

Administrar vRealize Automation

21 de diciembre de 2020
vRealize Automation 8.0

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 © 2021 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

- 1 Administrar vRealize Automation** 4
- 2 Administrar usuarios** 5
 - Cómo habilitar los grupos de Active Directory en vRealize Automation para los proyectos 6
 - Cómo eliminar usuarios en vRealize Automation 7
 - Cómo editar funciones de usuario en vRealize Automation 7
 - Cómo editar las asignaciones de funciones de grupo en vRealize Automation 8
- 3 Mantener el dispositivo** 10
 - Iniciar y detener vRealize Automation 10
 - Cómo habilitar la sincronización de hora 12
 - Cómo desactivar la sincronización de hora 13
 - Cómo se restablece la contraseña raíz 14
- 4 Trabajar con logs** 16
 - Cómo se trabaja con logs y paquetes de logs 16
 - Cómo se configura el reenvío de logs a vRealize Log Insight 18
- 5 Participar en el programa de mejora de la experiencia de cliente** 22
 - Cómo hay que unirse al programa o se abandona 22
 - Cómo se configura la hora de la recopilación de datos para el programa 23

Administrar vRealize Automation

1

Si bien la mayoría de tareas de administración de vRealize Automation se realizan desde VMware vRealize Suite Lifecycle Manager, en esta guía se describen algunas de las tareas de administración de usuarios y sistemas más importantes que se pueden realizar desde vRealize Automation.

Para obtener más información sobre cómo trabajar con vRealize Suite Lifecycle Manager, consulte [Instalación, actualización y administración de vRealize Suite Lifecycle Manager](#).

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 vRealize Automation 8.0.0 no admite la recuperación ante desastres. Para utilizar vRealize Automation en escenarios de recuperación ante desastres, actualice a vRealize Automation 8.0.1 o una versión posterior.

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 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.

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 vRealize Automation 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 la organización definen los permisos dentro del tenant; los propietarios de la 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
	■ Administrador de Service Broker
	■ Usuario 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 sobre cómo trabajar con LCM y Workspace ONE Access, consulte [Administración de usuarios con VMware Identity Manager](#).

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](#)

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 Cloud Assembly vRealize Automation](#) 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 Escriba en el campo de búsqueda 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.

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](#)
- [Cómo habilitar la sincronización de hora de vRealize Automation](#)
- [Cómo desactivar la sincronización de hora](#)
- [Cómo se restablece la contraseña raíz para vRealize Automation](#)

Iniciar y detener vRealize Automation

Observe los procedimientos adecuados al iniciar o cerrar vRealize Automation.

Cerrar vRealize Automation

Para conservar la integridad de los datos, desactive los servicios de vRealize Automation antes de apagar los dispositivos virtuales.

Nota Si es posible, evite utilizar los comandos `vraccli reset vidm`. Con este comando se restablece toda la configuración de Workspace One Access y se rompe 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/svc-stop.sh  
sleep 120  
/opt/scripts/deploy.sh --onlyClean
```

- 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:

```
kubect1 -n prelude get pods
```

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>Puede usar esta configuración cuando el servidor ESXi que aloja al dispositivo de 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.</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> <p>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>
systemd	<p>Esta configuración utiliza el daemon de systemd-timesyncd para sincronizar los relojes en su 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 --enable`.
- b Ejecute el comando `vracli ntp apply`.

La configuración de NTP de ESXi se aplica a la implementación de vRealize Automation.

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.

- b Ejecute el comando `vracli ntp apply`.

La configuración de NTP de systemd se aplica a la implementación de vRealize Automation.

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

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 que está sincronizado con el servidor NTP.

Cómo desactivar la sincronización de hora

Puede desactivar la sincronización de hora del protocolo de tiempo de redes (Network Time Protocol, NTP) en la implementación de vRealize Automation con la línea de comandos del dispositivo de vRealize Automation.

Requisitos previos

Compruebe haber configurado la sincronización de hora con ESXi o systemd. Consulte [Cómo habilitar la sincronización de hora de vRealize Automation](#).

Procedimiento

- 1** Inicie sesión en la línea de comandos del dispositivo de vRealize Automation como **raíz**.
- 2** Desactive una configuración de NTP de ESXi.
 - a Ejecute el comando `vracli ntp esxi --disable`.
 - b Ejecute el comando `vracli ntp apply`.

Se desactiva la configuración de NTP de ESXi.

- 3 Desactive una configuración de NTP de systemd.
 - a Ejecute el comando `vracli ntp systemd --disable FQDN_or_IP_of_systemd_server`.
 - b Ejecute el comando `vracli ntp apply`.

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

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 not 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.

Trabajar con logs en vRealize Automation

4

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](#)

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

Puede crear y utilizar logs de vRealize Automation y paquetes de logs en vRealize Automation.

Como alternativa, puede reenviar automáticamente los logs a vRealize Log Insight. Para obtener información sobre cómo reenviar logs a vRealize Log Insight, consulte [Cómo se configura el reenvío de logs a vRealize Log Insight](#).

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 log-bundle --help`.

Comandos de paquetes de logs

Puede crear un paquete de logs sencillo o un log (almacenamiento en frío) agregado de todos los servicios. Mientras que ambos paquetes de logs contienen todos los logs de sus servicios, el paquete de almacenamiento en frío contiene una copia de una secuencia agregada de versiones anteriores de los logs de servicio, que puede ser muy útiles para solucionar otros problemas. El agente de almacenamiento en frío agrega logs constantemente de los servicios y los almacena en el sistema de archivos local. Por lo general, todo lo que se necesita para solucionar problemas es un paquete de logs sencillo.

También puede modificar el valor de tiempo de espera predeterminado para recopilar logs de cada nodo.

En un entorno de clústeres, solo necesita ejecutar el comando `vracli log-bundle` en un nodo.

- Mostrar la ayuda del comando de paquete de logs:

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

- Cree un paquete de logs sencillo.

```
vracli log-bundle
```

- Cree un paquete de logs de almacenamiento en frío:

```
vracli log-bundle --include-cold-storage
```

- Cambie el valor de tiempo de espera para recopilar logs de cada nodo. Por ejemplo, si su entorno contiene archivos de log grandes, redes lentas, un uso elevado de CPU, etc., es posible que tenga que establecer el tiempo de espera en un valor superior al predeterminado de 1000 segundos.

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

Estructuras de paquetes de logs

Los servicios de vRealize Automation se encuentran en contenedores en pods de Kubernetes. El paquete de logs que se genera es un archivo de almacenamiento `tar.xz` con el formato de nombre `log-bundle-{{TIMESTAMP}}.tar.xz` (donde `TIMESTAMP` es una marca de tiempo en segundos). Un paquete de logs normal contiene los logs de todos los nodos del entorno. Si por algún motivo no se puede generar un paquete de logs, se creará un paquete de reserva en su lugar. El paquete de reserva solo contendrá los logs del nodo actual. Existen leves diferencias en la estructura de los dos tipos de paquetes de logs.

- Paquetes de logs normales

Los paquetes de logs normales se organizan en las siguientes categorías:

- Configuración y logs de hosts

La configuración de cada host y sus logs específicos del host se recopilan en un directorio por nodo de clúster (host). El nombre del directorio coincide con el nombre del host del nodo. El contenido del directorio coincide con el sistema de archivos del host. El número de directorios coincide con el número de nodos del clúster.

Los registros de almacenamiento en frío se encuentran en un log de JSON estructurado como `/nombre de host/services-logs/all/aggregated.log`.

- Logs de pod

Los servicios se encuentran en contenedores en pods de Kubernetes. Los logs de servicios se encuentran en el directorio `pods`, que contiene un único directorio por espacio de nombres con un nombre de archivo que coincide con el nombre del espacio de nombres. Normalmente hay una instancia de cada pod por nodo de clúster. El directorio de pod contiene un archivo de log por cada una de sus aplicaciones en el contenedor.

Por ejemplo, los logs del centro de control de vRealize Orchestrator se encuentran en un archivo de `vco-controlcenter-app.log` en cada uno de los directorios de `/pods/prelude/vco-app-hash/`.

- Archivo de entorno

El archivo de entorno contiene información sobre el uso de recursos actual por nodos y por pods. También contiene información de clúster y descripciones de todas las entidades de Kubernetes disponibles.

- Paquetes de logs de reserva

Si recibe un mensaje de error mientras espera a que finalice el comando `vracli`, se generará un paquete de reserva. Si recibe este error, tendrá que ejecutar el comando `vracli log-bundle` en cada host o nodo del clúster para recopilar la mayor cantidad de información posible.

- Logs del contenedor de reserva

Los logs de reserva se encuentran en el directorio `/fallback-containers`. Si desea identificar qué contenedor generó los logs en qué pod, examine el nombre del archivo de log:

```
nombre-pod-a-lgún-hash-nombre-contenedor-otro-hash.log
```

- Almacenamiento en frío de reserva

Si recopila los logs de almacenamiento en frío con el paquete, los logs de reserva del host actual se guardan en el directorio `/fallback-cold-storage`.

Cómo se configura el reenvío de logs a vRealize Log Insight

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 la API de vRealize Log Insight. La API que se proporciona permite que otros programas se comuniquen con vRealize Log Insight.

Para obtener más información sobre vRealize Log Insight, incluida la documentación de la API de vRealize Log Insight, consulte la [documentación de vRealize Log Insight](#) y también la página [/api/v1/events/ingest/{agentId}](#).

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

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`.

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": 443,
  "scheme": "https",
  "sslVerify": false
}
```

Nota Puede establecer un esquema de host (el valor predeterminado es https) y un puerto (el valor predeterminado es 443) diferentes para usarlos al enviar los logs, como se muestra en los siguientes ejemplos:

```
vracli vrli set some-host
vracli vrli set some-host:9543
vracli vrli set http://some-host:9543
```

La API de consumo de vRealize Log Insight utiliza el puerto 9543 como se describe en el tema de *Administrar vRealize Log Insight Puertos e interfaces externas* de la [documentación de vRealize log Insight](#).

Configurar o actualizar la integración de vRealize Log Insight

Command

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

Arguments

Los siguientes argumentos de línea de comandos se encuentran disponibles:

- `FQDN_OR_URL`: el FQDN o la dirección IP del servidor de vRealize Log Insight que se utilizará para publicar los logs mediante la configuración de la API de vRealize Log Insight. El puerto 443 y un esquema HTTPS se utilizan de forma predeterminada. Si hay que cambiar alguna de estas opciones de configuración, puede usar una URL en su lugar.
- opciones
 - `--agent-id SOME_ID`: establezca el ID del agente de creación de logs para este dispositivo. El valor predeterminado es 0. Se utiliza para identificar el agente de creación de logs para los logs que se publican en vRealize Log Insight mediante la configuración de la API de vRealize Log Insight.
 - `--environment ENV`: establezca un identificador para el entorno actual. Estará disponible en los logs de vRealize Log Insight como una etiqueta para cada evento de línea de log. El valor predeterminado es `prod`.
 - `--ca-file /path/to/server-ca.crt`: especifique un archivo que contenga el certificado de la entidad de certificación (CA) que se utilizó para firmar el certificado del servidor de vRealize Log Insight. Obligue al agente de creación de logs a confiar en la entidad de certificación especificada y habilítelo para comprobar el certificado del servidor de vRealize Log Insight. El archivo puede contener una cadena de certificados completa si hace falta para comprobar el certificado. En el caso de un certificado autofirmado, apruebe el certificado en sí.
 - `--ca-cert CA_CERT`: especifique un archivo siguiendo el mismo procedimiento que con `--ca-file`, pero apruebe el certificado (cadena) en línea como una cadena.
 - `--insecure::`: desactive la verificación SSL del certificado del servidor. Obligue al agente de creación de logs a aceptar cualquier certificado SSL al publicar 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

```
$ 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 --environment staging my-vrli.local
```

Borrar la integración de vRealize Log Insight

Command

```
vracli vrli unset
```

Arguments

No hay argumentos de línea de comandos.

Output

La confirmación se envía como texto sin formato.

Exit codes

Los siguientes códigos de salida son posibles:

- 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
```

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

5

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 pueden encontrar en el Centro de seguridad y confianza en <http://www.vmware.com/trustvmware/ceip.html>.

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.