Suite Lifecycle Manager.

A continuación se muestra una descripción de alto nivel del procedimiento que permite configurar varios tenants para vRealize Automation, incluida la configuración de DNS y certificados. Se enfoca en una implementación de un solo nodo, pero incluye notas para una configuración agrupada en clúster.

Consulte <https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/> para obtener más información y una demostración en video sobre cómo establecer una configuración de varias organizaciones en vRealize Automation.

Requisitos previos

- Instale y configure la versión 3.3.4 o posterior de Workspace ONE Access.
- Instale y configure la versión 8.5 de vRealize Suite Lifecycle Manager

Procedimiento

- 1 Cree los registros de DNS de tipo A y CNAME requeridos.
 - Para el tenant principal y cada subtenant, debe crear y aplicar un certificado de SAN.
 - Para implementaciones de un solo nodo, el FQDN de vRealize Automation apunta al dispositivo de vRealize Automation y el FQDN de Workspace ONE Access apunta al dispositivo de Workspace ONE Access.
 - Para implementaciones agrupadas en clúster, los FQDN basados en tenants de Workspace ONE Access y de vRealize Automation deben apuntar a sus respectivos equilibradores de carga. Workspace ONE Access está configurado con terminación SSL, de modo que el certificado se aplica en el clúster y en el equilibrador de carga de Workspace ONE Access. El equilibrador de carga de vRealize Automation utiliza el acceso directo a SSL, de modo que el certificado se aplica solo en el clúster de vRealize Automation.

Para obtener más información, consulte [Administrar certificados y la configuración de DNS en implementaciones de varias organizaciones de un solo nodo](#) y [Administrar la configuración de certificados y DNS en implementaciones de vRealize Automation agrupadas en clúster](#).

- 2 Cree o importe los certificados de varios dominios (SAN) necesarios para Workspace ONE Access y vRealize Automation.

Puede crear certificados en Lifecycle Manager mediante el servicio de almacén que le permite crear contraseñas y licencias de certificados. Si lo prefiere, puede utilizar un servidor de CA o algún otro mecanismo para generar certificados.

Si necesita agregar o crear tenants adicionales, debe volver a crear y aplicar los tenants de vRealize Automation y Workspace ONE Access.

Después de crear los certificados, puede aplicarlos en Lifecycle Manager mediante la función Operaciones de ciclo de vida. Debe seleccionar el entorno y el producto, y luego la opción Reemplazar certificado en el menú de la derecha. A continuación, puede seleccionar el producto. Al reemplazar un certificado, debe volver a confiar en todos los productos asociados de su entorno.

Debe esperar a que se aplique el certificado y que todos los servicios se reinicien antes de continuar con el siguiente paso.

Para obtener más información, consulte [Administrar certificados y la configuración de DNS en implementaciones de varias organizaciones de un solo nodo](#) y [Administrar la configuración de certificados y DNS en implementaciones de vRealize Automation agrupadas en clúster](#).

- 3 Aplique el certificado de SAN de Workspace ONE Access en el clúster o la instancia de Workspace ONE Access.

- 4 En vRealize Suite Lifecycle Manager, ejecute el asistente de habilitación de tenants a fin de habilitar varios tenants y crear un alias para el tenant principal predeterminado.

Para habilitar el tenant, es necesario crear un alias para el tenant principal o el tenant predeterminado de la organización del proveedor. Después de habilitar la tenant, puede acceder a Workspace ONE Access a través del FQDN del tenant principal.

Por ejemplo, si el FQDN de Workspace ONE Access existente es `idm.example.local` y crea un alias de tenant predeterminado, una vez habilitado el tenant, el FQDN de Workspace ONE Access cambia a `default-tenant.example.local` y todos los clientes que se comunican con Workspace ONE Access ahora lo hacen a través de `default-tenant.example.local`.

- 5 Aplique los certificados de SAN de vRealize Automation en el clúster o la instancia de vRealize Automation.

Puede aplicar certificados de SAN a través del servicio de Operaciones de ciclo de vida de Lifecycle Manager. Debe ver los detalles del entorno y, a continuación, seleccionar Reemplazar certificados en el menú de la derecha. Antes de agregar tenants, debe esperar a que se complete la tarea de reemplazo de certificados. Como parte del reemplazo de certificados, se reiniciarán los servicios de vRealize Automation.

- 6 En Lifecycle Manager, ejecute el asistente Agregar tenants para configurar los tenants deseados.

Los tenants se agregan mediante la página Administración de tenants de Lifecycle Manager que se encuentra en Administración de identidades y tenants. Solo puede agregar tenants para los que configuró previamente certificados y los ajustes de DNS.

Al crear un tenant, debe designar un administrador de tenants y puede seleccionar las conexiones de Active Directory de este tenant. Las conexiones disponibles se basan en las que están configuradas en el tenant predeterminado o principal. También debe seleccionar el producto o la instancia de producto a los que se asociará el tenant.

Pasos siguientes

Después de crear tenants, puede utilizar la página de administración de tenants de Lifecycle Manager que se encuentra en Administración de identidades y tenants para cambiar o agregar administradores de tenants, agregar directorios de Active Directory al tenant y cambiar las asociaciones de producto para el tenant.

También puede iniciar sesión en la instancia de Workspace ONE Access para ver y validar la configuración de tenants.

Administrar certificados y la configuración de DNS en implementaciones de varias organizaciones de un solo nodo

Las configuraciones de vRealize Automation para tenants de varias organizaciones se basan en la configuración coordinada entre varios productos. Debe garantizarse que los ajustes de DNS y los certificados estén establecidos correctamente para que la configuración de tenants de varias organizaciones funcione.

Esta configuración de varias organizaciones asume implementaciones de un solo nodo para los siguientes componentes:

- Lifecycle Manager
- Workspace ONE Access Identity Manager
- vRealize Automation

Además, se da por sentado que se empieza con un tenant predeterminado, que es la organización del proveedor, y que se crean dos subtenants, denominados tenant-1 y tenant-2.

Puede crear y aplicar certificados mediante el servicio de Locker en vRealize Suite Lifecycle Manager o puede utilizar otro mecanismo. Lifecycle Manager también permite reemplazar o volver a confiar en los certificados de vRealize Automation o Workspace ONE Access.

Requisitos de DNS

Debe crear registros de tipo A principal y de tipo CNAME para los componentes del sistema, tal como se describe a continuación.

- Cree ambos registros de tipo A principales para cada componente y para cada uno de los tenants que creará cuando habilite la configuración de varios tenants.
- Cree registros de tipo A de varios tenants para cada uno de los tenants que creará y para el tenant principal.
- Cree registros de tipo CNAME de varios tenants para cada uno de los tenants que creará, sin contar el tenant principal.

Requisitos de certificados para la implementación de varios tenants de nodo único

Debe crear dos certificados de nombre alternativo de asunto (Subject Alternative Name, SAN), uno para Workspace ONE Access y otro para vRealize Automation.

- El certificado de vRealize Automation muestra el nombre de host del servidor de vRealize Automation y los nombres de los tenants que creará.
- El certificado de Workspace ONE Access muestra el nombre de host del servidor de Workspace ONE Access y los nombres de tenants que está creando.
- Si utiliza nombres de SAN dedicados, los certificados deben actualizarse manualmente al agregar o eliminar hosts, o si cambia un nombre de host. También debe actualizar las entradas de DNS para los tenants. Para simplificar la configuración, puede utilizar comodines para los certificados de Workspace ONE Access y de vRealize Automation. Por ejemplo, `*.example.com` y `*.vra.example.com`.

Nota vRealize Automation 8.x solo admite certificados comodín para nombres DNS que coincidan con las especificaciones de la lista de sufijos públicos en <https://publicsuffix.org>. Por ejemplo, `*.myorg.com` es un nombre válido, mientras que `*.myorg.local` no lo es.

Tenga en cuenta que Lifecycle Manager no crea certificados independientes para cada tenant. En su lugar, crea un único certificado con cada nombre de host del tenant que aparece en la lista. Para las configuraciones básicas, el CNAME del tenant utiliza el siguiente formato: `tenantname.vrahostname.dominio`. Para las configuraciones de alta disponibilidad, el nombre utiliza el siguiente formato: `tenantname.vraLBhostname.dominio`.

Resumen

En la siguiente tabla, se resumen los requisitos de DNS y certificados para una instancia de Workspace ONE Access de un solo nodo y una implementación de vRealize Automation de un solo nodo.

Requisitos de DNS	Requisitos del certificado de SAN
Main A Type Records lcm.example.local WorkspaceOne.example.local vra.example.local	Workspace One Certificate Nombre de host: WorkspaceOne.example.local, default-tenant.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local
Multi-tenancy A Type Records default-tenant.example.local tenant-1.example.local tenant-2.example.local	
Multi-Tenancy CNAME Type Records tenant-1.vra.example.local tenant-2.vra.example.local	vRealize Automation Certificate Nombre de host: vra.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local

Administrar la configuración de certificados y DNS en implementaciones de vRealize Automation agrupadas en clúster

Debe coordinar la configuración de certificados y DNS entre todos los componentes aplicables a fin de configurar una implementación de vRealize Automation agrupada en clúster para varias organizaciones.

En una configuración agrupada en clúster típica, hay tres dispositivos de Workspace ONE Access y tres dispositivos de vRealize Automation, así como un solo dispositivo de Lifecycle Manager.

Esta configuración asume implementaciones agrupadas en clúster para los siguientes componentes:

- Dispositivos de Workspace ONE Access Identity Manager:
 - idm1.example.local
 - idm2.example.local
 - idm3.example.local
 - idm-lb.example.local
- Dispositivos de vRealize Automation:
 - vra-1.example.local
 - vra-2.example.local
 - vra-3.example.local
 - vra-lb.example.local
- Dispositivo de Lifecycle Manager

Requisitos de DNS

Debe crear ambos registros de tipo A principales para cada componente y para cada uno de los tenants que creará cuando habilite la configuración para varios tenants. Asimismo, debe crear registros de tipo CNAME de varios tenants para cada uno de los tenants que creará, sin contar el tenant principal. Por último, también debe crear registros de tipo A principales para los equilibradores de carga de Workspace ONE Access y vRealize Automation.

- Cree registros de tipo A para los tres dispositivos de Workspace ONE Access y para los dispositivos de vRealize Automation que apunten a sus respectivos FQDN.
- Además, cree registros de tipo A para el equilibrador de carga de Workspace ONE Access y el equilibrador de carga de vRealize Automation que apunten a sus respectivos FQDN.
- Cree registros de tipo A de varios tenants para el tenant predeterminado y para los tenant-1 y tenant-2 que apunten a la dirección IP del equilibrador de carga de Workspace ONE Access.
- Cree registros CNAME para los tenant-1 y tenant-2 que apuntan a la dirección IP del equilibrador de carga de vRealize Automation.

Requisitos de los certificados de nombre alternativo de asunto (SAN)

Debe crear dos certificados de Workspace ONE Access, uno que se aplique a los dispositivos del clúster y otro que se aplique al equilibrador de carga. Además, cree un certificado que se aplique a los dispositivos de vRealize Automation, a los tenants que va a crear (excluyendo el tenant predeterminado) y al equilibrador de carga.

- Cree un certificado para los dispositivos de Workspace ONE Access que muestren los FQDN de los dispositivos de Workspace ONE Access, así como el tenant predeterminado y otros tenants que cree. Este certificado debe incluir las direcciones IP de los dispositivos de Workspace ONE Access.
- Se recomienda crear una terminación SSL en el equilibrador de carga. Si desea admitir esta terminación, cree un certificado para el equilibrador de carga de Workspace ONE Access que enumere los FQDN del equilibrador de carga de Workspace ONE Access, así como el tenant predeterminado y todos los demás tenants que cree. Este certificado debe incluir la dirección IP del equilibrador de carga.
- Debe crear un certificado para vRealize Automation que enumere los nombres de host de los tres dispositivos de vRealize Automation, así como el equilibrador de carga relacionado y los tenants que esté creando. Además, debería enumerar las direcciones IP de los tres dispositivos de vRealize Automation.
- Para simplificar la configuración, puede utilizar comodines para los certificados de Workspace ONE Access y de vRealize Automation. Por ejemplo, `*.example.com`, `*.vra.example.com` y `*.vra-lb.example.com`.

Nota vRealize Automation 8.x solo admite certificados comodín para nombres DNS que coincidan con las especificaciones de la lista de sufijos públicos en <https://publicsuffix.org>. Por ejemplo, `*.myorg.com` es un nombre válido, mientras que `*.myorg.local` no lo es.

Si utiliza una configuración de Workspace ONE Access agrupada en clúster, tenga en cuenta que Lifecycle Manager no puede actualizar los certificados del equilibrador de carga, por lo que debe actualizarlos manualmente. Además, si necesita volver a registrar productos o servicios que son externos a Lifecycle Manager, debe hacerlo de forma manual.

Resumen de las entradas de DNS y los certificados para una configuración de varias organizaciones agrupada en clúster

En las siguientes tablas, se describen los registros de tipo A principales de DNS y los registros de tipo de nombre C, así como los requisitos de certificados para una implementación de varias organizaciones de una instancia de Workspace ONE Access agrupada en clúster y una instancia de vRealize Automation agrupada en clúster.

Requisitos de DNS	Requisitos del certificado de SAN
<p>Main A Type Records</p> <ul style="list-style-type: none"> ■ lcm.example.local ■ WorkspaceOne-1.example.local ■ WorkspaceOne-2.example.local ■ WorkspaceOne-3.example.local ■ WorkspaceOne-lb.example.local ■ vra-1.example.local ■ vra-2.example.local ■ vra-3.example.local ■ vra-lb.example.local 	<p>Workspace One Certificate</p> <p>Nombre de host:</p> <ul style="list-style-type: none"> ■ WorkspaceOne-1.example.local ■ WorkspaceOne-2.example.local ■ WorkspaceOne-3.example.local ■ default-tenant.example.local ■ tenant-1.example.local ■ tenant-2.example.local
<p>Multi-Tenancy A Type Records</p> <ul style="list-style-type: none"> ■ default-tenant.example.local ■ tenant-1.vra.example.local ■ tenant-2.vra.example.local <p>Nota Todos los registros de tipo A de varios tenants deben apuntar a la dirección IP del equilibrador de carga de vIDM/WS1A.</p>	<p>Workspace One LB Certificate (LB Terminated)</p> <p>Nombre de host:</p> <ul style="list-style-type: none"> ■ WorkspaceOne-lb.example.local ■ default-tenant.example.local ■ tenant-1.example.local ■ tenant-2.example.local
<p>Multi-Tenancy CNAME Type Records</p> <ul style="list-style-type: none"> ■ tenant-1.vra-lb.example.local - vra-lb.example.local ■ tenant-2.vra-lb.example.local - vra-lb.example.local 	<p>vRealize Automation Certificate</p> <p>Nombre de host:</p> <ul style="list-style-type: none"> ■ vra-1.example.local ■ vra-2.example.local ■ vra-3.example.local ■ vra-lb.example.local ■ tenant-1.example.local ■ tenant-2.example.local <p>No se requiere ningún certificado en el equilibrador de carga vRealize Automation, ya que utiliza el acceso directo a SSL.</p>

Nota Cada tenant adicional que agregue debe aparecer por separado en el certificado de vRealize Automation, los registros CNAME de varios tenants, los registros de tipo A de varios tenants, el certificado de Workspace ONE y el certificado de Workspace ONE LB.

Nota Los nombres de archivo *.local solo se emplean como ejemplo. Es posible que no se apliquen a la mayoría de los entornos empresariales.

Iniciar sesión en tenants y agregar usuarios en vRealize Automation

Después de crear tenants para vRealize Automation en Lifecycle Manager, puede iniciar sesión en Workspace ONE Access para ver los tenants y agregar usuarios.

Si desea ver los tenants creados para una implementación de vRealize Automation, inicie sesión en la instancia de Workspace ONE Access asociada. La URL que se utilizará es `https://default-tenantname.domainname.local` o, en el caso de una implementación que no esté agrupada en clúster, `https://idm.domainname.local`, que lo llevará de nuevo a la URL de Workspace ONE Access de tenant predeterminada.

Puede validar tenants específicos en Workspace ONE Access mediante la siguiente URL: `https://tenant-1.domainname.local`. Esta URL abre una página que muestra los usuarios del tenant especificado. Puede hacer clic en **Agregar usuario** para crear usuarios adicionales de forma ad hoc.

Los usuarios autorizados pueden iniciar sesión en la organización del proveedor principal en vRealize Automation mediante `https://vra.domainname.local`. Esta vista proporciona acceso a todos los servicios relacionados con vRealize Automation.

Los usuarios autorizados pueden iniciar sesión en los tenants correspondientes de vRealize Automation con `https://tenantname.vra.domainname.local`.

Para obtener más información sobre la administración de usuarios en Workspace ONE Access, consulte [Administrar usuarios y grupos](#).

Agregar usuarios locales

Puede agregar usuarios locales a la implementación mediante la instancia de Workspace ONE Access asociada. Los usuarios locales son usuarios que no se almacenan en ningún proveedor de identidad externo.

Usar vRealize Orchestrator con implementaciones de varias organizaciones de vRealize Automation

Puede utilizar vRealize Orchestrator con implementaciones de tenants de varias organizaciones de vRealize Automation.

El tenant predeterminado admite la integración con la integración de vRealize Orchestrator incorporada de forma inmediata. vRealize Orchestrator está disponible preconfigurado en la página Integraciones del tenant predeterminado. Los subtenants no tienen ninguna integración de vRealize Orchestrator registrada previamente. Sin embargo, tienen varias opciones para agregar una integración de vRealize Orchestrator.

- Los subtenants pueden agregar una integración con la instancia integrada de vRealize Orchestrator si se desplazan a **Infraestructura > Conexiones > Integraciones**.

Nota Si la instancia integrada de vRealize Orchestrator se agrega como una integración a varios tenants, todo el contenido de vRealize Orchestrator, incluido el inventario del complemento, se comparte entre dichos tenants.

- Los subtenants pueden agregar una instancia externa de vRealize Orchestrator que utilice la instancia de vRealize Automation de varias organizaciones como proveedor de autenticación.

Cualquier instancia de vRealize Orchestrator que utilice una implementación de varias organizaciones de vRealize Automation como proveedor de autenticación se puede registrar en cualquiera de los tenants mediante la creación de una nueva integración y el FQDN de vRealize Orchestrator sin proporcionar ninguna credencial.

Trabajar con logs en vRealize Automation

5

Puede utilizar la utilidad de línea de comandos `vracli` que se proporciona para crear y utilizar logs en vRealize Automation.

Puede utilizar los logs directamente en vRealize Automation o puede reenviar todos los logs a vRealize Log Insight.

Este capítulo incluye los siguientes temas:

- [Cómo se trabaja con logs y paquetes de logs en vRealize Automation](#)
- [Cómo se configura el reenvío de logs a vRealize Log Insight en vRealize Automation](#)
- [Cómo crear o actualizar una integración de syslog en vRealize Automation](#)
- [Cómo trabajar con paquetes de contenido](#)

Cómo se trabaja con logs y paquetes de logs en vRealize Automation

Varios servicios generan logs automáticamente. Puede generar paquetes de logs en vRealize Automation. También puede configurar el entorno para enviar los logs a vRealize Log Insight.

Utilice el argumento `--help` en la línea de comandos `vracli` (por ejemplo, `vracli log-bundle --help`) para obtener información sobre la utilidad de línea de comandos `vracli`.

Para obtener información relacionada con el uso de vRealize Log Insight, consulte [Cómo se configura el reenvío de logs a vRealize Log Insight en vRealize Automation](#).

Comandos de paquetes de logs

Puede crear un paquete de logs para que contenga todos los logs generados por los servicios que se ejecutan. Un paquete de logs contiene todos los logs de servicio. Puede utilizar un paquete de logs para solucionar problemas.

En un entorno de clústeres (modo de alta disponibilidad), ejecute el comando `vracli log-bundle` en un solo nodo. Los logs se extraen de todos los nodos del entorno. Sin embargo, en el caso de un problema de red u otro problema de clúster, los logs se extraen de todos los nodos que puedan alcanzarse. Por ejemplo, si un nodo está desconectado en un clúster de tres nodos, solo se recopilan logs de los dos nodos en buen estado. Los resultados del comando `vracli log-bundle` contienen información sobre los problemas encontrados y pasos para su solución alternativa.

- Para crear un paquete de logs, utilice SSH en cualquier nodo y ejecute el siguiente comando `vracli`:

```
vracli log-bundle
```

- Para cambiar el valor de tiempo de espera de la recopilación de logs en cada nodo, ejecute el siguiente comando `vracli`:

```
vracli log-bundle --collector-timeout $CUSTOM_TIMEOUT_IN_SECONDS
```

Por ejemplo, si su entorno contiene archivos de log grandes, redes lentas o un uso elevado de CPU, puede establecer el tiempo de espera en un valor superior al predeterminado de 1.000 segundos.

- Para determinar el espacio de disco que consume un log de servicio específico (como `ebs` o `vro`), ejecute el siguiente comando `vracli` y examine la salida del comando:

```
vracli disk-mgr
```

- Para configurar otras opciones, como el tiempo de espera del ensamblado y la ubicación del búfer, utilice el siguiente comando de ayuda `vracli`:

```
vracli log-bundle --help
```

Estructura de paquetes de logs

El paquete de logs es un archivo tar con marca de hora. El nombre del paquete coincide con el patrón de archivo `log-bundle-<date>T<time>.tar`, por ejemplo `log-bundle-20200629T131312.tar`. Generalmente, el paquete de logs contiene los logs de todos los nodos del entorno. Si se produce un error, este contiene tantos logs como sea posible. Como mínimo, contiene los logs del nodo local.

El paquete de logs se compone del siguiente contenido:

- Archivo de entorno

El archivo de entorno contiene los resultados de diversos comandos de mantenimiento de Kubernetes. Proporciona información sobre el uso de recursos actual por nodo y por pod. También contiene información del clúster y descripciones de todas las entidades de Kubernetes disponibles.

- Configuración y logs de hosts

La configuración de cada host (por ejemplo, su directorio `/etc`) y los logs específicos del host (por ejemplo, `journald`) se recopilan en un directorio para cada host o nodo del clúster. El nombre del directorio coincide con el nombre de host del nodo. El contenido interno del directorio coincide con el sistema de archivos del host. El número de directorios coincide con el número de nodos del clúster.

■ Logs de servicios

Los registros de los servicios de Kubernetes se encuentran en la siguiente estructura de carpetas:

- `<hostname>/services-logs/<namespace>/<app-name>/file-logs/<container-name>.log`
- `<hostname>/services-logs/<namespace>/<app-name>/console-logs/<container-name>.log`

Un ejemplo de nombre de archivo es `my-host-01/services-logs/prelude/vco-app/file-logs/vco-server-app.log`.

- *hostname* es el nombre de host del nodo en el que se ejecuta o se estaba ejecutando el contenedor de la aplicación. Por lo general, hay una instancia para cada uno de los nodos de cada servicio. Por ejemplo, 3 nodos = 3 instancias.
 - *namespace* es el espacio de nombres de Kubernetes en el que se implementó la aplicación. Para los servicios orientados al usuario, este valor es `prelude`.
 - *app-name* es el nombre de la aplicación de Kubernetes que generó los logs (por ejemplo, `provisioning-service-app`).
 - *container-name* es el nombre del contenedor que generó los logs. Algunas aplicaciones constan de varios contenedores. Por ejemplo, el contenedor de `vco-app` incluye los contenedores `vco-server-app` y `vco-controlcenter-app`.
- #### ■ Logs de pod (heredado)

Antes de los cambios en la arquitectura de logs realizados en vRealize Automation 8.2, los logs de servicios estaban ubicados en el directorio de cada pod en el paquete de logs. Si bien es posible seguir generando logs de pods en el paquete mediante el comando `vracli log-bundle --include-legacy-pod-logs`, no se recomienda hacerlo, dado que toda la información de los logs ya reside en los logs de cada uno de los servicios. La inclusión de los logs de pod puede aumentar de forma innecesaria el tiempo y el espacio necesarios para generar el paquete de logs.

Reducir el tamaño del paquete de registros

Para generar un paquete de registros más pequeño, utilice uno de los siguientes comandos `vracli log-bundle`:

- `vracli log-bundle --since-days n`

Utilice este comando para recopilar solo los archivos de registro que se generaron en el último número de días. De lo contrario, los logs se conservan y se recopilan durante los últimos 2 días. Por ejemplo:

```
vracli log-bundle --since-days 1
```

- `vracli log-bundle --services service_A,service_B,service_C`

Utilice este comando para recopilar solo los registros de los servicios proporcionados con nombre. Por ejemplo:

```
vracli log-bundle --services ebs-app,vco-app
```

- `vracli log-bundle --skip-heap-dumps`

Utilice este comando para excluir todos los volcados de pila del paquete de registros generado.

Mostrar logs

Puede generar los registros de una aplicación o un pod de servicio mediante el comando `vracli logs <pod_name>`.

Las siguientes opciones de comando están disponibles:

- `--service`

Muestra un registro combinado para todos los nodos de la aplicación en lugar de un solo pod

Ejemplo: `vracli logs --service abx-service-app`

- `--tail n`

Muestra las últimas líneas *n* del registro. El valor de *n* predeterminado es 10.

Ejemplo: `vracli logs --tail 20 abx-service-app-8598fcd4b4-tjwhk`

- `--file`

Muestra solo el archivo especificado. Si no se proporciona un nombre de archivo, se muestran todos los archivos.

Ejemplo: `vracli logs --file abx-service-app.log abx-service-app-8598fcd4b4-tjwhk`

Comprender la rotación de logs

En cuanto a la rotación de logs, debe tener en cuenta las siguientes consideraciones sobre logs del servicio:

- Todos los servicios generan logs. Los logs de servicio se almacenan en un disco `/var/log/services-logs` dedicado.
- Todos los logs se rotan con regularidad. La rotación se produce cada hora o cuando se alcanza un límite de tamaño determinado.
- Todas las rotaciones de logs antiguas se acaban comprimiendo.

- No hay ninguna cuota por servicio por las rotaciones de logs.
- El sistema conserva tantos logs como sea posible. La automatización comprueba regularmente el espacio de disco utilizado para los logs. Cuando el espacio se llena en un 70 %, los logs más antiguos se purgan hasta que el espacio de disco de los logs alcanza el 60 % de su capacidad.
- Puede cambiar el tamaño del disco de logs si necesita más espacio. Consulte [Aumentar el espacio de disco del dispositivo de vRealize Automation](#).

Para comprobar el espacio de disco de los logs, ejecute los siguientes comandos `vracli`. El espacio libre de `/dev/sdc(/var/log)` debe estar cerca del 30 % o más para cada nodo.

```
# vracli cluster exec -- bash -c 'current_node; vracli disk-mgr; exit 0'
sc1-10-182-1-103.eng.vmware.com
/dev/sda4(/):
  Total size: 47.80GiB
  Free: 34.46GiB(72.1%)
  Available(for non-superusers): 32.00GiB(66.9%)
  SCSI ID: (0:0)
/dev/sdb(/data):
  Total size: 140.68GiB
  Free: 116.68GiB(82.9%)
  Available(for non-superusers): 109.47GiB(77.8%)
  SCSI ID: (0:1)
/dev/sdc(/var/log):
  Total size: 21.48GiB
  Free: 20.76GiB(96.6%)
  Available(for non-superusers): 19.64GiB(91.4%)
  SCSI ID: (0:2)
/dev/sdd(/home):
  Total size: 29.36GiB
  Free: 29.01GiB(98.8%)
  Available(for non-superusers): 27.49GiB(93.7%)
  SCSI ID: (0:3)
```

Cómo se configura el reenvío de logs a vRealize Log Insight en vRealize Automation

Puede reenviar los logs desde vRealize Automation a vRealize Log Insight para aprovechar la función más robusta de análisis de logs y la generación de informes.

vRealize Automation se incluye con un agente de creación de logs [basado en Fluent](#). El agente recopila y almacena los logs para que puedan incluirse en un paquete de logs y se puedan examinar más adelante. Puede configurar el agente para que reenvíe una copia de los logs a un servidor de vRealize Log Insight mediante REST API de vRealize Log Insight. La API permite que otros programas se comuniquen con vRealize Log Insight.

Para obtener más información sobre vRealize Log Insight, incluida la documentación de REST API de vRealize Log Insight, consulte la [documentación de vRealize Log Insight](#).

Configure el agente de creación de logs para que reenvíe de forma continua los logs de vRealize Automation a vRealize Log Insight mediante la utilidad de línea de comandos de `vracli` proporcionada.

Todas las líneas de log se etiquetan con un nombre de host y una etiqueta de entorno, y se pueden examinar en vRealize Log Insight. En un entorno de alta disponibilidad (High Availability, HA), los logs se etiquetan con diferentes nombres de host en función del nodo del que provengan. La etiqueta de entorno se puede configurar mediante la opción `--environment ENV` como se describe a continuación en la sección *Configurar o actualizar la integración de vRealize Log Insight*. En un entorno de alta disponibilidad, la etiqueta de entorno tiene el mismo valor para todas las líneas de log, independientemente del nodo del que provengan.

Puede encontrar información sobre cómo utilizar la utilidad de línea de comandos `vracli` si utiliza el argumento `--help` en la línea de comandos de `vracli`. Por ejemplo: `vracli vrli --help`. Para obtener una respuesta fácil de usar, inicie el comando con `vracli -j vrli`.

Nota Solo puede configurar una única integración de registro remoto. Se da prioridad a vRealize Log Insight en el caso de que estén disponibles tanto un servidor de vRealize Log Insight como un servidor syslog.

Comprobar la configuración existente de vRealize Log Insight

Command

```
vracli vrli
```

Arguments

No hay argumentos de línea de comandos.

Output

La configuración actual de la integración de vRealize Log Insight se genera en formato JSON.

Exit codes

Los siguientes códigos de salida son posibles:

- 0: se configuró la integración con vRealize Log Insight.
- 1: se produjo una excepción como parte de la ejecución del comando. Revise el mensaje de error para conocer los detalles.
- 61 (ENODATA): no se configuró la integración con vRealize Log Insight. Revise el mensaje de error para conocer los detalles.

Example - check integration configuration

```
$ vracli vrli
No vRLI integration configured

$ vracli vrli
{
```

```

"agentId": "0",
"environment": "prod",
"host": "my-vrli.local",
"port": 9543,
"scheme": "https",
"sslVerify": false
}

```

Configurar o actualizar la integración de vRealize Log Insight

Command

```
vracli vrli set [options] FQDN_OR_URL
```

Nota Después de ejecutar el comando, el agente de creación de logs puede tardar hasta dos minutos en aplicar la configuración especificada.

Arguments

- FQDN_OR_URL

Especifica la dirección URL o el FQDN del servidor de vRealize Log Insight que se utilizará para publicar logs. De forma predeterminada, se usan el puerto 9543 y HTTPS. Si hay que cambiar alguna de estas opciones de configuración, puede usar una URL en su lugar.

```
vracli vrli set <options> https://FQDN:9543
```

Nota Puede establecer un esquema de host (el valor predeterminado es HTTPS) y un puerto (el valor predeterminado para HTTPS es 9543, y para HTTP es 9000) diferentes para usarlos al enviar los logs, como se muestra en los siguientes ejemplos:

```

vracli vrli set https://HOSTNAME:9543
vracli vrli set --insecure HOSTNAME
vracli vrli set http://HOSTNAME:9000

```

La instancia de REST API de consumo de vRealize Log Insight utiliza los puertos 9543 para HTTPS y 9000 para HTTP, como se describe en el tema *Administrar vRealize Log Insight Puertos e interfaces externas* de la [documentación de vRealize Log Insight](#).

- Opciones

- --agent-id SOME_ID

Establece el identificador del agente de creación de logs de este dispositivo. El valor predeterminado es 0. Se utiliza para identificar el agente cuando se publican logs en vRealize Log Insight mediante REST API de vRealize Log Insight.

- --environment ENV

Establece un identificador para el entorno actual. Estará disponible en los logs de vRealize Log Insight como una etiqueta para cada entrada de log. El valor predeterminado es `prod`.

- `--ca-file /path/to/server-ca.crt`

Especifica un archivo que contiene el certificado de la entidad de certificación (CA) que se utilizó para firmar el certificado del servidor de vRealize Log Insight. Esto hace que el agente de creación de logs confíe en la entidad de certificación especificada y que permita la comprobación del certificado del servidor de vRealize Log Insight si estaba firmado por una entidad que no es de confianza. El archivo puede contener una cadena de certificados completa para comprobar el certificado. En el caso de un certificado autofirmado, apruebe el certificado en sí.

- `--ca-cert CA_CERT`

La definición es idéntica a la de `--ca-file` que se indica más arriba, pero aprueba el certificado (cadena) en línea como una cadena.

- `--insecure`

Desactiva la verificación SSL del certificado del servidor. Obliga al agente de creación de logs a aceptar cualquier certificado SSL al publicar los logs.

- Opciones avanzadas

- `--request-max-size BYTES`

Se recopilan varios eventos de log con una sola llamada de API. Este argumento controla el tamaño de carga útil máximo, en bytes, de cada solicitud. Los valores válidos son números entre 4000 y 4 000 000. El valor predeterminado es 256 000. Para obtener información relacionada con los valores permitidos, consulte la sección sobre el consumo de eventos de vRealize Log Insight en la documentación de REST API de vRealize Log Insight. Si se establece un valor demasiado bajo, es posible que se descarten eventos de creación de logs que superen el tamaño permitido.

- `--request-timeout SECONDS`

Una llamada a la API puede dejar de responder por varios motivos, entre los que se incluyen problemas con un punto remoto, problemas de redes, etc. Este parámetro controla la cantidad de segundos que se debe esperar para que se complete cada operación, como abrir una conexión, escribir datos o esperar una respuesta, antes de que la llamada se reconozca como con errores. El valor no puede ser inferior a 1 segundo. El valor predeterminado es 30.

- `--request-immediate-retries RETRIES`

Los logs se almacenan en búfer en fragmentos agregados antes de su envío a vRealize Log Insight (consulte a continuación `--buffer-flush-thread-count`). Si se produce un error en una solicitud de API, se vuelve a intentar el log inmediatamente. La cantidad predeterminada de reintentos inmediatos es 3. Si ninguno de los reintentos se realiza correctamente, se revierte el fragmento de logs completo y se vuelve a intentar más tarde.

- `--request-http-compress`

Para reducir los volúmenes de tráfico de red, puede aplicar la compresión gzip a las solicitudes que se envían al servidor de vRealize Log Insight. Si no se especifica este parámetro, no se utiliza ninguna compresión.

- `--buffer-flush-thread-count THREADS`

Para obtener un mejor rendimiento y limitar el tráfico de red, los logs se almacenan en búfer de forma local en fragmentos antes de que se vacíen y se envíen al servidor de logs. Cada fragmento contiene logs de un solo servicio. En función de su entorno, los fragmentos pueden crecer y tardar mucho tiempo en depurarse. Este argumento controla la cantidad de fragmentos que se pueden vaciar simultáneamente. El valor predeterminado es 2.

Nota Al configurar la integración a través de HTTPS, si el servidor de vRealize Log Insight está configurado para utilizar un certificado que no es de confianza, como un certificado autofirmado o un certificado firmado por una entidad que no es de confianza, utilice una de las opciones `--ca-file`, `--ca-cert` o `--insecure`. En caso contrario, el agente de creación de logs no podrá validar la identidad del servidor y no enviará los logs. Cuando se utiliza `--ca-file` o `--ca-cert`, el certificado del servidor de vRealize Log Insight debe ser válido para el nombre de host del servidor. En todos los casos, compruebe la integración. Para ello, deje unos minutos para el procesamiento y, a continuación, compruebe que vRealize Log Insight haya recibido los logs.

Output

No se espera ningún resultado.

Exit codes

Los siguientes códigos de salida son posibles:

- 0: se actualizó la configuración.
- 1: se produjo una excepción como parte de la ejecución. Revise el mensaje de error para conocer los detalles.

Examples - Configure or update integration configuration

Las siguientes instrucciones de ejemplo se muestran en líneas de comandos separadas; sin embargo, los argumentos se pueden combinar en una sola línea de comandos. Por ejemplo, puede incluir varios argumentos al utilizar `vracli vrli set {somehost}` o `vracli vrli set --ca-file path/to/server-ca.crt` para modificar el identificador del agente o los valores del entorno predeterminados. Para obtener información relacionada, consulte la ayuda de comandos en línea en `vracli vrli --help`.

```
$ vracli vrli set my-vrli.local
$ vracli vrli set 10.20.30.40
$ vracli vrli set --ca-file /etc/ssl/certs/ca.crt 10.20.30.40
$ vracli vrli set --ca-cert "$(cat /etc/ssl/certs/ca.crt)" 10.20.30.40
$ vracli vrli set --insecure http://my-vrli.local:8080
$ vracli vrli set --agent-id my-vrli-agent my-vrli.local
```

```
$ vracli vrli set --request-http-compress
$ vracli vrli set --environment staging my-vrli.local
$ vracli vrli set --environment staging --request-max-size 10000 --request-timeout 120 --
request-immediate-retries 5 --buffer-flush-thread-count 4 my-vrli.local
```

Borrar la integración de vRealize Log Insight

Command

```
vracli vrli unset
```

Nota Después de ejecutar el comando, el agente de creación de logs puede tardar hasta dos minutos en aplicar la configuración especificada.

Arguments

No hay argumentos de línea de comandos.

Output

La confirmación se envía como texto sin formato.

Exit codes

Están disponibles los siguientes códigos de salida:

- 0: se borró la configuración o no existía ninguna.
- 1: se produjo una excepción como parte de la ejecución. Revise el mensaje de error para conocer los detalles.

Examples - Clear integration

```
$ vracli vrli unset
Clearing vRLI integration configuration

$ vracli vrli unset
No vRLI integration configured
```

Cómo crear o actualizar una integración de syslog en vRealize Automation

Puede configurar vRealize Automation para que envíe su información de registro a servidores syslog remotos.

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

La integración remota de syslog de vRealize Automation admite los siguientes tipos de conexión:

- Mediante UDP.

- Mediante TCP sin TLS.

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

- Mediante TCP con TLS.

Nota Solo puede configurar una única integración de registro remoto. Se da prioridad a vRealize Log Insight en el caso de que existan un servidor de vRealize Log Insight y un servidor syslog disponibles.

Para obtener información sobre la configuración de la integración de registros con vRealize Log Insight, consulte [Cómo se configura el reenvío de logs a vRealize Log Insight en vRealize Automation](#).

Requisitos previos

Configure un servidor syslog remoto.

Procedimiento

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

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

Nota Si no introduce un puerto en el comando `vracli remote-syslog set`, el valor predeterminado del puerto es 514.

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

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

Nota De forma predeterminada, el dispositivo de vRealize Automation solicita que confirme que desea sobrescribir la integración de syslog. Para omitir la solicitud de confirmación, agregue la marca `-f o --force` al comando `vracli remote-syslog set`.

Pasos siguientes

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

Cómo eliminar una integración de syslog para el registro en vRealize Automation

Puede eliminar las integraciones de syslog del dispositivo de vRealize Automation ejecutando el comando `vracli remote-syslog unset`.

Requisitos previos

Cree una o varias integraciones de syslog en el dispositivo de vRealize Automation. Consulte [Cómo crear o actualizar una integración de syslog en vRealize Automation](#).

Procedimiento

- 1 Inicie sesión en la línea de comandos del dispositivo de vRealize Automation como **raíz**.
- 2 Elimine las integraciones de syslog del dispositivo de vRealize Automation con uno de los siguientes métodos:
 - Para eliminar una integración de syslog específica, ejecute el comando `vracli remote-syslog unset -id Integration_name`.
 - Para eliminar todas las integraciones de syslog del dispositivo de vRealize Automation, ejecute el comando `vracli remote-syslog unset` sin la marca `-id`.

Nota De forma predeterminada, el dispositivo de vRealize Automation le solicita que confirme que desea eliminar todas las integraciones de syslog. Para omitir la solicitud de confirmación, agregue la marca `-f o --force` al comando `vracli remote-syslog unset`.

Cómo trabajar con paquetes de contenido

Los paquetes de contenido se alojan en Log Insight y contienen paneles, campos extraídos, consultas guardadas y alertas relacionadas con un producto específico o un conjunto de registros. Puede instalar paquetes de contenido compatibles con la comunidad desde VMware Sample Exchange y otros paquetes de contenido del catálogo de Content Pack.

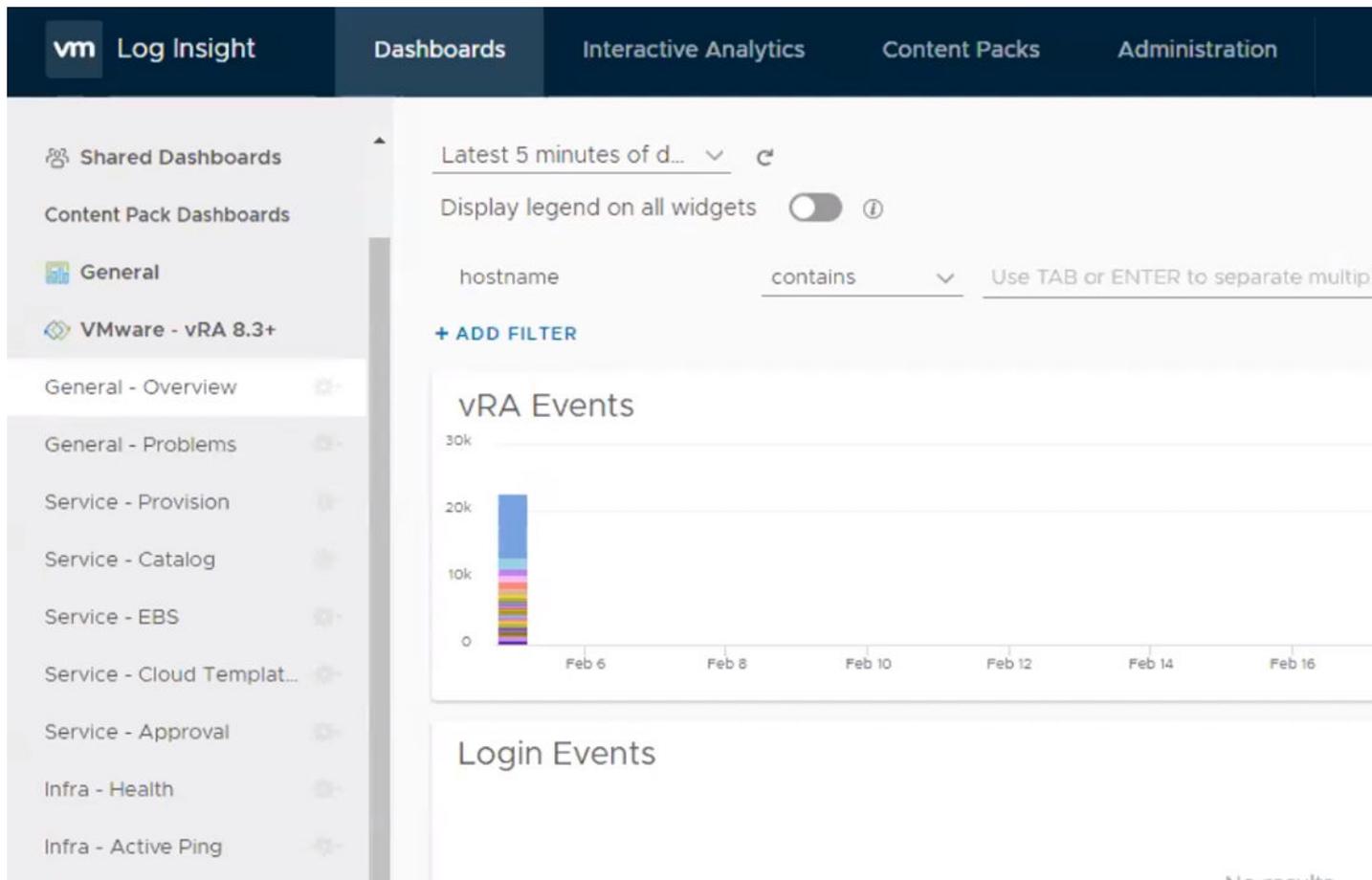
VMware vRealize Log Insight brinda administración automatizada de logs mediante agregación, análisis y búsqueda, lo que permite inteligencia operativa y visibilidad de toda la empresa en entornos dinámicos de nube híbrida. Los paquetes de contenido son complementos de VMware vRealize Log Insight que proporcionan conocimiento predefinido sobre tipos específicos de eventos, como mensajes de logs.

Para descargar un paquete de contenido, en Log Insight acceda a **Paquetes de contenido > Catálogo**. También puede importar paquetes de contenido haciendo clic en **+ Importar paquete de contenido**.

Paquete de contenido de vRA 8.x

El paquete de contenido de VMware vRealize Automation proporciona un resumen consolidado de los eventos de log en todos los componentes del entorno de vRA. Incluye varios paneles que proporcionan una descripción general, información sobre errores y operaciones, y el estado general de la instancia de vRA. Estos paneles se enumeran en la pestaña **Panel** junto con el resto de paneles de Log Insight. Una vez cargados, los paneles pueden tardar hasta 30 segundos en rellenarse con métricas.

Nota No se puede actualizar del paquete de contenido de vRA 7.5 o superior al paquete de contenido de vRA 8.3. Debe instalar el paquete de contenido de vRA 8.3. Una vez instalados, los paquetes de contenido de las versiones 8.3 y 7.5 funcionan por separado.



El paquete de contenido de vRealize Automation incluye estos paneles:

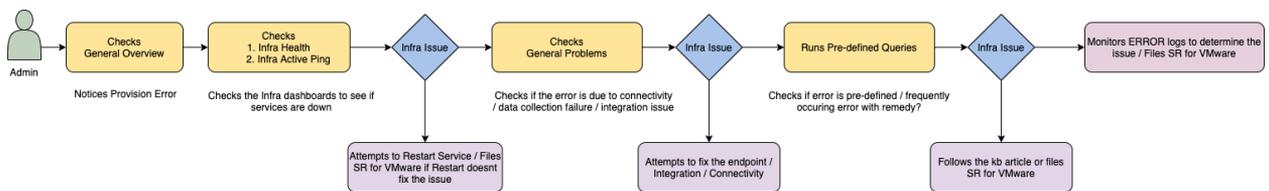
- General - Descripción general: captura una descripción general de métricas de alto nivel para vRA.
- General - Problemas:
- Servicio - Aprovisionar: captura problemas relacionados con el servicio de aprovisionamiento.
- Servicio - Catálogo: captura problemas relacionados con el servicio del catálogo.

- Servicio - EBS: captura problemas relacionados con el servicio de agentes de eventos.
- Servicio - Plantillas de nube: captura errores y métricas relacionados con plantillas de nube, recursos personalizados y acciones de recursos de Cloud Assembly.
- Servicio - Aprobación: captura errores y métricas relacionados con aprobaciones.
- Infraestructura - Estado: captura cuando los pods se reinician a lo largo del tiempo. Este panel es esencial para detectar interrupciones debido a límites de recursos.
- Infraestructura - Ping activo: captura la URL de comprobación de estado a lo largo del tiempo.

Cada panel contiene widgets individuales que proporcionan análisis más específicos. Para ver qué

tipo de análisis se realiza en cada widget, haga clic en el icono de información .

Como administrador de vRealize Automation, puede seguir este flujo de trabajo de paquete de contenido general para identificar errores y solucionar problemas.



Para obtener más información sobre el paquete de contenido de vRealize Automation 8.3, consulte [Paquete de contenido de Log Insight de vRealize Automation 8.3+](#) y [Cómo se configura el reenvío de logs a vRealize Log Insight](#).

Participar en el programa de mejora de la experiencia de cliente de vRealize Automation

6

Este producto participa en el Programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) de VMware. El CEIP proporciona a VMware información que le permite mejorar sus productos y servicios, solucionar problemas y ofrecer consejos relacionados con la mejor forma de implementar y utilizar los productos.

Los detalles relacionados con los datos recopilados mediante el CEIP, así como los fines para los que VMware los utiliza, se describen en la página del [programa de mejora de la experiencia de cliente](#).

Este capítulo incluye los siguientes temas:

- [Cómo hay que unirse al programa de mejora de la experiencia de cliente para vRealize Automation o cómo se abandona](#)
- [Cómo se configura la hora de la recopilación de datos para el programa de mejora de la experiencia de cliente de vRealize Automation](#)

Cómo hay que unirse al programa de mejora de la experiencia de cliente para vRealize Automation o cómo se abandona

Desde la línea de comandos del dispositivo de vRealize Automation, únase al programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) o abandónelo.

Puede unirse al CEIP al instalar vRealize Automation y con vRealize Lifecycle Manager (LCM). También puede unirse al programa mediante las opciones de la línea de comandos después de la instalación, así como abandonarlo.

Realice lo siguiente para unirse al programa de mejora de la experiencia de cliente mediante las opciones de la línea de comandos:

- 1 Inicie sesión en la línea de comandos del dispositivo de vRealize Automation como **raíz**.
- 2 Ejecute el comando `vracli ceip on`.
- 3 Revise la información del programa de mejora de la experiencia de cliente y ejecute el comando `vracli ceip on --acknowledge-ceip`.

- 4 Para reiniciar los servicios de vRealize Automation, ejecute el comando `/opt/scripts/deploy.sh`.

Realice lo siguiente para abandonar el programa de mejora de la experiencia de cliente mediante las opciones de la línea de comandos:

- 1 Inicie sesión en la línea de comandos del dispositivo de vRealize Automation como **raíz**.
- 2 Ejecute el comando `vracli ceip off`.
- 3 Para reiniciar los servicios de vRealize Automation, ejecute el comando `/opt/scripts/deploy.sh`.

Cómo se configura la hora de la recopilación de datos para el programa de mejora de la experiencia de cliente de vRealize Automation

Puede definir el día y la hora en que el programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) enviará los datos a VMware.

Procedimiento

- 1 Inicie sesión en la línea de comandos del dispositivo de vRealize Automation como **raíz**.
- 2 Abra el siguiente archivo en un editor de texto.
`/etc/telemetry/telemetry-collector-vami.properties`
- 3 Edite las propiedades del día de la semana (Day Of Week, DOW) y la hora del día (Hour Of Day, HOD).

Propiedad	Descripción
<code>frequency.dow=<day-of-week></code>	El día en que se efectúa la recopilación de datos.
<code>frequency.hod=<hour-of-day></code>	La hora local del día en que se efectúa la recopilación de datos. Los posibles valores oscilan entre 0 y 23.

- 4 Guarde y cierre `telemetry-collector-vami.properties`.
- 5 Aplique la configuración introduciendo el siguiente comando:

```
vcac-config telemetry-config-update --update-info
```

Los cambios se aplican a todos los nodos de la implementación.

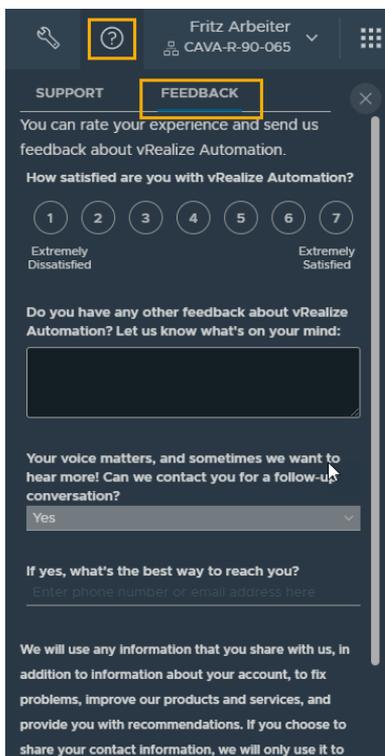
Activación del formulario de comentarios en el producto en vRealize Automation

7

Puede permitir que los usuarios proporcionen comentarios al equipo de desarrollo de vRealize Automation. Sus comentarios son importantes para nuestro proceso de desarrollo.

¿Cuál es el formulario de comentarios?

El formulario de comentarios se encuentra en el panel de soporte en una pestaña con la etiqueta Comentarios. Para abrir el formulario, haga clic en el botón **Ayuda** y, a continuación, haga clic en **Comentario**.



The screenshot shows a dark-themed user interface for vRealize Automation. At the top, there is a header with a question mark icon (highlighted with a yellow box), the user name 'Fritz Arbeiter', and the account ID 'CAVA-R-90-065'. Below the header, there are two tabs: 'SUPPORT' and 'FEEDBACK' (highlighted with a yellow box). The 'FEEDBACK' form contains the following elements:

- A message: "You can rate your experience and send us feedback about vRealize Automation."
- A question: "How satisfied are you with vRealize Automation?"
- A 7-point rating scale with buttons labeled 1 through 7. Below the scale, 'Extremely Dissatisfied' is on the left and 'Extremely Satisfied' is on the right.
- A question: "Do you have any other feedback about vRealize Automation? Let us know what's on your mind:"
- A text input field for providing additional feedback.
- A question: "Your voice matters, and sometimes we want to hear more! Can we contact you for a follow-up conversation?"
- A dropdown menu with 'Yes' selected.
- A question: "If yes, what's the best way to reach you?"
- A text input field with the placeholder "Enter phone number or email address here".
- A privacy notice at the bottom: "We will use any information that you share with us, in addition to information about your account, to fix problems, improve our products and services, and provide you with recommendations. If you choose to share your contact information, we will only use it to"

Cómo hacer que el formulario de comentarios esté disponible para los usuarios

El formulario de comentarios requiere que el host vRealize Automation tenga acceso a Internet y que las siguientes URL base se incluyan en la lista de permitidos de Internet.

- <https://lumos.vmware.com/>
- <https://feedback.esp.vmware.com/>

Si el host no tiene acceso a Internet, el formulario no estará disponible en el panel Ayuda.