

Administering vRealize Log Insight

12-OCT-2017

vRealize Log Insight 4.5



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

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

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Copyright © 2014–2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

Administrar vRealize Log Insight	7
Updated Information for <i>Administrar vRealize Log Insight</i>	8
1 Actualizar vRealize Log Insight	9
Ruta de acceso de actualización de vRealize Log Insight	9
Actualizar a vRealize Log Insight 4.5	10
Actualizar a vRealize Log Insight 4.3	11
Actualizar a vRealize Log Insight 4.0	12
Actualizar a vRealize Log Insight 3.6	13
2 Administrar cuentas de usuario de vRealize Log Insight	15
Descripción general de administración de usuarios	16
Control de acceso basado en funciones	16
Crear una cuenta de usuario nueva en vRealize Log Insight	17
Configurar el acceso de VMware Identity Manager a los grupos de Active Directory para vRealize Log Insight	18
Importar un grupo de Active Directory a vRealize Log Insight	20
Autenticar usuarios con la pertenencia a grupos de dominios múltiples	21
Definir un conjunto de datos	21
Crear y modificar funciones	23
Eliminar una cuenta de usuario de vRealize Log Insight	23
3 Configurar la autenticación	25
Habilitar la autenticación de usuario a través de VMware Identity Manager	25
Habilitar la autenticación de usuarios a través de Active Directory	27
Configurar el protocolo que se usará para Active Directory	28
4 Configurar vRealize Log Insight	30
vRealize Log Insight Límites de configuración	31
Configurar las opciones del dispositivo virtual	32
Configurar la contraseña SSH raíz para el dispositivo virtual vRealize Log Insight	32
Cambiar la configuración de redes de la vApp vRealize Log Insight	33
Aumentar la capacidad de almacenamiento del dispositivo virtual de vRealize Log Insight	34
Añadir memoria y CPU al dispositivo virtual vRealize Log Insight	36
Asigne una licencia permanente a vRealize Log Insight	36
Directiva de almacenamiento de registros	37

- Administrar notificaciones del sistema 37
 - Notificaciones del sistema de vRealize Log Insight 38
 - Configurar las notificaciones del sistema de vRealize Log Insight 46
- Añadir destino de reenvío de eventos de vRealize Log Insight 49
 - Configurar el reenvío de eventos de vRealize Log Insight con SSL 51
- Sincronice la hora en el dispositivo virtual de vRealize Log Insight 52
- Configurar el servidor SMTP para vRealize Log Insight 53
- Instalar un certificado SSL personalizado 54
 - Generar un certificado autofirmado 55
 - Generar una solicitud de firma de certificado 57
 - Solicitar la firma de una entidad de certificación 58
 - Concatenar archivos de certificados 58
 - Cargar certificado firmado 59
 - Configurar la conexión SSL entre el servidor vRealize Log Insight y los Log Insight Agents 59
- Cambiar el período de tiempo de espera predeterminado para las sesiones web de vRealize Log Insight 63
- Archivos 64
 - Habilitar o deshabilitar archivos de datos en vRealize Log Insight 64
 - Formatear los archivos de vRealize Log Insight 65
 - Importar un archivo de vRealize Log Insight a vRealize Log Insight 66
 - Exportar un archivo de Log Insight a un archivo de texto sin procesar o JSON 67
- Reinicie el servicio de vRealize Log Insight 68
- Apagar el dispositivo virtual de vRealize Log Insight 68
- Descargar un paquete de soporte de vRealize Log Insight 69
- Unirse al Programa de mejora de la experiencia de cliente o abandonarlo 70

- 5 Configurar clústeres de vRealize Log Insight 71**
 - Añadir un nodo de trabajador al clúster de vRealize Log Insight . 71
 - Implementar el dispositivo virtual vRealize Log Insight 72
 - Unirse a una implementación existente 75
 - Eliminar un nodo de trabajador de un clúster de vRealize Log Insight 76
 - Trabajar con un equilibrador de carga integrado 77
 - Habilitar el equilibrador de carga integrado 78
 - Consultar los resultados de comprobaciones de clústeres en producción 79

- 6 Puertos e interfaces externas 80**

- 7 Supervisar el estado de los agentes de Windows y Linux de vRealize Log Insight 84**

- 8 Habilitar la actualización automática de los agentes desde el servidor 85**

- 9 Trabajar con grupos de agentes 86**
 - [Fusión de configuraciones de grupos de agentes 87](#)
 - [Crear un grupo de agentes 87](#)
 - [Editar un grupo de agentes 88](#)
 - [Añadir un grupo de agentes de paquetes de contenidos como grupo de agentes 88](#)
 - [Eliminar un grupo de agentes 89](#)

- 10 Configurar y utilizar vRealize Log Insight Importer 90**
 - [Acerca del archivo de manifiesto de vRealize Log Insight Importer 91](#)
 - [Instalar, configurar y ejecutar vRealize Log Insight Importer 92](#)
 - [Ejemplos de configuración de archivos de manifiesto de vRealize Log Insight Importer 94](#)
 - [Parámetros de configuración de vRealize Log Insight Importer 95](#)

- 11 Supervisar vRealize Log Insight 97**
 - [Revisar el estado del dispositivo virtual vRealize Log Insight 97](#)
 - [Supervisar hosts que envían eventos de registro 98](#)

- 12 Integración de vRealize Log Insight con productos VMware 99**
 - [Conectar vRealize Log Insight a un entorno vSphere 100](#)
 - [vRealize Log Insight como servidor de Syslog 102](#)
 - [Configurar un host ESXi para que reenvíe eventos de registro a vRealize Log Insight 102](#)
 - [Modificar una configuración de host ESXi para reenviar eventos de registro a vRealize Log Insight 103](#)
 - [Eventos de notificación de vRealize Log Insight en vRealize Operations Manager 105](#)
 - [Configure vRealize Log Insight para extraer eventos, tareas y alarmas desde la instancia de vCenter Server . 106](#)
 - [Uso de vRealize Operations Manager con vRealize Log Insight 107](#)
 - [Requisitos de la integración con vRealize Operations Manager 107](#)
 - [Configurar vRealize Log Insight para enviar eventos de notificación a vRealize Operations Manager 109](#)
 - [Habilitar ejecución en contexto para vRealize Log Insight en vRealize Operations Manager 110](#)
 - [Deshabilitar inicio en contexto para vRealize Log Insight en vRealize Operations Manager 114](#)
 - [Agregar un dominio y una ruta de búsqueda de DNS 115](#)
 - [Eliminar el adaptador de vRealize Log Insight 115](#)
 - [Paquete de contenido de vRealize Operations Manager para vRealize Log Insight 117](#)

- 13 Consideraciones de seguridad para vRealize Log Insight 118**
 - [Puertos e interfaces externas 118](#)
 - [Archivos de configuración de vRealize Log Insight 122](#)
 - [Clave pública, certificado y almacén de claves de vRealize Log Insight 122](#)
 - [Archivo de licencia y CLUF de vRealize Log Insight 123](#)
 - [Archivos de registro de vRealize Log Insight 123](#)

- Cuentas de usuario de vRealize Log Insight 125
- Recomendaciones de firewall de vRealize Log Insight 126
- Actualizaciones y revisiones de seguridad 127

14 Copia de seguridad, restauración y recuperación de desastres 128

- Información general sobre copias de seguridad, restauración y recuperación de desastres 128
- Utilizar direcciones IP estáticas y FQDN 129
- Planificación y preparación 130
- Copia de seguridad de nodos y clústeres 131
- Agentes de Linux o Windows de copia de seguridad 133
- Restaurar nodos y clúster 133
 - Cambiar configuraciones tras la restauración 134
 - Restaurar en el mismo host 135
 - Restablecer a un host diferente 135
- Verificar restauraciones 138
- Recuperación de desastres 139

15 Solución de problemas de vRealize Log Insight 140

- vRealize Log Insight no tiene espacio en disco 140
- Los datos archivados podrían no importarse correctamente 141
- Usar la consola del dispositivo virtual para crear un paquete de soporte de vRealize Log Insight 141
- Restablecer la contraseña del usuario administrador 142
- Restablecer la contraseña del usuario de raíz 143
- No se pudo entregar alertas a vRealize Operations Manager 144
- Imposible iniciar sesión usando las credenciales de Active Directory 145
- SMTP no funciona con la opción STARTTLS habilitada 146
- Error en la actualización al no poder validar la firma del archivo .pak 146
- Error en la actualización por error interno del servidor 147

Administrar vRealize Log Insight

Administrar vRealize Log Insight proporciona información acerca de cómo administrar VMware[®] vRealize[™] Log Insight[™], incluido el modo de gestionar las cuentas de usuarios e integrar Log Insight Agents con otros productos de VMware. También incluye información sobre cómo administrar la seguridad de los productos y actualizar su implementación.

Esta está redactada para administradores de sistemas Linux o Windows con experiencia que están familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Updated Information for *Administrar vRealize Log Insight*

Administrar vRealize Log Insight is updated with each release of the product or when necessary.

This table provides the update history of *Administrar vRealize Log Insight*.

Revision	Description
10-OCT-2017	<ul style="list-style-type: none">■ Removal of note about deprecation of support for Active Directory.■ Minor bug fixes.
05-SEP-2017	<ul style="list-style-type: none">■ Clarification of hardware requirements.
002541-1	<ul style="list-style-type: none">■ Revisions provide clarification of support status for external load balancers and native Active Directory use. See Trabajar con un equilibrador de carga integrado and Chapter 3 Configurar la autenticación.
002541-0	Initial release.

Actualizar vRealize Log Insight

Según la versión actual de vRealize Log Insight, es posible actualizar a una versión más reciente.

Este capítulo cubre los siguientes temas:

- [Ruta de acceso de actualización de vRealize Log Insight](#)
- [Actualizar a vRealize Log Insight 4.5](#)
- [Actualizar a vRealize Log Insight 4.3](#)
- [Actualizar a vRealize Log Insight 4.0](#)
- [Actualizar a vRealize Log Insight 3.6](#)

Ruta de acceso de actualización de vRealize Log Insight

La ruta de acceso de actualización y el procedimiento a seguir varía según la versión instalada de vRealize Log Insight que desee actualizar.

También puede comprobar las rutas de acceso de actualización compatibles con la función **Ruta de acceso de actualización** en el sitio [Matrices de interoperabilidad de productos VMware](#).

Las actualizaciones de vRealize Log Insight son incrementales. Debe actualizar a las versiones intermedias.

Tabla 1-1. Rutas de acceso de actualización compatibles

Actualizar desde	Actualizar a	Procedimiento
vRealize Log Insight 4.3	vRealize Log Insight 4.5	Consulte Actualizar a vRealize Log Insight 4.5
vRealize Log Insight 4.0	vRealize Log Insight 4.3	Consulte Actualizar a vRealize Log Insight 4.3
vRealize Log Insight 3.6	vRealize Log Insight 4.0	Consulte Actualizar a vRealize Log Insight 4.0 .
vRealize Log Insight 3.3	vRealize Log Insight 3.6	Consulte Actualizar a vRealize Log Insight 3.6 .

Actualizar a vRealize Log Insight 4.5

Puede actualizar automáticamente un clúster a vRealize Log Insight 4.5.

La actualización de vRealize Log Insight debe realizarse desde el FQDN del nodo principal. No se admite la actualización mediante la dirección IP del equilibrador de carga integrado.

Durante la actualización, en primer lugar el nodo principal se actualiza y se reinicia. A continuación, cada nodo del clúster se actualiza secuencialmente. Puede consultar el estado actual de la actualización gradual en **Administración > Clúster**. Si se configura el equilibrador de carga integrado, sus IP se migran entre los nodos del clúster para que sus servicios (incluidos el consumo de eventos entrantes, la interfaz de usuario y la API) sigan estando disponibles durante la actualización gradual. Los detalles de bajo nivel se registran en el archivo `upgrade.log` de cada nodo individual. Se envía una notificación del sistema cuando la actualización se complete correctamente.

Si se detecta un problema que afecta a uno o a varios nodos durante el proceso de actualización, todo el clúster se revertirá automáticamente a la versión original que funciona. Es posible que los cambios en la configuración realizados después de iniciarse la actualización no sean válidos o consistentes. Por tanto, la configuración se revierte a un estado válido conocido que se ha guardado antes de iniciar la actualización. Los eventos que no se han consumido se pierden. El progreso se registra en el archivo `rollback.log` de cada nodo individual. Se envía una notificación del sistema cuando este proceso se complete. Cuando el problema se haya investigado y se haya solucionado, puede volver a intentar ejecutar la actualización.

Prerequisitos

- Verifique que aplica la actualización a una ruta de acceso de actualización compatible. Consulte [Ruta de acceso de actualización de vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtenga una copia del archivo `.pak` del paquete de actualización de vRealize Log Insight.
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 Haga clic en **Actualizar de PAK** para cargar el archivo `.pak`.
- 4 Accept the new EULA to complete the upgrade procedure.

Qué hacer a continuación

Una vez finalizado el proceso de actualización del nodo principal, puede visualizar el proceso de actualización remanente, que es automático.

Busque el correo electrónico enviado al Administrador para confirmar que la actualización finalizó en forma exitosa.

Actualizar a vRealize Log Insight 4.3

Puede actualizar automáticamente un clúster a vRealize Log Insight 4.3.

La actualización de vRealize Log Insight debe realizarse desde el FQDN del nodo principal. No se admite la actualización mediante la dirección IP del equilibrador de carga integrado.

Durante la actualización, en primer lugar el nodo principal se actualiza y se reinicia. A continuación, cada nodo del clúster se actualiza secuencialmente. Puede consultar el estado actual de la actualización gradual en **Administración > Clúster**. Si se configura el equilibrador de carga integrado, sus IP se migran entre los nodos del clúster para que sus servicios (incluidos el consumo de eventos entrantes, la interfaz de usuario y la API) sigan estando disponibles durante la actualización gradual. Los detalles de bajo nivel se registran en el archivo `upgrade.Log` de cada nodo individual. Se envía una notificación del sistema cuando la actualización se complete correctamente.

Si se detecta un problema que afecta a uno o a varios nodos durante el proceso de actualización, todo el clúster se revertirá automáticamente a la versión original que funciona. Es posible que los cambios en la configuración realizados después de iniciarse la actualización no sean válidos o consistentes. Por tanto, la configuración se revierte a un estado válido conocido que se ha guardado antes de iniciar la actualización. Los eventos que no se han consumido se pierden. El progreso se registra en el archivo `rollback.Log` de cada nodo individual. Se envía una notificación del sistema cuando este proceso se complete. Cuando el problema se haya investigado y se haya solucionado, puede volver a intentar ejecutar la actualización.

Prerequisitos

- Verifique que aplica la actualización a una ruta de acceso de actualización compatible. Consulte [Ruta de acceso de actualización de vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtenga una copia del archivo `.pak` del paquete de actualización de vRealize Log Insight.
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 Haga clic en **Actualizar de PAK** para cargar el archivo `.pak`.

- 4 Accept the new EULA to complete the upgrade procedure.

Qué hacer a continuación

Una vez finalizado el proceso de actualización del nodo principal, puede visualizar el proceso de actualización remanente, que es automático.

Busque el correo electrónico enviado al Administrador para confirmar que la actualización finalizó en forma exitosa.

Actualizar a vRealize Log Insight 4.0

Puede actualizar automáticamente un clúster a vRealize Log Insight 4.0.

La actualización de vRealize Log Insight debe realizarse desde el FQDN del nodo principal. No se admite la actualización mediante la dirección IP del equilibrador de carga integrado.

Durante la actualización, en primer lugar el nodo principal se actualiza y se reinicia. A continuación, cada nodo del clúster se actualiza secuencialmente. Puede consultar el estado actual de la actualización gradual en **Administración > Clúster**. Si se configura el equilibrador de carga integrado, sus IP se migran entre los nodos del clúster para que sus servicios (incluidos el consumo de eventos entrantes, la interfaz de usuario y la API) sigan estando disponibles durante la actualización gradual. Los detalles de bajo nivel se registran en el archivo `upgrade_log` de cada nodo individual. Se envía una notificación del sistema cuando la actualización se complete correctamente.

Si se detecta un problema que afecta a uno o a varios nodos durante el proceso de actualización, todo el clúster se revertirá automáticamente a la versión original que funciona. Es posible que los cambios en la configuración realizados después de iniciarse la actualización no sean válidos o consistentes. Por tanto, la configuración se revierte a un estado válido conocido que se ha guardado antes de iniciar la actualización. Los eventos que no se han consumido se pierden. El progreso se registra en el archivo `rollback_log` de cada nodo individual. Se envía una notificación del sistema cuando este proceso se complete. Cuando el problema se haya investigado y se haya solucionado, puede volver a intentar ejecutar la actualización.

Prerequisitos

- Verifique que aplica la actualización a una ruta de acceso de actualización compatible. Consulte [Ruta de acceso de actualización de vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtenga una copia del archivo `.pak` del paquete de actualización de vRealize Log Insight.
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.

- 3 Haga clic en **Actualizar de PAK** para cargar el archivo .pak.
- 4 Accept the new EULA to complete the upgrade procedure.

Qué hacer a continuación

Una vez finalizado el proceso de actualización del nodo principal, puede visualizar el proceso de actualización remanente, que es automático.

Busque el correo electrónico enviado al Administrador para confirmar que la actualización finalizó en forma exitosa.

Actualizar a vRealize Log Insight 3.6

Puede actualizar automáticamente un clúster a vRealize Log Insight 3.6.

La actualización de vRealize Log Insight debe realizarse desde el FQDN del nodo principal. No se admite la actualización mediante la dirección IP del equilibrador de carga integrado.

Durante la actualización, en primer lugar el nodo principal se actualiza y se reinicia. A continuación, cada nodo del clúster se actualiza secuencialmente. Puede consultar el estado actual de la actualización gradual en **Administración > Clúster**. Si se configura el equilibrador de carga integrado, sus IP se migran entre los nodos del clúster para que sus servicios (incluidos el consumo de eventos entrantes, la interfaz de usuario y la API) sigan estando disponibles durante la actualización gradual. Los detalles de bajo nivel se registran en el archivo `upgrade.log` de cada nodo individual. Se envía una notificación del sistema cuando la actualización se complete correctamente.

Si se detecta un problema que afecta a uno o a varios nodos durante el proceso de actualización, todo el clúster se revertirá automáticamente a la versión original que funciona. Es posible que los cambios en la configuración realizados después de iniciarse la actualización no sean válidos o consistentes. Por tanto, la configuración se revierte a un estado válido conocido que se ha guardado antes de iniciar la actualización. Los eventos que no se han consumido se pierden. El progreso se registra en el archivo `rollback.log` de cada nodo individual. Se envía una notificación del sistema cuando este proceso se complete. Cuando el problema se haya investigado y se haya solucionado, puede volver a intentar ejecutar la actualización.

Prerequisitos

- Verifique que aplica la actualización a una ruta de acceso de actualización compatible. Consulte [Ruta de acceso de actualización de vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtenga una copia del archivo .pak del paquete de actualización de vRealize Log Insight.
- Verify that you are logged in to the vRealize Log Insight `portnumber` Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.

- 2 Under Management, click **Cluster**.
- 3 Haga clic en **Actualizar de PAK** para cargar el archivo .pak.
- 4 Accept the new EULA to complete the upgrade procedure.

Qué hacer a continuación

Una vez finalizado el proceso de actualización del nodo principal, puede visualizar el proceso de actualización remanente, que es automático.

Busque el correo electrónico enviado al Administrador para confirmar que la actualización finalizó en forma exitosa.

Administrar cuentas de usuario de vRealize Log Insight

2

Los administradores pueden crear cuentas de usuario y funciones para proporcionar acceso a la interfaz web de vRealize Log Insight.

Solamente los usuarios con el permiso Editar administración pueden crear y editar cuentas de usuario. No obstante, los usuarios pueden cambiar su propio correo electrónico y contraseña de cuenta sin necesidad del permiso Editar administración.

Este capítulo cubre los siguientes temas:

- [Descripción general de administración de usuarios](#)
- [Control de acceso basado en funciones](#)
- [Crear una cuenta de usuario nueva en vRealize Log Insight](#)
- [Configurar el acceso de VMware Identity Manager a los grupos de Active Directory para vRealize Log Insight](#)
- [Importar un grupo de Active Directory a vRealize Log Insight](#)
- [Autenticar usuarios con la pertenencia a grupos de dominios múltiples](#)
- [Definir un conjunto de datos](#)
- [Crear y modificar funciones](#)
- [Eliminar una cuenta de usuario de vRealize Log Insight](#)

Descripción general de administración de usuarios

Los administradores del sistema utilizan una combinación de inicios de sesión del usuario, control de acceso basado en la función, permisos y conjuntos de datos para administrar los usuarios de vRealize Log Insight. El control de acceso basado en funciones permite a los administradores administrar los usuarios y las tareas que pueden desempeñar.

Las funciones son grupos de permisos que se requieren para realizar tareas en particular. Los administradores del sistema definen las funciones como parte de las directivas de seguridad de definición y conceden las funciones a los usuarios. Para modificar los permisos y las tareas asociadas a una función en particular, el administrador del sistema actualiza la configuración de la función. Los parámetros actualizados entran en vigencia para todos los usuarios relacionados con la función.

- Para permitir a un usuario realizar una tarea, el administrador del sistema concede la función al usuario.
- Para evitar que un usuario realice una tarea, el administrador del sistema deroga la función del usuario.

La administración del acceso, las funciones y los permisos para cada usuario se basa en la cuenta de inicio de sesión de su usuario. Es posible conceder a cada usuario varios permisos y funciones.

Cuando hay usuarios que no pueden visualizar ciertos objetos, acceder a ciertos objetos o efectuar ciertas operaciones, esto se debe a que no recibieron los permisos pertinentes.

Control de acceso basado en funciones

El control de acceso basado en la función permite a los administradores del sistema controlar el acceso del usuario a vRealize Log Insight y controlar las tareas que los usuarios pueden realizar una vez que inician sesión. Para implementar el control de acceso basado en la función, los administradores del sistema relacionan o revocan permisos y funciones con o desde las cuentas de inicio de sesión del usuario

Usuarios

Los administradores del sistema pueden controlar el acceso y las acciones de cada usuario al conceder o derogar permisos y funciones hacia o desde la cuenta de inicio de sesión del usuario.

Permisos

Los permisos controlan las acciones admitidas en vRealize Log Insight. Los permisos se aplican a tareas de usuario o administrativas particulares en vRealize Log Insight. Por ejemplo, puede conceder el permiso **Vista Administrador** para permitir que un usuario visualice los ajustes administrativos de vRealize Log Insight.

Conjuntos de datos Los conjuntos de datos constan de un conjunto de filtros. Puede utilizar los datos para brindar a los usuarios acceso al contenido específico al asociar un conjunto de datos con una función.

Funciones Las funciones son conjuntos de permisos y conjuntos de datos que pueden asociarse con los usuarios. Las funciones proporcionan una manera conveniente de empaquetar todos los permisos necesarios para realizar una tarea. Un usuario puede tener asignadas funciones múltiples.

Crear una cuenta de usuario nueva en vRealize Log Insight

Los usuarios a los que se otorga la función de superadministrador pueden crear cuentas de usuario para proporcionar acceso a la interfaz de usuario web de vRealize Log Insight.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Verifique que configuró la compatibilidad con VMware Identity Manager o Active Directory si está creando cuentas de usuario que usan alguno de estos tipos de autenticación. Consulte [Habilitar la autenticación de usuario a través de VMware Identity Manager](#) y [Habilitar la autenticación de usuarios a través de Active Directory](#)

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Haga clic en **Usuarios y grupos**.
- 4 Click **New User**.
- 5 Seleccione una opción del menú desplegable **Autenticación**.
 - Si está utilizando la autenticación integrada predeterminada, introduzca un nombre de usuario, una contraseña y, de forma opcional, una dirección de correo electrónico. Copie la contraseña desde el cuadro de texto **Contraseña** y proporciónela al usuario.
 - Si está utilizando la autenticación de Active Directory o de VMware Identity Manager, introduzca el dominio al que el usuario pertenece, el nombre de usuario y, de forma opcional, la dirección de correo electrónico de la cuenta del nombre de usuario.

6 From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
User	Users can access the full functionality of vRealize Log Insight. You can view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage your own user accounts to change a password or email address. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack from the Marketplace. However, you can import a content pack into your own user space which is visible only to you.
Dashboard User	Dashboard users can only use the Dashboards page of vRealize Log Insight.
View Only Admin	View Admin users can view Admin information, have full User access, and can edit Shared content.
Super Admin	Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.

7 Haga clic en **Guardar**.

- En la autenticación integrada, la información se guarda de forma local.
- En la autenticación VMware Identity Manager, vRealize Log Insight verifica si VMware Identity Manager se sincroniza con el grupo especificado y su dominio. Si no se puede encontrar el grupo, un cuadro de diálogo le informará que vRealize Log Insight no puede verificar ese grupo. Puede guardar el grupo sin verificación o cancelar y corregir el dominio o el nombre del grupo.

Configurar el acceso de VMware Identity Manager a los grupos de Active Directory para vRealize Log Insight

Puede usar grupos de Active Directory con vRealize Log Insight a través de la autenticación de Single Sign-On de VMware Identity Manager. El sitio debe configurarse para la autenticación de VMware Identity Manager que está habilitada para la compatibilidad con Active Directory y deben existir la sincronización del servidor.

También debe importar información del grupo a vRealize Log Insight

Un usuario de VMware Identity Manager hereda las funciones que se asignan a cualquier grupo al que pertenece el usuario además de las funciones que se asignan al usuario individual. Por ejemplo, un administrador puede asignar al GrupoA la función de **Vista Administrador** y asignar al usuario Bob la función de **Usuario**. Bob también puede ser asignado al GrupoA. Cuando Bob inicia sesión, hereda la función del grupo y tiene privilegios para las funciones **Vista Administrador** y **Usuario**.

Este no es un grupo local de VMware Identity Manager, sino un grupo de Active Directory que se sincronizó con VMware Identity Manager.

Prerequisitos

- Verifique que haya configurado el atributo UPN (userPrincipalName). Se puede configurar a través de la interfaz de administrador de VMware Identity Manager en **Administración de acceso e identidad > Atributos de usuario**.

- Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight como usuario con permiso **Editar administrador**. El formato de la dirección URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight.
- Verifique que haya configurado la compatibilidad con VMware Identity Manager en vRealize Log Insight. Consulte [Habilitar la autenticación de usuario a través de VMware Identity Manager](#)

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Users and Groups**.
- 4 Diríjase a la tabla Grupos de directorios y haga clic en **Nuevo grupo**.
- 5 Seleccione **VMware Identity Manager** en el menú desplegable **Tipo**.

El nombre de dominio predeterminado que especificó al configurar la compatibilidad con VMware Identity Manager aparecerá en el cuadro de texto **Dominio**.

- 6 Cambie el nombre de dominio al nombre del grupo de Active Directory.
- 7 Introduzca el nombre del grupo que desea añadir.
- 8 From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
User	Users can access the full functionality of vRealize Log Insight. You can view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage your own user accounts to change a password or email address. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack from the Marketplace. However, you can import a content pack into your own user space which is visible only to you.
Dashboard User	Dashboard users can only use the Dashboards page of vRealize Log Insight.
View Only Admin	View Admin users can view Admin information, have full User access, and can edit Shared content.
Super Admin	Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.

- 9 Haga clic en **Guardar**.

vRealize Log Insight verifica si VMware Identity Manager se sincroniza con el grupo especificado y su dominio. Si no se puede encontrar el grupo, un cuadro de diálogo le informará que vRealize Log Insight no puede verificar ese grupo. Puede guardar el grupo sin verificación o cancelar y corregir el dominio o el nombre del grupo.

Los usuarios que pertenecen al grupo que añadió pueden usar su cuenta de VMware Identity Manager para iniciar sesión en vRealize Log Insight y tener el mismo nivel de permisos que el grupo al que pertenecen.

Importar un grupo de Active Directory a vRealize Log Insight

En vez de añadir usuarios de dominio individuales, puede añadir grupos de dominio para permitir que los usuarios inicien sesión en vRealize Log Insight.

When you enable AD support in vRealize Log Insight, you configure a domain name and provide a binding user that belongs to the domain. vRealize Log Insight uses the binding user to verify the connection to the AD domain, and to verify the existence of AD users and groups.

Los grupos de Active Directory que añade a vRealize Log Insight deben pertenecer al dominio del usuario vinculado o bien a un dominio de confianza para el dominio del usuario vinculado.

Un usuario de Active Directory hereda las funciones que se asignan a cualquier grupo al que pertenece el usuario además de las funciones que se asignan al usuario individual. Por ejemplo, un administrador puede asignar al GrupoA la función de **Vista Administrador** y asignar al usuario Bob la función de **Usuario**. Bob también puede ser asignado al GrupoA. Cuando Bob inicia sesión, hereda la función del grupo y tiene privilegios para las funciones **Vista Administrador** y **Usuario**.

Prerequisitos

- Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight como usuario con permiso **Editar administrador**. El formato de la dirección URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight.
- Compruebe que configuró el soporte de AD. Consulte [Habilitar la autenticación de usuarios a través de Active Directory](#)

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Users and Groups**.
- 4 En Grupos de directorios, haga clic en **Nuevo grupo**.
- 5 En el menú desplegable **Tipo**, haga clic en Active Directory.

El nombre de dominio predeterminado que especificó al configurar la compatibilidad con Active Directory aparecerá en el cuadro de texto **Dominio**. Si va a añadir grupos desde el dominio predeterminado, no modifique el nombre del dominio.

- 6 (Opcional) Si desea añadir un grupo desde un dominio que confía en el dominio predeterminado, escriba el nombre del dominio que otorga la confianza en el cuadro de texto **Dominio**.

- 7 Introduzca el nombre del grupo que desea añadir.
- 8 From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
User	Users can access the full functionality of vRealize Log Insight. You can view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage your own user accounts to change a password or email address. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack from the Marketplace. However, you can import a content pack into your own user space which is visible only to you.
Dashboard User	Dashboard users can only use the Dashboards page of vRealize Log Insight.
View Only Admin	View Admin users can view Admin information, have full User access, and can edit Shared content.
Super Admin	Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.

- 9 Haga clic en **Guardar**.

vRealize Log Insight verifica si el grupo de AD existe en el dominio especificado o en un dominio que otorga la confianza. Si no se puede encontrar el grupo, un cuadro de diálogo le informará que vRealize Log Insight no puede verificar ese grupo. Puede guardar el grupo sin verificación o cancelar y corregir el nombre del grupo.

Los usuarios que pertenecen al grupo de Active Directory que añadió pueden usar su cuenta de dominio para iniciar sesión en vRealize Log Insight y tener el mismo nivel de permisos que el grupo al que pertenecen.

Autenticar usuarios con la pertenencia a grupos de dominios múltiples

Los administradores tienen dos maneras de habilitar a los usuarios de otro dominio de confianza para autenticarse en vRealize Log Insight.

- Agregue manualmente a cada usuario.
- Configure un grupo en el mismo dominio que los usuarios y agregue el grupo.

Definir un conjunto de datos

Puede definir un conjunto de datos para brindar a los usuarios acceso a contenidos específicos.

Las restricciones basadas en texto no son compatibles con los conjuntos de datos.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Data Sets**.
- 4 Haga clic en **Nuevo conjunto de datos**.
- 5 Haga clic en **Añadir filtro**.
- 6 Use el primer menú desplegable para seleccionar cualquier campo definido dentro de vRealize Log Insight.

Por ejemplo, **hostname**.

La lista incluye todos los campos definidos disponibles estáticamente, en paquetes de contenido y en contenido personalizado.

NOTA: Los campos numéricos contienen los operadores adicionales =, >, <, >= y <=, que los campos de cadena no contienen. Estos operadores realizan comparaciones numéricas. Usarlos devuelve resultados diferentes que al usar operadores de cadenas. Por ejemplo, el filtro **response_time = 02** coincide con un evento que incluye un campo **response_time** con un valor 2. El filtro **response_time contains 02** no tiene la misma concordancia.

- 7 Use el segundo menú desplegable para seleccionar la operación que se debe aplicar al campo seleccionado en el primer menú desplegable.

Por ejemplo, seleccione **contains**. El filtro **contains** se corresponde con tokens completos: la búsqueda de la cadena "err" no devuelve "error" como resultado.

- 8 En el cuadro de texto que está a la derecha del menú desplegable del filtro, introduzca el valor que desea usar como filtro.

Puede usar múltiples valores. El operador entre estos valores es OR.

NOTA: El cuadro de texto no está disponible si selecciona el operador **exists** en el segundo menú desplegable.

- 9 (Opcional) Para añadir más filtros, haga clic en **Añadir filtro**.
- 10 Click **Save**.

Qué hacer a continuación

Asocie un conjunto de datos con una función de usuario. Consulte [Crear y modificar funciones](#).

Crear y modificar funciones

Puede crear funciones personalizadas o modificar funciones predefinidas para permitir que los usuarios lleven a cabo determinadas tareas y accedan a contenidos específicos.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Roles**.
- 4 Haga clic en **Nueva función** o en  para editar una función existente.
Primero debe clonar las funciones de superadministrador y de usuario antes de poder editarlas.
- 5 Modifique los cuadros de texto **Nombre** y **Descripción**.
- 6 Seleccione uno o más permisos de la lista de Permisos.

Opción	Descripción
Editar administrador	Puede editar la información y la configuración del administrador
Vista Administrador	Puede ver la información y la configuración del administrador
Editar compartido	Puede editar contenido compartido
Análisis	Puede utilizar Análisis interactivo
Panel de control	Puede ver los paneles de control

- 7 (Opcional) En la lista **Conjuntos de datos** que está a la derecha, seleccione un conjunto de datos para asociar con la función de usuario.
- 8 Click **Save**.

Eliminar una cuenta de usuario de vRealize Log Insight

Puede eliminar cuentas de usuarios usando la interfaz de usuario de administración de vRealize Log Insight.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Users and Groups**.
- 4 Seleccione la casilla de verificación junto al nombre de usuario que desea eliminar.
- 5 Haga clic en el icono **Eliminar** .

Configurar la autenticación

Puede utilizar varios métodos de autenticación con su implementación.

Los métodos de autenticación incluyen la autenticación local, la autenticación de VMware Identity Manager y la autenticación de Active Directory. Puede usar más de un método en la misma implementación; los usuarios, posteriormente, seleccionarán el tipo de autenticación al iniciar sesión.

vRealize Log Insight incluye una versión de vRealize Log Insight disponible en la página de descarga del producto que incluye el siguiente conjunto de funciones:

- Integración del directorio para autenticar a los usuarios en directorios existentes, como Active Directory o LDAP.
- Integración de inicio de sesión único con otros productos de VMware que también admiten la funcionalidad de Single Sign-On
- Single Sign-On con varios proveedores de identidades terceros, como ADFS, Ping Federate y otros.
- Autenticación de dos factores mediante la integración con software de terceros, como RSA SecurID, Entrust y otros. No se incluye la autenticación de dos factores con VMware Verify.

La autenticación local es un componente de vRealize Log Insight. Para usarla, debe crear un usuario y una contraseña locales que se almacenan en el servidor vRealize Log Insight. Un administrador de productos debe habilitar vRealize Log Insight y Active Directory.

Este capítulo cubre los siguientes temas:

- [Habilitar la autenticación de usuario a través de VMware Identity Manager](#)
- [Habilitar la autenticación de usuarios a través de Active Directory](#)

Habilitar la autenticación de usuario a través de VMware Identity Manager

Cuando un administrador lo habilita, la autenticación de VMware Identity Manager se puede usar con vRealize Log Insight.

Con la autenticación de VMware Identity Manager, los usuarios pueden usar Single Sign-On en todos los productos VMware que usan el mismo Identity Manager.

Los usuarios de Active Directory también se autentican a través de VMware Identity Manager cuando se sincronizan los servidores de VMware Identity Manager y de Active Directory. Consulte la documentación de VMware Identity Manager para obtener más información sobre la sincronización.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Configuración, haga clic en **Autenticación**.
- 3 Seleccione **Habilitar Single Sign-On**.
- 4 En el cuadro de texto **Host**, introduzca un identificador de host para la instancia de VMware Identity Manager que se utiliza para autenticar usuarios.

Por ejemplo, `company-name.vmwareidentity.com`.
- 5 En el cuadro de texto **Puerto de API**, especifique el puerto que se utilizará para conectarse a la instancia de VMware Identity Manager. El predeterminado es 443.
- 6 De forma opcional, introduzca el VMware Identity Manager arrendatario. Esto es obligatorio solo si el modo del arrendatario está configurado en VMware Identity Manager como una ruta integrada en el arrendatario.
- 7 Especifique las credenciales de usuario de VMware Identity Manager en los cuadros de texto **Nombre de usuario** y **Contraseña**.

Esta información solo se utiliza una vez durante la configuración para crear un cliente vRealize Log Insight en VMware Identity Manager y no se almacena de forma local en vRealize Log Insight. El usuario debe tener permiso para ejecutar los comandos API en el arrendatario.
- 8 Haga clic en **Comprobar conexión** para verificar que la conexión funciona.
- 9 En el menú desplegable **Redireccionar host de URL**, seleccione el Nombre de host o la IP que se utilizarán en la URL de redireccionamiento para registrarlos en VMware Identity Manager.

Si al menos una IP virtual está definida por el equilibrador de carga integrado, VMware Identity Manager realizará el redireccionamiento a la VIP seleccionada. Si el equilibrador de carga integrado no está configurado, se usa en su lugar la dirección IP del nodo principal.
- 10 Seleccione si desea permitir que el inicio de sesión para los usuarios de Active Directory se pueda realizar a través de VMware Identity Manager.

Puede usar esta opción para los usuarios de Active Directory cuando VMware Identity Manager se sincroniza con esa instancia de Active Directory.
- 11 Click **Save**.

Habilitar la autenticación de usuarios a través de Active Directory

Puede autenticar usuarios mediante Active Directory. Esto simplifica el proceso de inicio de sesión de los usuarios, ya que les permite usar una contraseña común para varios fines.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Configuración, haga clic en **Autenticación**.
- 3 Seleccione **Habilitar compatibilidad con Active Directory**.
- 4 En el cuadro de texto **Dominio predeterminado**, escriba un nombre de dominio.

Por ejemplo, `company-name.com`.

NOTA: No puede enumerar varios dominios en el cuadro de texto del dominio predeterminado. Si el dominio predeterminado que especifica es de confianza para otros dominios, vRealize Log Insight usa el dominio predeterminado y el usuario vinculante para verificar que los usuarios y grupos de AD en los dominios de confianza.

Si cambia a un dominio diferente que ya incluye usuarios y grupos, la autenticación fallará para los usuarios y grupos existentes, y los datos guardados por los usuarios existentes se perderán.

- 5 Si tiene controladores de dominio localizados geográficamente o con restricción de seguridad, especifique manualmente aquellos controladores que estén más cerca de esta instancia de vRealize Log Insight.

NOTA: No se admiten servidores de autorización de Active Directory de carga equilibrada.

- 6 Introduzca las credenciales de un usuario vinculante que pertenece al dominio predeterminado.
vRealize Log Insight usa el dominio predeterminado y el usuario vinculante para verificar usuarios y grupos de AD en el dominio predeterminado, y en dominios que confían en el dominio predeterminado.
- 7 Especifique los valores para el tipo de conexión.
Esta conexión se utiliza para la autenticación de Active Directory.
- 8 Click **Save**.

Qué hacer a continuación

Proporcione permisos a usuarios y grupos de AD para acceder a la instancia actual de vRealize Log Insight.

Configurar el protocolo que se usará para Active Directory

Puede configurar el protocolo para usar cuando se conecta a Active Directory. De forma predeterminada, cuando vRealize Log Insight se conecta a Active Directory, primero intenta LDAP SSL y luego LDAP sin SSL, si fuera necesario.

Si desea limitar la comunicación de Active Directory con un protocolo en particular, o desea cambiar el orden de los protocolos que se intentan, debe aplicar configuraciones adicionales en el dispositivo virtual de vRealize Log Insight.

Prerequisitos

- Verifique que tiene las credenciales del usuario raíz para iniciar sesión en el dispositivo virtual de vRealize Log Insight. Consulte [Configurar la contraseña SSH raíz para el dispositivo virtual vRealize Log Insight](#)
- Para habilitar conexiones SSH, verifique que el puerto 22 de TCP esté abierto.

Procedimiento

- 1 Establezca una conexión SSH con el dispositivo virtual de vRealize Log Insight e inicie sesión como usuario raíz.
- 2 Desplácese a la siguiente ubicación: `/storage/var/loginsight/config`
- 3 Localice el último archivo de configuración, donde [número] es el más grande: `/storage/core/loginsight/config/loginsight-config.xml#[number]`
- 4 Copie el último archivo de configuración: `/storage/core/loginsight/config/loginsight-config.xml#[number]`
- 5 Aumente [número] y guarde en la siguiente ubicación: `/storage/core/loginsight/config/loginsight-config.xml#[number + 1]`
- 6 Abra el archivo para edición.
- 7 En la sección Authentication, añada la línea que corresponda a la configuración que desea aplicar:

Opción	Descripción
<code><ad-protocols value="LDAP" /></code>	Para usar específicamente LDAP sin SSL
<code><ad-protocols value="LDAPS" /></code>	Para usar específicamente LDAP con SSL solamente

Opción	Descripción
<code><ad-protocols value="LDAP, LDAPS" /></code>	Para usar específicamente LDAP primero y luego usar LDAP con SSL
<code><ad-protocols value="LDAPS, LDAP" /></code>	Para usar específicamente LDAPS primero y luego usar LDAP sin SSL

Cuando no selecciona un protocolo, vRealize Log Insight intenta usar LDAP primero y luego LDAP con SSL.

- 8 Guarde y cierre el archivo.
- 9 Ejecute el comando `service loginsight restart`.

4

Configurar vRealize Log Insight

Puede configurar y personalizar vRealize Log Insight para cambiar la configuración predeterminada, la configuración de redes y modificar los recursos de almacenamiento. También puede configurar las notificaciones del sistema.

Este capítulo cubre los siguientes temas:

- [vRealize Log Insight Límites de configuración](#)
- [Configurar las opciones del dispositivo virtual](#)
- [Asigne una licencia permanente a vRealize Log Insight](#)
- [Directiva de almacenamiento de registros](#)
- [Administrar notificaciones del sistema](#)
- [Añadir destino de reenvío de eventos de vRealize Log Insight](#)
- [Sincronice la hora en el dispositivo virtual de vRealize Log Insight](#)
- [Configurar el servidor SMTP para vRealize Log Insight](#)
- [Instalar un certificado SSL personalizado](#)
- [Cambiar el período de tiempo de espera predeterminado para las sesiones web de vRealize Log Insight](#)
- [Archivos](#)
- [Reinicie el servicio de vRealize Log Insight](#)
- [Apagar el dispositivo virtual de vRealize Log Insight](#)
- [Descargar un paquete de soporte de vRealize Log Insight](#)
- [Unirse al Programa de mejora de la experiencia de cliente o abandonarlo](#)

vRealize Log Insight Límites de configuración

Cuando configura vRealize Log Insight, debe permanecer en el nivel de los valores máximos admitidos, o por debajo de ellos.

Tabla 4-1. vRealize Log Insight Máximos de configuración

Elemento	Máxima
Configuración de nodos	
CPU	16 vCPU
Memoria	32 GB
Dispositivo de almacenamiento (vmdk)	2 TB - 512 bytes
Almacenamiento total abordable	4 TB (unidad de + OS) Un almacenamiento de registro abordable de 4 TB máximo en VMDK, con un tamaño máximo de 2 TB cada uno. Puede tener dos VMDK de 2TB o cuatro de 1 TB, etc. Cuando llegue al máximo permitido, debe migrar a un tamaño de clúster mayor en vez de añadir más discos a la máquina virtual existente.
Conexiones de syslog	750
Configuración del clúster	
Nodos	12 (principal + 11 de trabajador)
Consumo por nodo	
Eventos por segundo	15 000 eps
Longitud de mensajes de syslog	10 KB (campo de texto)
Solicitud de API HTTP POST de consumo	16 KB (campo de texto); 4 MB por solicitud HTTP POST
Integraciones	
vRealize Operations Manager	1
vSphere vCenter Server	10
Dominios de Active Directory	1
Servidores de correo electrónico	1
Servidores DNS	2
Servidores NTP	4
Reenviadores	10

Configurar las opciones del dispositivo virtual

Puede modificar la configuración del dispositivo virtual, incluida la capacidad de almacenamiento y la memoria o la capacidad de la CPU.

Configurar la contraseña SSH raíz para el dispositivo virtual vRealize Log Insight

De forma predeterminada, la conexión SSH al dispositivo virtual está deshabilitada. Puede configurar la contraseña SSH raíz desde VMware Remote Console o cuando implemente el dispositivo virtual vRealize Log Insight.

Como práctica recomendada, establezca la contraseña SSH raíz cuando implemente el archivo .ova de vRealize Log Insight. Para obtener más información, consulte [Implementar el dispositivo virtual vRealize Log Insight](#).

También puede habilitar SSH y establecer la contraseña raíz desde VMware Remote Console.

Prerequisitos

Compruebe que el dispositivo virtual vRealize Log Insight esté implementado y en funcionamiento.

Procedimiento

- 1 En el inventario de vSphere Client, haga clic en el dispositivo virtual vRealize Log Insight y abra la pestaña **Consola**.
- 2 Diríjase a una línea de comandos siguiendo la combinación de teclas especificadas en la pantalla de presentación.
- 3 En la consola, introduzca **root** y presione Entrar. Deje la contraseña vacía y presione Entrar.
Aparecerá el siguiente mensaje en la consola: `Se solicita cambiar la contraseña. Elija una contraseña nueva.`
- 4 Deje la antigua contraseña vacía y presione Entrar.
- 5 Escriba una nueva contraseña para el usuario raíz, presione Entrar, vuelva a escribir la nueva contraseña para el usuario raíz y presione Entrar.

La contraseña debe contener al menos ocho caracteres y debe incluir al menos una letra mayúscula, una letra minúscula, un dígito y un carácter especial. No puede repetir el mismo carácter más de cuatro veces.

Aparecerá el siguiente mensaje: `Se cambió la contraseña.`

Qué hacer a continuación

Puede usar la contraseña raíz para establecer conexiones SSH con el dispositivo virtual vRealize Log Insight.

Cambiar la configuración de redes de la vApp vRealize Log Insight

Puede cambiar la configuración de redes del dispositivo virtual vRealize Log Insight editando las propiedades de vApp en vSphere Client.

Prerequisitos

Compruebe que posee los permisos para editar las propiedades de vApp.

Procedimiento

- 1 Apague la vApp vRealize Log Insight.
- 2 En el inventario, haga clic con el botón derecho en la vApp vRealize Log Insight y seleccione **Editar configuración**.
- 3 Haga clic en la pestaña **Opciones** y seleccione **Opciones de vApp > Directiva de asignación de IP**.
- 4 Seleccione una opción de asignación de IP.

Opción	Descripción
Fija	Las direcciones IP se configuran manualmente. No se realiza ninguna asignación automática.
Transitoria	Las direcciones IP se asignan automáticamente usando grupos de IP desde un rango especificado cuando la vApp está encendida. Las direcciones IP se liberan cuando el dispositivo se apaga.
DHCP	Un servidor DHCP se utiliza para asignar las direcciones IP. Las direcciones asignadas por el servidor DHCP son visibles en los entornos OVF de las máquinas virtuales que se inician en la vApp.

- 5 (Opcional) Si selecciona **Fija**, haga clic en **Opciones de vApp > Propiedades** y asigne una dirección IP, máscara de red, puerta de enlace, DNS y nombre de host para la vApp vRealize Log Insight.

ADVERTENCIA: No especifique más de dos servidores de nombre de dominio. Si especifica más de dos servidores de nombre de dominio, todos los servidores de nombre de dominio configurados serán ignorados en el dispositivo virtual vRealize Log Insight.

- 6 Encienda la vApp vRealize Log Insight.

Aumentar la capacidad de almacenamiento del dispositivo virtual de vRealize Log Insight

Puede aumentar los recursos de almacenamiento asignados a vRealize Log Insight a medida que se incrementen sus necesidades.

Aumente el espacio de almacenamiento añadiendo un nuevo disco virtual al dispositivo virtual de vRealize Log Insight. Puede agregar tantos discos como necesite, hasta un total de almacenamiento abordable de 4 TB (+ unidad de SO). El total puede ser una combinación de dos discos de 2 TB, cuatro de 1 TB u otras combinaciones. Consulte [vRealize Log Insight Límites de configuración](#).

Prerequisitos

- Log in to the vSphere Client as a user who has privileges to modify the hardware of virtual machines in the environment.
- Desconecte el dispositivo virtual de vRealize Log Insight de manera segura. Consulte [Apagar el dispositivo virtual de vRealize Log Insight](#)

Procedimiento

- 1 In the vSphere Client inventory, right-click the vRealize Log Insight virtual machine and select **Edit Settings**.
- 2 On the **Hardware** tab, click **Add**.
- 3 Seleccione **Disco duro** y haga clic en **Siguiente**.

4 Seleccione **Crear un nuevo disco virtual** y haga clic en **Siguiente**.

- a Escriba la capacidad de disco.

vRealize Log Insight admite discos duros virtuales de hasta 2 TB. Si necesita más capacidad, añada más de un disco duro virtual.

- b Seleccione un formato de disco.

Opción	Descripción
Aprovisionamiento grueso sin escritura de ceros	Crea un disco virtual en el formato grueso predeterminado. El espacio requerido para el disco virtual se asigna cuando se crea el disco virtual. Los datos del dispositivo físico no se borran durante la creación, sino que se reducen a cero en la primera escritura desde el dispositivo virtual según demanda.
Aprovisionamiento grueso con escritura de ceros	Crea un tipo de disco virtual grueso compatible con características de agrupación de clústeres como Fault Tolerance (Tolerancia a errores). El espacio requerido para el disco virtual se asigna al momento de la creación. En comparación con la falta de formato, los datos que residen en el dispositivo físico se escriben en cero cuando se crea el disco virtual. Crear discos con este formato puede requerir mucho más tiempo que hacerlo con otros tipos. Cree discos de aprovisionamiento grueso con escritura de ceros siempre que sea posible para alcanzar un mejor rendimiento y operación del dispositivo virtual de vRealize Log Insight.
Aprovisionamiento fino	Crea un disco en formato fino. Utilice este formato para ahorrar espacio de almacenamiento.

- c Para seleccionar un almacén de datos, examine la ubicación del almacén de datos y haga clic en **Siguiente**.

5 Acepte el nodo del dispositivo virtual predeterminado y haga clic en **Siguiente**.

6 Review the information and click **Finish**.

7 Click **OK** to save your changes and close the dialog box.

Cuando encienda el dispositivo virtual de vRealize Log Insight, la máquina virtual descubre el disco virtual nuevo y lo añade automáticamente al volumen de datos predeterminado. Primero, desconecte completamente la máquina virtual. Para obtener más información sobre cómo encender dispositivos virtuales, consulte <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html>.

ADVERTENCIA: Después de añadir un disco al dispositivo virtual, no puede eliminarlo de manera segura. Eliminar discos del dispositivo virtual de vRealize Log Insight puede generar la pérdida completa de los datos.

Añadir memoria y CPU al dispositivo virtual vRealize Log Insight

Puede cambiar la cantidad de memoria y CPU asignadas a un dispositivo virtual vRealize Log Insight tras la implementación.

Es posible que deba ajustar la asignación de recursos si, por ejemplo, aumenta la cantidad de eventos en su entorno.

Prerequisitos

- Inicie sesión en vSphere Client como usuario que tiene privilegios para modificar el hardware de máquinas virtuales en el entorno.
- Desconecte el dispositivo virtual de vRealize Log Insight de manera segura. Consulte [Apagar el dispositivo virtual de vRealize Log Insight](#)

Procedimiento

- 1 In the vSphere Client inventory, right-click the vRealize Log Insight virtual machine and select **Edit Settings**.
- 2 On the **Hardware** tab, click **Add**.
- 3 ajuste la cantidad de CPU y de memoria según sea necesario.
- 4 Review the information and click **Finish**.
- 5 Click **OK** to save your changes and close the dialog box.

Cuando encienda el dispositivo virtual vRealize Log Insight, la máquina virtual comenzará a utilizar los nuevos recursos.

Asigne una licencia permanente a vRealize Log Insight

Puede usar vRealize Log Insight únicamente con una clave de licencia válida.

Puede obtener una licencia de evaluación cuando descarga vRealize Log Insight desde el sitio web de VMware. Esta licencia es válida por 60 días. Cuando caduque la licencia de evaluación, deberá asignar una licencia permanente para continuar usando vRealize Log Insight.

Como parte de la interoperabilidad de la solución, los usuarios de VMware NSX o las ediciones Standard, Advanced o Enterprise pueden disponer de la licencia para vRealize Log Insight con su clave de licencia de NSX. Para obtener más información, consulte la documentación de VMware NSX.

Use la sección Administración de la interfaz de usuario web de vRealize Log Insight para revisar el estado de la licencia de vRealize Log Insight y administrar su licencia.

Prerequisitos

- Obtenga una clave de licencia válida de My VMware™.

- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Administración, seleccione **Licencia**.
- 3 En el cuadro de texto **Clave de licencia**, escriba su clave de licencia y haga clic en **Establecer clave**. Si tiene una clave de licencia de VMware NSX, introdúzcala aquí.
- 4 Compruebe que el estado de la licencia sea Activo y que el tipo de licencia y el día de caducidad sean correctos.

Directiva de almacenamiento de registros

El dispositivo virtual vRealize Log Insight utiliza un mínimo de 100 GB de almacenamiento para registros entrantes.

Cuando el volumen de los registros que se importan a vRealize Log Insight alcanza el límite de 100 GB, los mensajes antiguos se retiran de forma automática y periódica basados en el principio "primero en llegar, primero en retirarse". Para preservar los mensajes antiguos, puede habilitar la función de archivo de vRealize Log Insight. Consulte [Habilitar o deshabilitar archivos de datos en vRealize Log Insight](#).

Los datos guardados por vRealize Log Insight son inmutables. Después de importar un registro, no será posible eliminarlo hasta que haya sido retirado automáticamente.

Administrar notificaciones del sistema

vRealize Log Insight incluye notificaciones del sistema integradas sobre la actividad relacionada con el estado de vRealize Log Insight, por ejemplo, si el espacio de disco está casi agotado y se van a eliminar archivos de registro antiguos. Los administradores pueden configurar la frecuencia y el destino de las notificaciones del sistema.

Las notificaciones del sistema le informan de problemas críticos que requieren atención inmediata, le proporcionan advertencias que requieren una respuesta y le informan de las actividades normales del sistema. Estas notificaciones se suspenden durante la actualización, pero funcionan el resto del tiempo.

Un administrador puede especificar la frecuencia con que se envían notificaciones al activarse y a qué direcciones de correo electrónico se mandan. Las notificaciones del sistema relacionadas con vRealize Log Insight también se pueden enviar a aplicaciones de terceros.

No son iguales que las consultas de alerta, que definen los usuarios. Para obtener más información acerca de las consultas de alerta, consulte [Agregar una consulta de alerta en Log Insight para enviar notificaciones por correo electrónico](#).

Notificaciones del sistema de vRealize Log Insight

vRealize Log Insight ofrece dos conjuntos de notificaciones: las generales, que se aplican a todas las configuraciones del producto, y las relacionadas con los clústeres para sus implementaciones.

Las siguientes tablas incluyen y describen las notificaciones del sistema de vRealize Log Insight.

Notificaciones del sistema generales

vRealize Log Insight envía notificaciones cuando las condiciones pueden requerir intervención administrativa, por ejemplo, en los errores de archivo o los retrasos en la programación de alertas.

Nombre de la notificación	Descripción
<p>Pronto no será posible buscar los datos más antiguos</p>	<p>Esta notificación le indica cuándo se espera que vRealize Log Insight comience a retirar datos antiguos del almacenamiento del dispositivo virtual y cuál es el tamaño esperado de los datos disponibles para consulta según la tasa de consumo actual. Los datos rotados se archivan únicamente si se configuró esta opción, o se eliminan si no se configuró. La notificación se envía después de cada reinicio del servicio de vRealize Log Insight.</p>
<p>Tiempo de retención del repositorio</p>	<p>Un período de retención es la cantidad de tiempo durante el cual los datos se mantienen en el disco duro de la instancia de vRealize Log Insight. Un período de retención se determina por la cantidad de datos que puede mantener el sistema y la tasa de consumo actual. Por ejemplo, si recibe 10 GB de datos al día (después de indexar) y cuenta con 300 GB de espacio, la tasa de retención es de 30 días. Cuando se alcanza el límite de almacenamiento, los datos antiguos se eliminarán para permitir el acceso de los datos que se acaban de introducir. Esta notificación le indica cuándo la cantidad de datos disponibles para consulta que vRealize Log Insight puede almacenar según las tasas de consumo actuales supera el espacio de almacenamiento que está disponible en el dispositivo virtual. Los usuarios administradores pueden definir el valor umbral de notificación de almacenamiento. Consulte Configurar vRealize Log Insight para enviar notificaciones de estado.</p>

Nombre de la notificación	Descripción
Eventos descartados	<p>Esta notificación le indica que vRealize Log Insight no pudo consumir todos los mensajes entrantes de registro.</p> <ul style="list-style-type: none"> ■ Si se descartan los mensajes TCP, según el seguimiento del servidor de vRealize Log Insight, se enviará una notificación del sistema en ambos casos de la siguiente manera: <ul style="list-style-type: none"> ■ Una vez al día ■ Cada vez que se reinicia el servicio de vRealize Log Insight de forma manual o automática. ■ El correo electrónico contiene el número de mensajes descartados desde que se envió el último correo electrónico de notificación y la cantidad total de mensajes descartados desde que se reinició vRealize Log Insight por última vez. <p>NOTA: La hora de la línea de envío es controlada por el cliente del correo electrónico y está en la zona horaria local, mientras que el cuerpo del correo electrónico muestra el horario UTC.</p>
Sectores de almacenamiento de índice dañados	<p>Esta notificación le indica que parte del índice en disco está dañado. Un índice dañado generalmente indica problemas graves con el sistema de almacenamiento subyacente. La parte dañada del índice quedará excluida de las consultas de servicio. Un índice dañado afecta el consumo de datos nuevos. vRealize Log Insight verifica la integridad del índice cuando se pone en marcha el servicio. Si se detecta algún tipo de daño, vRealize Log Insight envía una notificación del sistema de la siguiente manera:</p> <ul style="list-style-type: none"> ■ Una vez al día ■ Cada vez que se reinicia el servicio de vRealize Log Insight de forma manual o automática.
Sin disco	<p>Esta notificación le indica que vRealize Log Insight se está quedando sin espacio de disco asignado. Esta notificación indica que vRealize Log Insight experimenta problemas de almacenamiento.</p>

Nombre de la notificación	Descripción
Espacio de archivo casi lleno	Esta notificación le indica que está a punto de agotarse el espacio de disco del servidor NFS que se utiliza para archivar datos de vRealize Log Insight.
Cambio en el espacio total del disco	Esta notificación le indica que disminuyó el tamaño total de la partición del almacenamiento de datos de vRealize Log Insight. Generalmente esto indica un problema grave en el sistema de almacenamiento subyacente. Cuando vRealize Log Insight detecta esta condición, envía una notificación de la siguiente manera: <ul style="list-style-type: none"> ■ Inmediatamente ■ Una vez al día
Archivos pendientes	Esta notificación le indica que vRealize Log Insight no puede archivar datos según lo previsto. Suele informar sobre problemas relacionados con el almacenamiento NFS que configuró para archivar datos.
Licencia a punto de caducar	Esta notificación le indica que la licencia de vRealize Log Insight está a punto de caducar.
Caducó la licencia	Esta notificación le indica que la licencia de vRealize Log Insight está caducada.
No se puede conectar con el servidor de AD.	Esta notificación le indica que vRealize Log Insight no puede conectarse al servidor de Active Directory configurado.

Nombre de la notificación	Descripción
<p>No se puede obtener la dirección IP de alta disponibilidad [dirección IP] porque ya está en poder de otra máquina</p>	<p>Esta notificación le indica que el clúster de vRealize Log Insight no pudo obtener la dirección IP configurada para el equilibrador de carga integrado (ILB). El motivo más frecuente para recibir esta notificación es que otro host dentro de la misma red posee la dirección IP; por lo tanto, esta no está disponible para el clúster.</p> <p>Puede resolver este conflicto ya sea liberando la dirección IP del host que la posee actualmente o bien configurando el equilibrador de carga integrado de Log Insight con una dirección IP estática que esté disponible en la red. Al cambiar la dirección IP del ILB, recuerde volver a configurar todos los clientes para que envíen los registros a la nueva dirección IP o a un FQDN/URL que resuelva la dirección IP. También debe anular la configuración de todos los vCenter Server integrados con vRealize Log Insight y volver a configurarlos desde la página de integración de vSphere.</p>
<p>La dirección IP de alta disponibilidad [dirección IP] no está disponible debido a demasiados errores de nodos.</p>	<p>Esta notificación le indica que la dirección IP configurada para el equilibrador de carga integrado (ILB) no está disponible. Esto significa que los clientes que intenten enviar registros a un clúster de vRealize Log Insight mediante la dirección IP del ILB o un FQDN o una URL que lleven a esta dirección IP verán que no está disponible. El motivo más frecuente para que aparezca esta notificación es que la mayoría de los nodos del clúster de vRealize Log Insight no están en buen estado, no están disponibles o no se puede acceder a ellos desde el nodo principal. Otro motivo común es que no se habilitó la sincronización de hora NTP o que los servidores NTP configurados tienen una significativa desviación horaria entre sí. Para confirmar si el problema aún persiste, intente comprobar mediante ping (si está permitido) la dirección IP para verificar que no está accesible.</p> <p>Puede resolver el problema asegurándose de que la mayoría de los nodos del clúster tengan un estado óptimo y estén accesibles, y habilitando la sincronización de hora NTP con servidores NTP precisos.</p>

Nombre de la notificación	Descripción
<p>Demasiadas migraciones de dirección IP de alta disponibilidad [su dirección IP] entre los nodos de vRealize Log Insight</p>	<p>Esta notificación le indica que la dirección IP configurada para el equilibrador de carga integrado (ILB) migró demasiadas veces durante los últimos 10 minutos. En condiciones de funcionamiento normal, la dirección IP raramente se desplaza entre los nodos del clúster de vRealize Log Insight. Sin embargo, la dirección IP podría desplazarse si el nodo del propietario actual se reinicia o se pone en mantenimiento. El otro motivo puede ser falta de sincronización horaria entre los nodos del clúster de Log Insight, que es esencial para el funcionamiento normal del clúster. En este último caso, puede solucionar el problema habilitando la sincronización de hora NTP con servidores NTP precisos.</p>
<p>Error del certificado SSL</p>	<p>Esta notificación le indica que un origen de syslog inició una conexión con vRealize Log Insight a través de SSL, pero la finalizó de forma inesperada. Esto puede indicar que el origen de syslog no pudo confirmar la validez del certificado SSL. Para que vRealize Log Insight acepte mensajes de syslog por medio de SSL, se requiere un certificado validado por el cliente y los relojes del sistema deben estar sincronizados. Puede haber un problema con el certificado SSL o con el servicio de hora de red.</p> <p>Puede validar que el certificado SSL es de confianza en el origen de syslog, volver a configurar el origen para que no use SSL o bien volver a instalar el certificado SSL. Consulte Configurar los parámetros SSL del agente de vRealize Log Insight y Instalar un certificado SSL personalizado.</p>
<p>Error de recopilación de vCenter</p>	<p>Esta notificación le indica que vRealize Log Insight no puede recopilar eventos, tareas ni alarmas de vCenter. Consulte el archivo <code>/storage/var/loginsight/plugins/vsphere/li-vsphere.log</code> para saber qué error concreto provocó que no se pudiera realizar la recopilación y comprobar si la recopilación funciona como debe.</p>

Nombre de la notificación	Descripción
<p>Eventos descartados del reenviador de eventos</p>	<p>Esta notificación del sistema se envía cuando un reenviador descarta eventos a causa de problemas de conexión o de sobrecarga.</p> <p>Ejemplo:</p> <pre data-bbox="1023 401 1445 806"> Log Insight Admin Alert: Event Forwarder Events Dropped This alert is about your Log Insight installation on https://<your_url> Event Forwarder Events Dropped triggered at 2016-08-02T18:41:06.972Z Log Insight just dropped 670 events for forwarder target 'Test', reason: Pending queue is full. </pre>
<p>Consultas de alerta fuera del calendario</p>	<p>Esta notificación le indica que vRealize Log Insight no pudo ejecutar una alerta de usuario en el momento establecido. Este retraso se puede deber a una o más alertas de usuario ineficientes o a que el sistema no cuenta con el tamaño adecuado para el consumo y la carga de consultas.</p>
<p>Alerta deshabilitada automáticamente</p>	<p>Si se ejecutó una alerta al menos diez veces y su tiempo de ejecución medio es superior a una hora, dicha alerta se considera ineficiente y se deshabilita para evitar que afecte a otras alertas de usuario.</p>
<p>Consulta de alerta ineficiente</p>	<p>Si una alerta tarda más de una hora en completarse, se considera ineficiente.</p>

Notificaciones del sistema sobre clústeres

vRealize Log Insight envía notificaciones sobre los cambios en la topología del clúster, por ejemplo, si se agregan nuevos miembros o hay problemas de comunicación transitorios entre los nodos.

Enviado por	Nombre de la notificación	Descripción
Nodo principal	Se requiere aprobación para un nuevo nodo de trabajador	Esta notificación le indica que hay una solicitud de pertenencia de un nodo de trabajador. Un usuario administrador debe aprobarla o rechazarla.
Nodo principal	Nuevo nodo de trabajador aprobado	Esta notificación le indica que un usuario administrador aprobó una solicitud de pertenencia de un nodo de trabajador para unirse a un clúster de vRealize Log Insight.
Nodo principal	Nuevo nodo de trabajador rechazado	Esta notificación le indica que un usuario administrador rechazó una solicitud de pertenencia de un nodo de trabajador para unirse a un clúster de vRealize Log Insight. Si la solicitud se rechazó por error, un usuario administrador puede volver a enviar la solicitud desde el nodo de trabajador y luego aprobarla en el nodo principal.
Nodo principal	Los nodos máximos admitidos excedidos a causa del nodo de trabajador	Esta notificación le indica que la cantidad de nodos de trabajador en el clúster de Log Insight superó el número máximo admitido con un nuevo nodo de trabajador.
Nodo principal	Se han superado los nodos admitidos, se ha rechazado el nuevo nodo de trabajador	Esta notificación le indica que un usuario administrador intentó agregar un número de nodos al clúster superior al máximo admitido, por lo que se rechazó el nodo.
Nodo principal	Nodo de trabajador desconectado	Esta notificación le indica que un nodo de trabajador conectado previamente se desconectó del clúster de vRealize Log Insight.
Nodo principal	Nodo de trabajador conectado de nuevo	Esta notificación le indica que un nodo de trabajador se volvió a conectar al clúster de vRealize Log Insight.
Nodo principal	Nodo de trabajador rechazado por el administrador	Esta notificación le indica que un usuario administrador revocó la pertenencia de un nodo de trabajador y este ya no forma parte del clúster de vRealize Log Insight.

Enviado por	Nombre de la notificación	Descripción
Nodo principal	Nodo de trabajador desconocido rechazado	Esta notificación le indica que el nodo principal de vRealize Log Insight rechazó una solicitud de un nodo de trabajador porque no lo reconoce. Si el nodo de trabajador es un nodo válido y debería añadirse al clúster, inicie sesión en el nodo de trabajador, elimine su archivo token y la configuración del usuario en <code>/storage/core/loginsight/config/</code> y ejecute <code>restart loginsight service</code> en el nodo de trabajador.
Nodo principal	El nodo de trabajador ha entrado al modo de mantenimiento	Esta notificación le indica que un nodo de trabajador se puso en modo de mantenimiento y un usuario administrador debe desactivar este modo en el nodo de trabajador para que pueda recibir cambios de configuración y contestar consultas.
Nodo principal	El nodo de trabajador ha regresado al servicio	Esta notificación le indica que un nodo de trabajador salió del modo de mantenimiento y volvió al servicio.
Nodo de trabajador	Principal con error o desconectado del nodo de trabajador	Esta notificación le indica que un nodo de trabajador que envía la notificación no se puede comunicar con el nodo principal de vRealize Log Insight. Esto puede indicar que el nodo principal ha fallado y quizás deba reiniciarse. Si el nodo principal falló, no es posible configurar el clúster y no se pueden enviar las consultas hasta que esté nuevamente en línea. Los nodos de trabajador continúan consumiendo mensajes. NOTA: Es posible que reciba un gran número de este tipo de notificaciones debido a que muchos nodos de trabajo pueden detectar el error del nodo principal de forma independiente y generar notificaciones.
Nodo de trabajador	Nodo principal conectado al nodo de trabajador	Esta notificación le indica que un nodo de trabajador que envía la notificación se volvió a conectar al nodo principal de vRealize Log Insight.

Configurar las notificaciones del sistema de vRealize Log Insight

Como administrador, puede configurar las notificaciones del sistema de vRealize Log Insight para que envíe notificaciones a las aplicaciones de terceros y también correos electrónicos a usuarios específicos cuando se active una notificación.

vRealize Log Insight genera estas notificaciones cuando ocurre un evento importante del sistema, por ejemplo cuando el espacio en disco está casi agotado y vRealize Log Insight debe comenzar a eliminar o archivar los archivos de registro antiguos.

Configurar vRealize Log Insight para enviar notificaciones de estado

Un administrador puede configurar vRealize Log Insight para que envíe notificaciones relacionadas con su propio estado.

Si no se puede entregar un mensaje de correo electrónico, se le notificará del error en la interfaz web.

Prerequisitos

- Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.
- Compruebe que el servidor SMTP esté configurado para vRealize Log Insight. Para obtener más información, consulte [Configurar el servidor SMTP para vRealize Log Insight](#).

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Configuration, click **General**.
- 3 En el encabezado Alertas, configure las notificaciones del sistema.
 - a En el cuadro de texto **Enviar notificaciones del sistema por correo electrónico a**, escriba las direcciones de correo electrónico que recibirán las notificaciones.
Use comas para separar varias direcciones de correo electrónico.
 - b Seleccione la casilla de verificación de **Umbral de notificación de retención** y establezca el umbral que activa las notificaciones.

Se enviará una notificación cuando la cantidad de datos que puede contener el sistema sea insuficiente para el periodo de tiempo especificado. Este valor se calcula según la tasa de consumo actual.
- 4 Click **Save**.
- 5 Click **Restart Log Insight** to apply your changes.

Configurar las notificaciones de sistema de vRealize Log Insight para productos de terceros

Un administrador puede configurar vRealize Log Insight para que envíe notificaciones relacionadas con su propio estado para aplicaciones de terceros.

vRealize Log Insight genera estas notificaciones cuando ocurre un evento importante del sistema, por ejemplo cuando el espacio en disco está casi agotado y vRealize Log Insight debe comenzar a eliminar los archivos de registro antiguos.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Configuration, click **General**.
- 3 En el encabezado Alertas, configure las notificaciones del sistema.
 - a En el cuadro de texto **Enviar notificaciones del sistema de HTTP Post a**, escriba las direcciones de correo electrónico que recibirán las notificaciones.
 - b (Opcional) Confirme que la casilla **Enviar una notificación cuando la capacidad sea inferior a** y el umbral asociado están configurados correctamente para el entorno.
- 4 Click **Save**.

Qué hacer a continuación

Al trabajar con la salida de webhook de la notificación, cree un shim para asignar el formato del webhook de vRealize Log Insight al formato usado por la aplicación de terceros.

Acerca de usar Webhooks para enviar alertas a productos de terceros

Puede enviar notificaciones del sistema de vRealize Log Insight a productos de terceros usando webhooks.

vRealize Log Insight usa webhooks para enviar alertas por medio de HTTP POST a otras aplicaciones. vRealize Log Insight envía un webhook en su propio formato de propiedad exclusiva y las soluciones de terceros esperan que los webhooks entrantes usen sus propios formatos de propiedad exclusiva. Para usar la información enviada con los webhooks de vRealize Log Insight, la aplicación de terceros debe tener una compatibilidad nativa con el formato vRealize Log Insight o debe crear una asignación con un shim entre los formatos vRealize Log Insight y el formato de terceros. El shim traduce o asigna el formato vRealize Log Insight a un formato diferente.

Las notificaciones del sistema, las alertas que se crean con consultas de mensajes y las alertas creadas con consultas agregadas tienen su propio formato de webhook.

Debe ser administrador de vRealize Log Insight para crear notificaciones de sistema.

Se admite la autenticación HTTP básica. Introduzca las credenciales en la URL utilizando el formulario `{{https://nombredeusuario:contraseña@nombredehost/ruta}}`

Formato de webhook para una notificación del sistema

El formato de un webhook de vRealize Log Insight depende del tipo de consulta desde la que se creó. Las notificaciones del sistema, las consultas de mensajes de alerta y las alertas generadas desde consultas de usuario agregadas tienen su propio formato de webhook.

Debe ser administrador de vRealize Log Insight para configurar que vRealize Log Insight envíe notificaciones del sistema.

Si envía una notificación de sistema a un programa de terceros, debe escribir un shim para que los formatos de dicho programa puedan comprender la información de vRealize Log Insight.

Formato de webhook para notificaciones del sistema

El siguiente ejemplo muestra el formato de webhook de vRealize Log Insight para las notificaciones del sistema.

```
{
  "AlertName": " Admin Alert: Worker node has returned to service (Host = 127.0.0.2)",
  "messages": [
    {
      "text": "This notification was generated from Log Insight node (Host = 127.0.0.2,
Node Identifier = a31cad22-65c2-4131-8e6c-27790892a1f9).
A worker node has returned to service after having been in maintenance mode.
The Log Insight master node reports that worker node has finished maintenance
and exited maintenance mode. The node will resume receiving configuration changes and
serving queries. The node is also now ready to start receiving incoming log messages."

      "timestamp": 1458665320514, "fields": []
    }
  ]
}
```

Añadir destino de reenvío de eventos de vRealize Log Insight

Se puede configurar un servidor de vRealize Log Insight para reenviar los eventos entrantes a un destino de API de consumo o syslog.

Utilice el reenvío de eventos para enviar eventos etiquetados o filtrados a uno o varios destinos remotos como vRealize Log Insight, syslog o ambos. El reenvío de eventos puede utilizarse para admitir las herramientas existentes de registro como SIEM y consolidar el registro a través de redes diferentes como DMZ o WAN.

NOTA: Los reenviadores de eventos pueden ser independientes o estar en un clúster, pero son una instancia independiente del destino remoto. Las instancias configuradas para reenviar los eventos también los almacenan de forma local y se pueden utilizar para consultar datos.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Compruebe que el destino pueda manejar la cantidad de eventos que se reenvían. Si el clúster de destino es mucho más pequeño que la instancia de reenvío, algunos eventos podrían descartarse.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Administración, haga clic en **Reenvío de eventos**.
- 3 Haga clic en **+Nuevo destino** y proporcione la siguiente información.

Opción	Descripción
Nombre	Un nombre único para el nuevo destino.
Host	La dirección IP o el nombre de dominio totalmente calificado.

ADVERTENCIA: Un bucle de reenvío es una configuración en la que el clúster de vRealize Log Insight se reenvía eventos a sí mismo o a otro clúster, que es el que vuelve a reenviarlos al clúster original. Este bucle crea un número indefinido de copias de cada evento de reenvío. La interfaz web de vRealize Log Insight no permite configurar un evento que se reenvíe a sí mismo. Sin embargo, vRealize Log Insight no puede evitar que se produzca un bucle de reenvío indirecto, por ejemplo, que el clúster A de vRealize Log Insight realice un reenvío al clúster B y que este último vuelva a reenviar el mismo evento al clúster A. Cuando cree los destinos de reenvío, preste atención para no crear bucles de reenvío indirectos.

Opción	Descripción
Protocolo	<p>API de consumo o syslog. El valor predeterminado es la API de consumo (CFAPI).</p> <p>Cuando los eventos se reenvían mediante la API de consumo, la fuente original del evento se preserva en el campo de origen. Cuando los eventos se reenvían mediante un syslog, la fuente original del evento se pierde y el receptor puede grabar el origen del mensaje como la dirección IP o el nombre de host del reenviador de vRealize Log Insight.</p> <p>NOTA: El campo de origen puede tener valores diferentes dependiendo del protocolo seleccionado en el reenviador de eventos:</p> <ul style="list-style-type: none"> a Para la API de consumo, el origen es la dirección IP del emisor inicial (el originador del evento). b Para syslog, el origen es la dirección IP de la instancia de vRealize Log Insight del reenviador del evento. Además, el texto del mensaje de syslog contiene <code>_li_source_path</code>, que apunta a la dirección IP del emisor inicial.
Usar SSL	<p>Opcionalmente, puede proteger la conexión con SSL para la API de consumo. La raíz de confianza del servidor remoto se valida y el reenvío de eventos con SSL no funciona con los certificados autofirmados instalados en servidores de destino de forma predeterminada. Si no es de confianza, importe el certificado raíz de confianza del servidor remoto al almacén de claves del reenviador. Consulte Configurar el reenvío de eventos de vRealize Log Insight con SSL.</p>
Etiquetas	<p>Opcionalmente, puede agregar pares de etiquetas con valores predefinidos. Las etiquetas le permiten consultar eventos más fácilmente. Puede añadir múltiples etiquetas separadas por comas.</p>
Reenviar etiquetas complementarias	<p>Puede elegir si desea reenviar etiquetas complementarias para syslog.</p> <p>Las etiquetas complementarias son aquellas que agregó el clúster, por ejemplo, "vc_username" o "vc_vmname" y se pueden reenviar con las etiquetas que proceden directamente de los orígenes. Las etiquetas complementarias siempre se reenvían cuando se utiliza la API de consumo.</p>
Transporte	<p>Seleccione un protocolo de transporte de syslog. Puede elegir UDP o TCP.</p>

4 (Opcional) Para controlar qué eventos se reenvían, haga clic en **+ Añadir filtro**.

Seleccione los campos y las restricciones para definir los eventos deseados. Solo los campos estáticos están disponibles para su uso como filtros. Si no selecciona un filtro, se reenvían todos los eventos. Puede ver los resultados del filtro que está compilando haciendo clic en **Ejecutar en Análisis interactivo**.

Opción	Descripción
coincide	<p>Encuentra las cadenas que coinciden con la cadena especificada y la especificación con caracteres comodín.</p> <p>Por ejemplo, <code>test*</code> coincide con las cadenas como <code>test123</code> o <code>test-run</code>, pero no con <code>my-test-run</code>. <code>test</code> coincide con <code>test</code>, pero no con <code>test123</code>.</p>
no coincide	<p>Excluye las cadenas que coinciden con esa cadena especificada y la especificación con caracteres comodín.</p> <p>Por ejemplo, <code>test*</code> filtra <code>test123</code>, pero no excluye <code>mytest123</code>.</p>

Opción	Descripción
comienza con	Encuentra las cadenas que empiezan por la cadena de caracteres especificada. Por ejemplo, test encuentra test123 o test , pero no my-test123 .
no comienza con	Excluye las cadenas que empiezan por la cadena de caracteres especificada. Por ejemplo, test filtra test123 , pero no excluye my-test123 .

- 5 (Opcional) Haga clic en **Mostrar configuración avanzada** para modificar los siguientes datos de reenvío.

Opción	Descripción
Puerto	El puerto al cual se envían los eventos en el destino remoto. El valor predeterminado se establece en función del protocolo especificado. No lo cambie a menos que el destino remoto escuche en un puerto diferente.
Caché de disco	La cantidad de espacio en disco local que se debe reservar para almacenar en búfer los eventos que se configuran para reenvío. El almacenamiento en búfer se utiliza cuando el destino remoto no está disponible o no puede procesar los eventos que se le envían. Si se llena el búfer local y el destino remoto sigue sin estar disponible, los eventos locales más recientes se descartan y no se reenvían al destino remoto, aunque el destino remoto vuelva a estar en línea. El valor predeterminado es 200 MB.
Número de trabajadores	La cantidad de conexiones salientes simultáneas que se deben usar. Establezca un número de trabajadores más alto para tener una latencia de red más alta en el destino de reenvío y un número más alto de eventos reenviados por segundo. El valor predeterminado es 8.

- 6 Para verificar su configuración, haga clic en **Probar**.

- 7 Haga clic en **Guardar**.

Qué hacer a continuación

- [Configurar el reenvío de eventos de vRealize Log Insight con SSL](#).
- Puede editar o clonar un destino de reenvío de eventos. Si edita el destino para cambiar el nombre de un reenviador de eventos, se restablecen todas las estadísticas.

Configurar el reenvío de eventos de vRealize Log Insight con SSL

Puede configurar un servidor vRealize Log Insight para que reenvíe los eventos entrantes a otro servidor Log Insight mediante un destino API de consumo con SSL.

Prerequisitos

El reenvío de eventos con SSL no funciona con el certificado autofirmado que está instalado en los servidores de destino de forma predeterminada. Usando los pasos que figuran en [Generar una solicitud de firma de certificado](#), se debe crear y luego cargar un certificado SSL personalizado. Consulte [Instalar un certificado SSL personalizado](#)

Procedimiento

- 1 Copie el certificado raíz de confianza en un directorio temporal en la instancia del reenviador. Por ejemplo, /home.
- 2 SSH a la instancia del reenviador y ejecute los siguientes comandos.

```
localhost:~ # cd /usr/java/default/lib/security/
localhost:/usr/java/default/lib/security # ../../bin/keytool
-import -alias loginsight -file /home/cacert.crt -keystore cacerts
```

La contraseña de almacén de claves predeterminada es **changeit**.

NOTA: Las versiones de Java pueden variar con el tiempo.

- 3 Reinicie la instancia de vRealize Log Insight.

Si usa un entorno de clúster de vRealize Log Insight, esta operación se deber realizar en todos los nodos con el mismo certificado.

Qué hacer a continuación

Habilite la conexión SSL. Consulte [Exigir solo conexiones SSL](#).

Sincronice la hora en el dispositivo virtual de vRealize Log Insight

Debe sincronizar la hora en el dispositivo virtual de vRealize Log Insight con un servidor NTP o con el host de ESX/ESXi en el cual implementó el dispositivo virtual.

La hora es esencial a la funcionalidad central de vRealize Log Insight.

De manera predeterminada, vRealize Log Insight sincroniza la hora con una lista predefinida de servidores NTP públicos. Si no es posible acceder a los servidores NTP públicos a causa de un firewall, puede usar el servidor NTP interno de su compañía. Si no hay servidores NTP disponibles, puede sincronizar la hora con el host de ESX/ESXi donde implementó el dispositivo virtual de vRealize Log Insight.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Configuración, haga clic en **Hora**.

- 3 En el menú desplegable **Sinc. hora con**, seleccione el origen de la hora.

Opción	Descripción
Servidor NTP	Sincroniza la hora en el dispositivo virtual de vRealize Log Insight con uno de los servidores NTP de la lista.
Host de ESX/ESXi	Sincroniza la hora en el dispositivo virtual de vRealize Log Insight con el host de ESX/ESXi en el cual implementó el dispositivo virtual.

- 4 (Opcional) Si seleccionó la sincronización con el servidor NTP, enumere las direcciones del servidor NTP y haga clic en **Probar**.

NOTA: Probar la conexión con los servidores NTP puede requerir hasta 20 segundos por servidor.

- 5 Click **Save**.

Configurar el servidor SMTP para vRealize Log Insight

Puede configurar un SMTP para permitir que vRealize Log Insight envíe alertas por correo electrónico.

Las alertas del sistema se generan cuando vRealize Log Insight detecta un evento importante del sistema, por ejemplo, cuando la capacidad de almacenamiento en el dispositivo virtual alcanza los valores del umbral establecidos.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Configuración, haga clic en **SMTP**.
- 3 Escriba la dirección de correo electrónico y el número de puerto del servidor SMTP.
- 4 Si el servidor SMTP usa una conexión cifrada, seleccione el protocolo de cifrado.
- 5 En el cuadro de texto **Emisor**, escriba la dirección de correo electrónico que va a utilizar al enviar alertas de sistema.

La dirección del **Emisor** aparecerá como la dirección de origen en los correos electrónicos de notificación del sistema. No es necesario que sea una dirección real y puede ser algo que represente a la instancia específica de vRealize Log Insight. Por ejemplo, `loginisght@ejemplo.com`.

- 6 Escriba un nombre de usuario y una contraseña para autenticar con el servidor SMTP al enviar alertas de sistema.
- 7 Escriba un correo electrónico de destino y haga clic en **Enviar correo electrónico de prueba** para verificar la conexión.
- 8 Click **Save**.

Instalar un certificado SSL personalizado

De forma predeterminada, vRealize Log Insight instala un certificado SSL autofirmado en el dispositivo virtual.

El certificado autofirmado genera advertencias de seguridad cuando se conecta con la interfaz de usuario web de vRealize Log Insight. Si no desea usar un certificado autofirmado de seguridad, puede instalar un certificado SSL personalizado. La única función que requiere un certificado SSL personalizado es Reenvío de eventos a través de SSL. Si tiene una configuración de clúster con ILB habilitado, consulte [Habilitar el equilibrador de carga integrado](#) para conocer los requisitos específicos de un certificado SSL personalizado.

NOTA: The vRealize Log Insight Web user interface and the Log Insight Ingestion protocol `cfapi` use the same certificate for authentication.

Prerequisitos

- Verify that your custom SSL certificate meets the following requirements.
 - The CommonName contains a wildcard or exact match for the Master node or FQDN of the virtual IP address. Optionally, all other IP addresses and FQDNs are listed as subjectAltName.
 - The certificate file contains both a valid private key and a valid certificate chain.
 - The private key is generated by the RSA or the DSA algorithm.
 - The private key is not encrypted by a pass phrase.
 - If the certificate is signed by a chain of other certificates, all other certificates are included in the certificate file that you plan to import.
 - The private key and all the certificates that are included in the certificate file are PEM-encoded. vRealize Log Insight does not support DER-encoded certificates and private keys.
 - The private key and all the certificates that are included in the certificate file are in the PEM format. vRealize Log Insight does not support certificates in the PFX, PKCS12, PKCS7, or other formats.
- Verifique que concatene todo el cuerpo de cada certificado en un archivo de texto individual en el orden siguiente.
 - a La clave privada: `your_domain_name.key`
 - b El certificado primario: `your_domain_name.crt`
 - c El certificado intermedio: `DigiCertCA.crt`
 - d El certificado raíz: `TrustedRoot.crt`

- Verifique que incluya las etiquetas de inicio y finalización de cada certificado en el siguiente formato.

```

-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----

```

- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

1 Generar un certificado autofirmado

Puede generar un certificado autofirmado para Windows o Linux si usa la herramienta OpenSSL.

2 Generar una solicitud de firma de certificado

Genere una solicitud de firma de certificado usando la herramienta OpenSSL para Windows.

3 Solicitar la firma de una entidad de certificación

Envíe la solicitud de firma de certificado a la Entidad de certificación que elija y solicite una firma.

4 Concatenar archivos de certificados

Combine sus archivos de claves y certificados en un archivo PEM.

5 Cargar certificado firmado

Puede cargar un certificado SSL firmado.

6 Configurar la conexión SSL entre el servidor vRealize Log Insight y los Log Insight Agents

La función SSL le permite proporcionar conexiones SSL únicamente entre los Log Insight Agents y el vRealize Log Insight Server a través del flujo seguro de API de consumo. También puede configurar los diversos parámetros SSL de los Log Insight Agents.

Generar un certificado autofirmado

Puede generar un certificado autofirmado para Windows o Linux si usa la herramienta OpenSSL.

Prerequisitos

- Descargue el instalador correspondiente para OpenSSL de <https://www.openssl.org/community/binaries.html>. Use el instalador de OpenSSL descargado para instalarlo en Windows.

- Edite el archivo `openssl.cfg` para añadir otros parámetros requeridos. Asegúrese de que la sección `[req]` tenga el parámetro `req_extensions` definido.

```
[req]
.
.
req_extensions=v3_req #
```

- Añada una entrada Nombre alternativo del sujeto correspondiente para el nombre de host o la dirección IP de su servidor, por ejemplo, `server-01.loginsight.domain`. No puede especificar un patrón para el nombre de host.

```
[v3_req]
.
.
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

Procedimiento

- 1 Cree una carpeta para guardar sus archivos de certificado, por ejemplo, `C:\Certs\LogInsight`.
- 2 Abra una solicitud de comando y ejecute el siguiente comando.

```
C:\Certs\LogInsight>openssl req -x509 -nodes -newkey 2048 -keyout server.key -out server.crt -days 3650
```

OpenSSL le solicita suministrar propiedades del certificado, incluido el país, la organización, y demás.

- 3 Introduzca la dirección IP o el nombre de host exactos de su servidor de vRealize Log Insight, o la dirección del clúster de vRealize Log Insight si está habilitado el equilibrio de cargas.

Esta propiedad es la única para la que se debe especificar un valor de manera obligatoria.

Se crean dos archivos, `server.key` y `server.crt`.

- `server.key` es una nueva clave privada con codificación PEM.
- `server.crt` es un nuevo certificado con codificación PEM firmado por `server.key`.

Qué hacer a continuación

- Concatene los archivos de certificado. Consulte [Concatenar archivos de certificados](#).
- Cargue el certificado firmado. Consulte [Cargar certificado firmado](#).

Generar una solicitud de firma de certificado

Genere una solicitud de firma de certificado usando la herramienta OpenSSL para Windows.

Prerequisitos

- Descargue el instalador correspondiente para OpenSSL de <http://www.openssl.org/related/binaries.html>. Use el instalador de OpenSSL descargado para instalarlo en Windows.
- Edite el archivo `openssl.cfg` para añadir otros parámetros requeridos. Asegúrese de que la sección `[req]` tenga el parámetro `req_extensions` definido.

```
[req]
.
.
req_extensions=v3_req #
```

- Añada una entrada Nombre alternativo del sujeto correspondiente para el nombre de host o la dirección IP de su servidor, por ejemplo, `server-01.loginsight.domain`. No puede especificar un patrón para el nombre de host.

```
[v3_req]
.
.
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

Procedimiento

- 1 Cree una carpeta para guardar sus archivos de certificado, por ejemplo, `C:\Certs\LogInsight`.
- 2 Abra una solicitud de comando y ejecute el siguiente comando para generar su clave privada.

```
C:\Certs\LogInsight>openssl genrsa -out server.key 2048
```

- 3 Cree una solicitud de firma de certificado ejecutando el siguiente comando.

```
C:\Certs\LogInsight>openssl req -new -key server.key -out server.csr
```

NOTA: Este comando se ejecuta de manera interactiva y le formula numerosas preguntas. Su entidad de certificación comprobará sus respuestas. Sus respuestas deben coincidir con los documentos legales en relación con el registro de su empresa.

- 4 Siga las instrucciones en pantalla e introduzca la información que se incorporará a su solicitud de certificado.

IMPORTANTE: En el campo Nombre común, introduzca el nombre de host o la dirección IP de su servidor, por ejemplo, **correo.su.dominio**. Si desea incluir todos los subdominios, introduzca ***su.dominio**.

Su archivo de solicitud de firma de certificado `server.csr` se genera y guarda.

Solicitar la firma de una entidad de certificación

Envíe la solicitud de firma de certificado a la Entidad de certificación que elija y solicite una firma.

Procedimiento

- ◆ Envíe su archivo `server.csr` a una Entidad de certificación.

NOTA: Solicite que la Entidad de certificación codifique su archivo en el formato PEM.

La Entidad de certificación procesa su solicitud y le envía un archivo `server.crt` cifrado en el formato PEM.

Concatenar archivos de certificados

Combine sus archivos de claves y certificados en un archivo PEM.

Procedimiento

- 1 Cree un nuevo archivo `server.pem` y ábralo en el editor de texto.
- 2 Copie los contenidos de su archivo `server.key` y péguelo en `server.pem` usando el siguiente formato.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
```

- 3 Copie los contenidos de su archivo `server.crt` y péguelo en `server.pem` usando el siguiente formato.

```
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
```

- 4 Si las entidades de certificación le proporcionaron un certificado intermedio o encadenado, adjunte los certificados intermedios o encadenados al final del archivo de certificado público en el siguiente formato.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

- 5 Guarde su archivo `server.pem`.

Cargar certificado firmado

Puede cargar un certificado SSL firmado.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Configuración, haga clic en **Certificado SSL**.
- 3 Busque el certificado SSL personalizado y haga clic en **Abrir**.
- 4 Click **Save**.
- 5 Reinicie vRealize Log Insight.

Qué hacer a continuación

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see [ESXi Logs Stop Arriving in Log Insight](#).

Configurar la conexión SSL entre el servidor vRealize Log Insight y los Log Insight Agents

La función SSL le permite proporcionar conexiones SSL únicamente entre los Log Insight Agents y el vRealize Log Insight Server a través del flujo seguro de API de consumo. También puede configurar los diversos parámetros SSL de los Log Insight Agents.

Los agentes de vRealize Log Insight se comunican a través de TLSv.1.2. Se deshabilita SSLv.3/TLSv.1.0 para cumplir los criterios de seguridad.

Principales funciones SSL

Comprender las principales funciones SSL puede ayudarlo a configurar Log Insight Agents correctamente.

El agente de vRealize Log Insight almacena certificados y los usa para verificar la identidad del servidor durante todas las conexiones con un servidor determinado excepto la primera. Si la identidad del servidor no puede confirmarse, el agente de vRealize Log Insight rechaza la conexión con el servidor y escribe un mensaje de error adecuado en el registro. Los certificados recibidos por el agente se almacenan en la carpeta cert.

- Para Windows, vaya a `C:\ProgramData\VMware\Log Insight Agent\cert`.
- Para Linux, vaya a `/var/lib/loginsight-agent/cert`.

Cuando el agente de vRealize Log Insight establece una conexión segura con el servidor de vRealize Log Insight, el agente comprueba la validez del certificado recibido del servidor vRealize Log Insight. El agente de vRealize Log Insight usa certificados raíz de confianza del sistema.

- El Log Insight Linux Agent carga certificados de confianza de `/etc/pki/tls/certs/ca-bundle.crt` o de `/etc/ssl/certs/ca-certificates.crt`.
- El Log Insight Windows Agent usa certificados raíz del sistema.

Si el agente de vRealize Log Insight tiene un certificado autofirmado almacenado localmente y recibe un certificado autofirmado válido diferente con la misma clave pública, el agente acepta el nuevo certificado. Esto puede suceder cuando se vuelve a generar un certificado autofirmado usando la misma clave privada, pero con detalles diferentes como una nueva fecha de vencimiento. De lo contrario, se rechaza la conexión.

Si el agente de vRealize Log Insight tiene un certificado autofirmado almacenado localmente y recibe un certificado firmado por una CA válido, el agente de vRealize Log Insight reemplaza de manera silenciosa el nuevo certificado aceptado.

Si el agente de vRealize Log Insight recibe el certificado autofirmado después de tener un certificado firmado por una CA, el agente de Log Insight lo rechaza. El agente de vRealize Log Insight acepta el certificado autofirmado recibido del servidor de vRealize Log Insight solo cuando se conecta al servidor por primera vez.

Si el agente de vRealize Log Insight tiene un certificado firmado por CA almacenado localmente y recibe un certificado válido firmado por otra CA de confianza, el agente lo rechaza. Puede modificar las opciones de configuración del agente de vRealize Log Insight para que acepte el nuevo certificado. Consulte [Configurar los parámetros SSL del agente de vRealize Log Insight](#).

Los agentes de vRealize Log Insight se comunican a través de TLSv.1.2. Se deshabilita SSLv.3/TLSv.1.0 para cumplir los criterios de seguridad.

Exigir solo conexiones SSL

Puede usar la interfaz de usuario web de vRealize Log Insight para configurar vRealize Log Insight Agents y la API de consumo para permitir que solo haya conexiones SSL en el servidor.

Normalmente, se puede acceder a la API de vRealize Log Insight a través del puerto 9000 (HTTP) y el puerto 9543 (HTTPS). Tanto el agente de vRealize Log Insight como los clientes de la API personalizada pueden utilizar ambos puertos. Todas las solicitudes autenticadas requieren SSL, pero las no autenticadas (incluido el tráfico de consumo del agente de vRealize Log Insight) se pueden realizar de ambas formas. Puede forzar todas las solicitudes API para que utilicen conexiones SSL. Esta opción no restringe el tráfico del puerto 514 (syslog) ni afecta a la interfaz de usuario de vRealize Log Insight. Por tanto, las solicitudes del puerto 80 (HTTP) siguen redireccionando tráfico al puerto 443 (HTTPS).

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Configuración, haga clic en **SSL**.
- 3 En SSL de servidor de API, seleccione **Exigir conexión SSL**.
- 4 Click **Save**.

La API de vRealize Log Insight solo permite conexiones SSL en el servidor. Se rechazan las conexiones no pertenecientes a SSL.

Configurar los parámetros SSL del agente de vRealize Log Insight

Puede editar el archivo de configuración del agente de vRealize Log Insight para cambiar la configuración SSL, añadir una ruta de acceso a los certificados raíz de confianza, y definir si los certificados son aceptados por el agente.

Este procedimiento se aplica a los agentes de vRealize Log Insight de Windows y Linux.

Prerequisitos

Para el agente de Linux de vRealize Log Insight:

- Inicie sesión como **raíz** o use `sudo` para ejecutar comandos de la consola.
- Inicie sesión en la máquina de Linux en la que instaló el agente de Linux de vRealize Log Insight, abra una consola y ejecute `pgrep liagent` para verificar que el agente de Linux de vRealize Log Insight esté instalado y ejecutándose.

Para el agente de Windows de vRealize Log Insight:

- Log in to the Windows machine on which you installed the vRealize Log Insight Windows agent and start the Services manager to verify that the vRealize Log Insight agent service is installed.

Procedimiento

- 1 Desplácese hasta la carpeta que incluye el archivo `liagent.ini`.

Sistema operativo	Ruta de acceso
Linux	<code>/var/lib/loginsight-agent/</code>
Windows	<code>%ProgramData%\VMware\Log Insight Agent</code>

- 2 Open the `liagent.ini` file in any text editor.
- 3 Añada las siguientes claves a la sección `[server]` del archivo `liagent.ini`.

Clave	Descripción
<code>ssl_ca_path</code>	<p>Anula la ruta de almacenamiento predeterminada para los certificados raíz firmados por una entidad de certificación, que se usan para verificar los certificados del mismo nivel de conexión.</p> <p>Linux: si no se especifica ningún valor, el agente intenta cargar certificados de confianza de los archivos <code>/etc/pki/tls/certs/ca-bundle.crt</code> o <code>/etc/ssl/certs/ca-certificates.crt</code>.</p> <p>Windows: si no se especifica ningún valor, el agente de Windows de vRealize Log Insight carga certificados del almacén de certificados raíz de Windows.</p> <p>Cuando se especifica una ruta para <code>ssl_ca_path</code>, esta anula los valores predeterminados para los agentes de Windows y de Linux. Puede especificar como valor un archivo donde se concatenen varios certificados en formato PEM, o bien un directorio que contenga certificados en formato PEM y tengan nombres de la forma <code>hash.0</code> (consulte la opción <code>-hash</code> de la utilidad <code>x509</code>).</p>
<code>ssl_accept_any</code>	<p>Define si el agente de vRealize Log Insight acepta certificados. Los valores posibles son <code>yes</code>, <code>1</code>, <code>no</code> o <code>0</code>. Cuando el valor se establece en <code>sí</code> o <code>1</code>, el agente acepta certificados del servidor y establece una conexión segura para enviar datos. El valor predeterminado es <code>no</code>.</p>

Clave	Descripción
ssl_accept_any_trusted	Los valores posibles son sí, 1, no o 0. Si el agente de vRealize Log Insight tiene un certificado firmado por una entidad de certificación de confianza almacenado localmente y recibe un certificado válido firmado por una entidad de certificación de confianza diferente, marca la opción de configuración. Si el valor se establece en sí o 1, el agente acepta el nuevo certificado válido. Si el valor se establece en no o 0, rechaza el certificado y termina la conexión. El valor predeterminado es no.
ssl_cn	El campo Common Name del certificado autofirmado. El valor predeterminado es VMware vCenter Log Insight. Puede definir un Common Name personalizado para comprobar en función del campo Common Name del certificado. El agente de vRealize Log Insight comprueba el campo Common Name del certificado recibido en función del nombre de host especificado para la clave hostname en la sección [server]. Si no coinciden, el agente compara el campo Common Name con la clave ssl_cn en el archivo liagent.ini. Si los valores coinciden, el agente de vRealize Log Insight acepta el certificado.

NOTA: Estas claves se ignoran si SSL está deshabilitado.

- 4 Save and close the liagent.ini file.

Ejemplo: Configuración

A continuación se incluye un ejemplo de la configuración SSL.

```
proto=cfapi
port=9543
ssl=yes
ssl_ca_path=/etc/pki/tls/certs/ca-bundle.crt
ssl_accept_any=no
ssl_accept_any_trusted=yes
ssl_cn=LOGINSIGHT
```

Cambiar el período de tiempo de espera predeterminado para las sesiones web de vRealize Log Insight

De modo predeterminado, a fin de mantener seguro el entorno, las sesiones web de vRealize Log Insight caducan en 30 minutos. Puede aumentar o disminuir la duración del tiempo de espera.

Puede modificar el período de tiempo de espera mediante la UI web.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Configuration, click **General**.
- 3 En el panel Sesión del navegador, especifique un valor de tiempo de espera en minutos.
El valor `-1` deshabilita los tiempos de espera de la sesión.
- 4 Click **Save**.

Archivos

Habilitar o deshabilitar archivos de datos en vRealize Log Insight

El archivo de datos conserva registros anteriores que pueden eliminarse de otra forma del dispositivo virtual de vRealize Log Insight a causa de restricciones de almacenamiento. vRealize Log Insight puede almacenar datos archivados en montajes de NFS.

vRealize Log Insight recopila y almacena registros en disco en una serie de depósitos de 1 GB. Un depósito comprende archivos de registro comprimidos y un índice. Un depósito incluye todo lo necesario para realizar consultas para un intervalo de tiempo específico. Cuando el tamaño del depósito supera 1 GB, vRealize Log Insight deja de escribir, cierra todos los archivos del depósito y lo sella.

Cuando use el archivado de datos, vRealize Log Insight copia los archivos de registro comprimidos del depósito a un montaje NFS cuando el depósito está sellado. Los depósitos que se sellan cuando no está habilitado el archivado de datos no se archivan de forma retroactiva.

La ruta de acceso creada dentro de una exportación de archivos emplea el formato **año/mes/día/hora/bucketuuid/data.blob** y se basa en la marca de tiempo en que se creó originalmente el depósito en UTC.

NOTA: vRealize Log Insight no administra el montaje NFS usado para fines de archivo. Si las notificaciones del sistema están habilitadas, vRealize Log Insight envía un correo electrónico cuando el montaje NFS está a punto de quedarse sin espacio o no está disponible. Si el montaje de NFS no tiene suficiente espacio libre o no está disponible durante un periodo mayor que el de retención del dispositivo virtual, vRealize Log Insight deja de consumir datos nuevos. Empieza a recopilar datos de nuevo cuando el montaje de NFS cuenta con suficiente espacio libre, vuelve a estar disponible o el archivado está deshabilitado.

Prerequisitos

- Verifique que tenga acceso a una partición NFS que cumpla con los siguientes requisitos.
 - La partición NFS debe permitir operaciones de lectura y escritura para cuentas invitadas.
 - El montaje no debe requerir autenticación.
 - El servidor NFS debe admitir NFS v3.
 - Si usa un servidor Windows NFS, permita el acceso UNIX de usuario sin asignar (por UID/GID).
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Configuración, haga clic en **Archivo**.
- 3 Seleccione **Habilitar archivado de datos** e introduzca la ruta a una partición NFS para archivar los registros con el formato `nfs://servername<: número-puerto>/exportname`.
El número de puerto predeterminado es 2049.
- 4 Haga clic en **Probar** para verificar la conexión.
- 5 Click **Save**.

NOTA: El archivo de datos conserva los eventos de registro que se han eliminado desde entonces del dispositivo virtual de vRealize Log Insight a causa de restricciones de almacenamiento. Los eventos de registro que se han eliminado del dispositivo virtual de vRealize Log Insight, pero que se han archivado ya no pueden buscarse. Si desea buscar registros archivados, debe importarlos a una instancia de vRealize Log Insight. Para obtener más información sobre cómo importar archivos de registro archivados, consulte [Importar un archivo de vRealize Log Insight a vRealize Log Insight](#).

Qué hacer a continuación

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see [ESXi Logs Stop Arriving in Log Insight](#).

Formatear los archivos de vRealize Log Insight

vRealize Log Insight archiva los datos en un formato específico.

vRealize Log Insight almacena archivos en un servidor NFS y los organiza en directorios jerárquicos basados en tiempo de archivo. Por ejemplo,

```
/backup/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49/data.blob
```

donde `/backup` es la ubicación NFS, `2014/08/07/16` es la hora de almacenamiento, `bd234b2d-df98-44ae-991a-e0562f10a49` es el identificador del depósito, y `data.blob` son los datos archivados para el depósito.

Los datos de archivo `data.blob` son un archivo comprimido que usa codificación interna vRealize Log Insight. Incluye el contenido original de todos los mensajes almacenados en el depósito, junto con los campos estáticos, como la marca de tiempo, el nombre de host, el origen y el nombre de la aplicación.

Puede importar datos archivados a vRealize Log Insight, exportar datos de archivo a un archivo de texto sin procesar y extraer contenido de mensaje de datos de archivo. Consulte [Exportar un archivo de Log Insight a un archivo de texto sin procesar o JSON](#) y [Importar un archivo de vRealize Log Insight a vRealize Log Insight](#).

Importar un archivo de vRealize Log Insight a vRealize Log Insight

El archivo de datos conserva registros anteriores que pueden eliminarse de otra forma del dispositivo virtual de vRealize Log Insight a causa de restricciones de almacenamiento. Consulte [Habilitar o deshabilitar archivos de datos en vRealize Log Insight](#). Puede usar la línea de comandos para importar registros que se hayan archivado en vRealize Log Insight.

NOTA: Aunque vRealize Log Insight puede manejar los datos históricos y de tiempo real en forma simultánea, se sugiere implementar una instancia separada de vRealize Log Insight para procesar los archivos de registro importados.

Prerequisitos

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- Verifique que tenga acceso al servidor NFS donde se archivan los registros de vRealize Log Insight.
- Verifique que el dispositivo virtual de vRealize Log Insight tenga espacio en disco suficiente para alojar los archivos de registro importados.

El espacio libre mínimo en la partición `/storage/core` en el dispositivo virtual debe ser aproximadamente igual a 10 veces el tamaño del registro archivado que desea importar.

Procedimiento

- 1 Establezca una conexión SSH con vRealize Log Insight vApp e inicie sesión como usuario raíz.
- 2 Monte la carpeta compartida en el servidor NFS donde residen los datos archivados.
- 3 Para importar un directorio de los registros de vRealize Log Insight archivados, ejecute el siguiente comando.

```
/usr/lib/loginsight/application/bin/loginsight repository import Path-To-Archived-Log-Data-Folder.
```

NOTA: Importar datos archivados puede demorar una gran cantidad de tiempo, según el tamaño de la carpeta importada.

4 Cierre la conexión SSH.

Qué hacer a continuación

Puede buscar, filtrar y analizar los eventos de registro importados.

Exportar un archivo de Log Insight a un archivo de texto sin procesar o JSON

Puede usar la línea de comandos para exportar un archivo de vRealize Log Insight a un archivo de texto sin procesar o en formato JSON.

NOTA: Este es un procedimiento avanzado. La sintaxis del comando y los formatos de salida pueden cambiar en versiones posteriores de vRealize Log Insight sin compatibilidad con versiones anteriores.

Prerequisitos

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- Verifique que el dispositivo virtual de vRealize Log Insight tenga espacio en disco suficiente para alojar los archivos exportados.

Procedimiento

- 1 Establezca una conexión SSH con vRealize Log Insight vApp e inicie sesión como usuario raíz.
- 2 Cree un directorio de archivos en vRealize Log Insight vApp.

```
mkdir /archive
```

- 3 Monte la carpeta compartida en el servidor NFS donde residen los datos archivados ejecutando el siguiente comando.

```
mount -t nfs archive-fileshare:archive directory path /archive
```

- 4 Compruebe el espacio de almacenamiento disponible en vRealize Log Insight vApp.

```
df -h
```

- 5 Exporte un archivo de vRealize Log Insight a un archivo de texto sin procesar.

```
/usr/lib/loginsight/application/sbin/repo-exporter -d archive-file-directory output-file
```

Por ejemplo,

```
/usr/lib/loginsight/application/sbin/repo-exporter -d /archive/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49 /tmp/output.txt
```

- 6 Exporta el contenido de un mensaje de un archivo de vRealize Log Insight en formato JSON.

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d archive-file-directory output-file.
```

Por ejemplo,

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d /archive/2014/08/07/16/bd234b2d-  
df98-44ae-991a-e0562f10a49 /tmp/output.json
```

- 7 Cierre la conexión SSH.

Reinicie el servicio de vRealize Log Insight

Puede reiniciar vRealize Log Insight usando la página Administrador en la interfaz de usuario web.

ADVERTENCIA: El reinicio de vRealize Log Insight cierra todas las sesiones del usuario activo. Los usuarios de la instancia vRealize Log Insight estarán forzados a volver a iniciar sesión.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 Seleccione un nodo de clúster.
- 4 Haga clic en **Reiniciar principal** y haga clic en **Reiniciar**.

Qué hacer a continuación

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see [ESXi Logs Stop Arriving in Log Insight](#).

Apagar el dispositivo virtual de vRealize Log Insight

Para evitar la pérdida de datos al apagar un nodo de trabajador o principal vRealize Log Insight, debe apagar el nodo siguiendo una secuencia estricta de pasos.

Debe apagar el dispositivo virtual de vRealize Log Insight antes de realizar cambios en el hardware virtual del dispositivo.

Puede apagar el dispositivo virtual de vRealize Log Insight mediante la opción del menú **Alimentación > Desconectar invitado** en vSphere Client usando la consola del dispositivo virtual o estableciendo una conexión SSH con el dispositivo virtual de vRealize Log Insight y ejecutando un comando.

Prerequisitos

- If you plan to connect to the vRealize Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.
- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Establezca una conexión SSH con vRealize Log Insight vApp e inicie sesión como usuario raíz.
- 2 Para apagar el dispositivo virtual de vRealize Log Insight, ejecute `shutdown -h now`.

Qué hacer a continuación

Puede modificar en forma segura el hardware virtual del dispositivo virtual de vRealize Log Insight.

Descargar un paquete de soporte de vRealize Log Insight

Si vRealize Log Insight no funciona según lo previsto debido a un problema, puede enviar una copia de los archivos de registro y configuración al servicio de soporte técnico de VMware en forma de un paquete de soporte.

Solo es necesario descargar un paquete de soporte para todo el clúster si el servicio de soporte técnico de VMware así lo solicita. Puede crear el paquete de forma estática (que usa espacio de disco en el nodo) o por streaming (que no lo usa y almacena el paquete en el equipo de arranque predeterminado).

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Administración, haga clic en **Clúster**.
- 3 En el encabezado Soporte, haga clic en **Descargar paquete de soporte**.

El sistema de vRealize Log Insight recopila la información del diagnóstico y envía estos datos al navegador en un archivo tar comprimido.

- 4 Seleccione el método para crear el paquete.
 - Seleccione **Paquete de soporte estático** para crear un paquete de forma local. La creación del paquete consume espacio de disco en el nodo.
 - Seleccione **Paquete de soporte de streaming** para iniciar la transmisión del paquete de soporte inmediatamente. Este método no utiliza espacio de disco en el nodo.
- 5 Haga clic en **Continuar**.
- 6 En el cuadro de diálogo Descarga de archivos, haga clic en **Guardar**.

7 Seleccione una ubicación en la que desee guardar el archivo tar y haga clic en **Guardar**.

Qué hacer a continuación

Puede revisar el contenido de los archivos de registro en busca de mensajes de error. Cuando resuelva o cierre problemas, elimine el paquete de soporte desactualizado para ahorrar espacio en disco.

Unirse al Programa de mejora de la experiencia de cliente o abandonarlo

Puede unirse al Programa de mejora de la experiencia de cliente de VMware o abandonarlo después de implementar vRealize Log Insight.

Es posible elegir si desea participar en el Programa de mejora de la experiencia de cliente cuando instala vRealize Log Insight. Tras la instalación, puede unirse al programa o abandonarlo siguiendo estos pasos.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Configuration, click **General**.
- 3 En el panel Programa de mejora de la experiencia de cliente, seleccione o desmarque la casilla **Participar en el Programa para la mejora de la experiencia de usuario de VMware**.
Cuando se selecciona, la opción activa el Programa y envía datos a `https://vmware.com`.
- 4 Click **Save**.

Configurar clústeres de vRealize Log Insight

5

Puede añadir, eliminar y actualizar los nodos de un clúster de vRealize Log Insight.

NOTA: La agrupación WAN en clústeres no es compatible con vRealize Log Insight. Las versiones actuales de vRealize Log Insight no admiten la agrupación de clústeres por WAN (también llamada geocustering, agrupación de clústeres remota o de alta disponibilidad). Todos los nodos de un clúster deben implementarse en la misma LAN de capa 2. Además, los puertos que se describen en [Puertos e interfaces externas](#) deben abrirse entre nodos para una correcta comunicación.

Este capítulo cubre los siguientes temas:

- [Añadir un nodo de trabajador al clúster de vRealize Log Insight.](#)
- [Eliminar un nodo de trabajador de un clúster de vRealize Log Insight](#)
- [Trabajar con un equilibrador de carga integrado](#)
- [Consultar los resultados de comprobaciones de clústeres en producción](#)

Añadir un nodo de trabajador al clúster de vRealize Log Insight .

Implemente una nueva instancia del dispositivo virtual Log Insight y añádala a un nodo principal de Log Insight.

Procedimiento

1 [Implementar el dispositivo virtual vRealize Log Insight](#)

Descargue el dispositivo virtual vRealize Log Insight. VMware distribuye el dispositivo virtual vRealize Log Insight como un archivo .ova. Implemente el dispositivo virtual vRealize Log Insight usando vSphere Client.

2 [Unirse a una implementación existente](#)

Después de implementar y establecer un nodo de vRealize Log Insight independiente, puede implementar una nueva instancia de vRealize Log Insight y añadirla al nodo existente para formar un clúster de vRealize Log Insight.

Implementar el dispositivo virtual vRealize Log Insight

Descargue el dispositivo virtual vRealize Log Insight. VMware distribuye el dispositivo virtual vRealize Log Insight como un archivo .ova. Implemente el dispositivo virtual vRealize Log Insight usando vSphere Client.

Prerequisitos

- Compruebe que tiene una copia del dispositivo virtual vRealize Log Insight .ova.
- Compruebe que cuenta con permisos para implementar plantillas de OVF en el inventario.
- Compruebe que su entorno tenga suficientes recursos para acomodar los requisitos mínimos del dispositivo virtual vRealize Log Insight. Consulte [Requisitos mínimos](#).
- Compruebe que ha leído atentamente las recomendaciones de dimensionamiento del dispositivo virtual. Consulte [Dimensionar el dispositivo virtual Log Insight](#).

Procedimiento

- 1 En vSphere Client, seleccione **Archivo > Implementar plantilla de OVF**.
- 2 Siga las indicaciones del asistente **Implementar plantilla de OVF**.
- 3 En la página Seleccionar configuración, seleccione el tamaño del dispositivo virtual vRealize Log Insight en función del tamaño del entorno para el cual intenta recopilar registros.

Pequeño es el requisito mínimo para los entornos de producción.

vRealize Log Insight proporciona tamaños de máquinas virtuales preestablecidos que puede seleccionar para cumplir los requisitos de consumo del entorno. La configuración preestablecida cuenta con combinaciones certificadas de tamaños de los recursos informáticos y de disco, aunque puede agregar recursos adicionales posteriormente. La configuración reducida consume los recursos mínimos sin dejar de estar admitida. La configuración muy reducida solo es apropiada para demostraciones.

Opción	Tasa de consumo del registro	CPU virtuales	Memoria	IOPS	Conexiones de syslog (conexiones de TCP activas)	Eventos por segundo
Extrapequeño	6 GB por día	2	4 GB	75	20	400
Pequeño	30 GB por día	4	8 GB	500	100	2000

Opción	Tasa de consumo del registro	CPU virtuales	Memoria	IOPS	Conexiones de syslog (conexiones de TCP activas)	Eventos por segundo
Mediano	75 GB por día	8	16 GB	1000	250	5000
Grande	225 GB por día	16	32 GB	1500	750	15.000

NOTA: Puede usar un agregador para incrementar la cantidad de conexiones syslog que envían eventos a vRealize Log Insight. No obstante, la cantidad máxima de eventos por segundo es fija y no depende del uso de un agregador syslog. No es posible utilizar una instancia de vRealize Log Insight como agregador syslog.

NOTA: Si selecciona **Grande**, debe actualizar el hardware virtual en la máquina virtual vRealize Log Insight después de la implementación.

4 En la página Seleccionar almacenamiento, seleccione un formato de disco.

- **Aprovisionamiento grueso sin escritura de ceros** crea un disco virtual en un formato grueso predeterminado. El espacio requerido para el disco virtual se asigna cuando se crea el disco virtual. Los datos que quedan en el dispositivo físico no se borran durante la creación, sino que se reducen a cero en la primera escritura desde el dispositivo virtual según demanda.
- El filtro **contiene** crea un tipo de disco virtual grueso compatible con características de agrupación de clústeres como Fault Tolerance (Tolerancia a errores). El espacio requerido para el disco virtual se asigna al momento de la creación. En contraste al formato plano, los datos que quedan en el dispositivo físico se reducen a cero cuando se crea el disco virtual. Crear discos con este formato puede requerir mucho más tiempo que hacerlo con otros tipos.

IMPORTANTE: Implemente el dispositivo virtual vRealize Log Insight con discos de aprovisionamiento grueso con escritura de ceros siempre que sea posible para un mejor rendimiento y funcionamiento del dispositivo virtual.

- **Aprovisionamiento fino** crea un disco en formato fino. El disco crece a medida que crecen los datos guardados en él. Si su dispositivo de almacenamiento no es compatible con los discos de aprovisionamiento grueso, o desea conservar el espacio no utilizado del disco en el dispositivo virtual vRealize Log Insight, implemente el dispositivo virtual con los discos de aprovisionamiento fino.

NOTA: Encoger discos en el dispositivo virtual vRealize Log Insight no es compatible y puede resultar en corrupción o en pérdida de datos.

- 5 (Opcional) En la página Configurar redes, configure los parámetros de redes para el dispositivo virtual vRealize Log Insight.

Si no proporciona las opciones de configuración de redes, como la información de la puerta de enlace, los servidores DNS y la dirección IP, vRealize Log Insight utilizará DHCP para configurar dichas opciones.

ADVERTENCIA: No especifique más de dos servidores de nombre de dominio. Si especifica más de dos servidores de nombre de dominio, todos los servidores de nombre de dominio configurados serán ignorados en el dispositivo virtual vRealize Log Insight.

Utilice una lista separada por comas para especificar los servidores de nombres de dominio.

- 6 (Opcional) En la página Personalizar plantilla, configure las propiedades de red si no está usando DHCP.
- 7 (Opcional) En la página Personalizar plantilla, seleccione **Otras propiedades** y establezca la contraseña raíz para el dispositivo virtual vRealize Log Insight.

La contraseña raíz es necesaria para SSH. También puede establecer esta contraseña en VMware Remote Console.

- 8 Siga las indicaciones para completar la implementación.

Para obtener información sobre el modo de implementar dispositivos virtuales, consulte la *Guía del usuario para la implementación de vApps y dispositivos virtuales*.

Después de encender el dispositivo virtual, comienza un proceso de inicialización. El proceso de inicialización tarda varios minutos en completarse. Al finalizar el proceso, el dispositivo virtual se reinicia.

- 9 Desplácese hasta la pestaña **Consola** y revise la dirección IP del dispositivo virtual vRealize Log Insight.

Prefijo de dirección IP	Descripción
https://	La configuración de DHCP en el dispositivo virtual es correcta.
http://	Error en la configuración de DHCP en el dispositivo virtual. <ol style="list-style-type: none"> Apague el dispositivo virtual vRealize Log Insight. Haga clic con el botón derecho en el dispositivo virtual y seleccione Editar configuración. Establezca una dirección IP estática para el dispositivo virtual.

Qué hacer a continuación

- Si desea configurar una implementación de vRealize Log Insight independiente, consulte [Configurar nueva instalación de Log Insight](#).

The vRealize Log Insight Web interface is available at `https://log-insight-host/` where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Unirse a una implementación existente

Después de implementar y establecer un nodo de vRealize Log Insight independiente, puede implementar una nueva instancia de vRealize Log Insight y añadirla al nodo existente para formar un clúster de vRealize Log Insight.

vRealize Log Insight puede realizar el escalamiento horizontal mediante el uso de múltiples instancias del dispositivo virtual en clústeres. Estos habilitan el escalamiento lineal del rendimiento de consumo, aumentan el rendimiento de la consulta y permiten el consumo de alta disponibilidad. En el modo del clúster, vRealize Log Insight proporciona nodos principal y de trabajador. Los nodos principal y de trabajador son responsables de una subred de datos. Los nodos principales pueden consultar todos los subconjuntos de datos y añadir los resultados.

IMPORTANTE: Configure un mínimo de tres nodos en un clúster de vRealize Log Insight para proporcionar alta disponibilidad de consumo, configuración y espacio del usuario.

Prerequisitos

- En vSphere Client, anote la dirección IP del dispositivo virtual de vRealize Log Insight de trabajador.
- Verifique que tenga la dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight principal.
- Verifique que tenga una cuenta de administrador en el dispositivo virtual de vRealize Log Insight principal.
- Verifique que las versiones de los nodos principal y de trabajador de vRealize Log Insight estén sincronizadas. No añada una versión anterior del nodo de trabajador de vRealize Log Insight a una nueva versión del nodo principal de vRealize Log Insight.
- Debe sincronizar la hora en que el dispositivo virtual de vRealize Log Insight con un servidor NTP. Consulte [Sincronizar la hora en el dispositivo virtual de Log Insight](#).
- Para obtener información sobre las versiones admitidas del explorador, consulte las [Notas de la versión de vRealize Log Insight](#).

Procedimiento

- 1 Use un explorador compatible para desplazarse a la interfaz de usuario web del nodo de trabajador de vRealize Log Insight.

El formato de la URL es `https://log_insight-host/`, donde `log_insight-host` es la dirección IP o el nombre de host del dispositivo virtual de trabajador de vRealize Log Insight.

Se abre el asistente de configuración inicial.

- 2 Haga clic en **Unirse a implementación existente**.

- 3 Introduzca la dirección IP o el nombre de host del nodo principal de vRealize Log Insight y haga clic en **Ir**.

El nodo de trabajador envía una solicitud al nodo principal de vRealize Log Insight para unirse a la implementación existente.

- 4 Seleccione la opción **Haga clic aquí para acceder a la página Administración de clústeres**.

- 5 Inicie sesión como administrador.

Se carga la página Clúster.

- 6 Haga clic en **Permitir**.

El nodo de trabajador se une a la implementación existente y vRealize Log Insight comienza a operar en un clúster.

Qué hacer a continuación

- Para añadir otro nodo de trabajador, implemente una nueva instancia de vRealize Log Insight y agréguela al clúster usando el asistente de inicio.
- Repita el procedimiento para añadir un mínimo de dos nodos de trabajador de vRealize Log Insight.

Eliminar un nodo de trabajador de un clúster de vRealize Log Insight

Es posible eliminar un nodo de trabajador que ya no funciona correctamente de un clúster de vRealize Log Insight y añadirlo a un clúster diferente o iniciar una implementación independiente. No elimine los nodos desde trabajador que funcionan correctamente desde un clúster.

Al quitar un nodo se produce una pérdida de datos. Si es necesario quitar un nodo, asegúrese de que primero se haya realizado una copia de seguridad. Evite quitar nodos dentro de los 30 minutos de haber añadido nuevos.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 In the Workers table, find the node you want, click the pause icon,  and click **Continue**.

The node is now in maintenance mode.

NOTA: A node in maintenance mode continues to receive logs.

- 4 Haga clic en  para quitar el nodo.

vRealize Log Insight elimina el nodo del clúster y envía una notificación por correo electrónico.

Qué hacer a continuación

Desplácese hasta la interfaz de usuario web del nodo eliminado para configurarlo. Puede añadir el nodo al clúster de vRealize Log Insight diferente existente o iniciar una implementación nueva independiente.

Trabajar con un equilibrador de carga integrado

Puede habilitar el equilibrador de carga integrado (ILB) de vRealize Log Insight en un clúster de vRealize Log Insight para garantizar que el tráfico de ingesta entrante sea aceptado por vRealize Log Insight, incluso si algunos nodos de vRealize Log Insight no están disponibles. También puede configurar varias direcciones IP virtuales.

Es muy recomendable habilitar el ILB en un entorno de clúster de vRealize Log Insight para equilibrar correctamente el tráfico entre los nodos de un clúster y minimizar la sobrecarga administrativa.

NOTA: External load balancers are not suggested for use with vRealize Log Insight. Support will be removed in a later version.

Se recomienda incluir el ILB en todas las implementaciones, incluidas las instancias de nodo único. Envíe consultas y tráfico de consumo al ILB para que se pueda admitir fácilmente un clúster en el futuro si fuera necesario.

El ILB garantiza que el tráfico de consumo entrante sea aceptado por vRealize Log Insight, incluso si algunos nodos de vRealize Log Insight no están disponibles. El ILB también equilibra el tráfico entrante de manera justa entre los nodos de vRealize Log Insight disponibles. Los clientes vRealize Log Insight, que usan la interfaz de usuario web y el consumo (a través de Syslog o la API de consumo), deben conectarse a vRealize Log Insight a través de la dirección de ILB.

ILB requiere que todos los nodos de vRealize Log Insight estén en la misma red de Capa 2, tal como detrás del mismo conmutador o que puedan de cualquier otra forma recibir solicitudes de ARP y enviar solicitudes de ARP entre sí. La dirección IP del ILB debe establecerse de modo tal que cualquier nodo de vRealize Log Insight pueda tener una y recibir tráfico para ella. Comúnmente, esto implica que la dirección IP del ILB estará en la misma subred que la dirección física de los nodos de vRealize Log Insight. Después de configurar la dirección IP del ILB, intente ejecutar el comando ping en él desde una red diferente para garantizar que esté accesible.

Para simplificar futuros cambios y actualizaciones, puede hacer que los clientes apunten a un FQDN que se resuelva en la dirección IP del ILB, en lugar de apuntar directamente a la dirección IP del ILB.

Acerca de la configuración de Direct Server Return

El equilibrador de carga de vRealize Log Insight utiliza una configuración de Direct Server Return (DSR). En DSR, todo el tráfico entrante pasa por el nodo de vRealize Log Insight que es el nodo equilibrador de carga actual, mientras que el tráfico de retorno se envía desde los servidores vRealize Log Insight directamente de vuelta al cliente, sin necesidad de que pase por el nodo equilibrador de carga.

Direcciones IP virtuales múltiples

Puede configurar varias direcciones IP virtuales (vIP) para el equilibrador de carga integrado. Puede configurar una lista de etiquetas estáticas para cada vIP, de modo que cada mensaje de registro recibido de la vIP se anote con las etiquetas configuradas.

Habilitar el equilibrador de carga integrado

Al habilitar el equilibrador de carga integrado (ILB) de vRealize Log Insight en un clúster de vRealize Log Insight, puede configurar una o más direcciones IP virtuales. Opcionalmente, puede permitir a los usuarios acceder al clúster mediante FQDN.

Prerequisitos

- Verifique que todos los nodos de vRealize Log Insight y la dirección IP del equilibrador de carga integrado estén en la misma red.
- Los nodos principal y de trabajador de vRealize Log Insight deben tener los mismos certificados. De lo contrario, los agentes de vRealize Log Insight configurados para conectarse a través de SSL rechazan la conexión. Al cargar un certificado con firma de CA a los nodos principal y de trabajador de vRealize Log Insight, establezca la dirección IP de Nombre común a ILB durante la solicitud de generación de certificados. Consulte [Generar una solicitud de firma de certificado](#).
- You must synchronize the time on the vRealize Log Insight virtual appliance with an NTP server. See [Synchronize the Time on the Log Insight Virtual Appliance](#).

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 En Configuración, seleccione **Dirección IP virtual nueva** e introduzca la dirección IP virtual (vIP) que se debe usar para el equilibrio de carga integrado.
- 4 (Opcional) Para configurar varias direcciones IP virtuales, haga clic en **Dirección IP virtual nueva** e introduzca la dirección IP. Puede elegir introducir el nombre FQDN y las etiquetas.
 - Cada vIP debe estar en la misma subred que al menos una interfaz de red en cada nodo y la vIP debe estar disponible (no debe ser utilizada por otra máquina).
 - Las etiquetas le permiten agregar campos con valores predefinidos a los eventos, para facilitar la consulta. Puede agregar varias etiquetas separadas por comas. Todos los eventos que se introducen en el sistema a través de una vIP se marcan con las etiquetas de la vIP.
 - Puede configurar una lista de etiquetas estáticas (clave=valor) para una vIP de ILB, de modo que cada mensaje de registro recibido de la vIP se anote con las etiquetas configuradas.
- 5 (Opcional) Para permitir a los usuarios de vRealize Log Insight acceder al clúster a través de FQDN, haga que los clientes apunten al FQDN en lugar de apuntar directamente a la dirección IP del ILB configurado.

6 Haga clic en **Guardar**.

El equilibrador de carga integrado está administrado por un nodo en el clúster de vRealize Log Insight, declarado el líder para ese servicio. El líder actual está indicado por el texto (ILB) junto al nodo.

Consultar los resultados de comprobaciones de clústeres en producción

El servicio de comprobación de clústeres en producción ejecuta una serie de comprobaciones regularmente en cada nodo. Puede consultar los resultados más recientes de estas comprobaciones usando la interfaz de línea de comandos.

El servicio averigua, por ejemplo, si el clúster funciona y está configurado según lo previsto o si existe algún problema con las integraciones en otros sistemas. A continuación se incluyen más comprobaciones.

- ¿Está NTP configurado en una implementación con varios hosts?
- ¿Es Active Directory accesible (si está configurado actualmente)?
- ¿Se puede realizar la autenticación de Active Directory (si está configurado actualmente)?
- ¿Son accesibles los hosts de Active Directory y de Kerberos (si Active Directory está configurado actualmente)?
- ¿Se ejecuta el sistema en una implementación de dos hosts que no es compatible?
- ¿Hay espacio suficiente en /tmp para llevar a cabo una actualización?
- ¿Hay espacio suficiente en /storage/core para llevar a cabo una actualización?
- ¿Está localhost colocado correctamente dentro de /etc/hosts?

Procedimiento

- 1 En la línea de comandos, establezca una conexión SSH con el dispositivo virtual de vRealize Log Insight e inicie sesión como usuario raíz.
- 2 En la línea de comandos, escriba `/usr/lib/loginsight/application/sbin/query-check-results.sh` y presione **Entrar**.

Puertos e interfaces externas

vRealize Log Insight usa servicios, puertos e interfaces externas específicos que son necesarios.

Puertos de comunicación

vRealize Log Insight usa los protocolos y puertos de comunicación enumerados en este tema. Los puertos necesarios se organizan en función de si se necesitan para los orígenes, para la interfaz de usuario, entre clústeres o para servicios externos, o bien si se pueden bloquear con un firewall. Algunos puertos se usan solamente si se habilita la integración correspondiente.

NOTA: vRealize Log Insight no admite clústeres WAN (también denominados geoclústeres, clústeres de alta disponibilidad o clústeres remotos). Todos los nodos de un clúster deben implementarse en la misma LAN de capa 2. Además, los puertos descritos en esta sección deben estar abiertos entre nodos para una correcta comunicación.

El tráfico de red de vRealize Log Insight tiene distintos orígenes.

Estación de trabajo administrativa	La máquina que usa un administrador de sistema para administrar el dispositivo virtual de vRealize Log Insight de manera remota.
Estación de trabajo del usuario	La máquina en la que un usuario de vRealize Log Insight usa un explorador para acceder a la interfaz web de vRealize Log Insight.
Sistema que envía registros	El endpoint que envía registros a vRealize Log Insight para análisis y búsqueda. Por ejemplo, los endpoints incluyen hosts ESXi, máquinas virtuales o cualquier sistema con una dirección IP.
Log Insight Agents	El agente que reside en una máquina Windows o Linux, y envía eventos del sistema operativo e inicia sesión en vRealize Log Insight a través de API.
Dispositivo vRealize Log Insight	Cualquier dispositivo virtual de vRealize Log Insight, principal o de trabajador, donde residen los servicios de vRealize Log Insight. El sistema operativo base del dispositivo es SUSE 11 SP3.

Puertos necesarios para orígenes que envían datos

Los siguientes puertos deben estar abiertos al tráfico de red desde orígenes que envían datos a vRealize Log Insight, tanto para conexiones desde fuera del clúster como para conexiones de carga equilibrada entre nodos del clúster.

Origen	Destino	Puerto	Protocolo	Descripción del servicio
Sistema que envía registros	Dispositivo vRealize Log Insight	514	TCP, UDP	Tráfico de syslog saliente configurado como un destino de reenvío
Sistema que envía registros	Dispositivo vRealize Log Insight	1514, 6514	TCP	Datos de syslog a través de SSL
Agentes de vRealize Log Insight	Dispositivo vRealize Log Insight	9000	TCP	API de consumo de Log Insight
Agentes de vRealize Log Insight	Dispositivo vRealize Log Insight	9543	TCP	API de consumo de Log Insight a través de SSL

Puertos necesarios para la interfaz de usuario

Los siguientes puertos deben estar abiertos al tráfico de red que necesite utilizar la interfaz de usuario de vRealize Log Insight, tanto para conexiones fuera del clúster como para conexiones de carga equilibrada entre nodos del clúster.

Origen	Destino	Puerto	Protocolo	Descripción del servicio
Estación de trabajo administrativa	Dispositivo vRealize Log Insight	22	TCP	SSH: conectividad shell segura
Estación de trabajo del usuario	Dispositivo vRealize Log Insight	80	TCP	HTTP: interfaz web
Estación de trabajo del usuario	Dispositivo vRealize Log Insight	443	TCP	HTTPS: interfaz web

Puertos necesarios entre nodos de clúster

Los siguientes puertos solo deben estar abiertos en un nodo principal de vRealize Log Insight para el acceso de red desde los nodos de trabajador para máxima seguridad. Además, se deben tener en cuenta los puertos usados para los orígenes y el tráfico de la interfaz de usuario que tienen carga equilibrada entre los nodos del clúster.

Origen	Destino	Puerto	Protocolo	Descripción del servicio
Dispositivo vRealize Log Insight	Dispositivo vRealize Log Insight	7000	TCP	Replicación y consulta de Cassandra
Dispositivo vRealize Log Insight	Dispositivo vRealize Log Insight	9042	TCP	Servicio de Cassandra para clientes de protocolos nativos
Dispositivo vRealize Log Insight	Dispositivo vRealize Log Insight	9160	TCP	Servicio de Cassandra para clientes Thrift
Dispositivo vRealize Log Insight	Dispositivo vRealize Log Insight	59778, 16520-16580	TCP	Servicio Thrift de vRealize Log Insight

Puertos necesarios para servicios externos

Los siguientes puertos deben estar abiertos para permitir el tráfico de red saliente desde los nodos del clúster de vRealize Log Insight hasta servicios remotos.

Origen	Destino	Puerto	Protocolo	Descripción del servicio
Dispositivo vRealize Log Insight	Servidor NTP	123	UDP	NTPD: proporciona sincronización de hora NTP NOTA: El puerto está abierto solo si elige usar la sincronización de hora NTP
Dispositivo vRealize Log Insight	Servidor de correo	25	TCP	SMTP: servicio de correo para alertas salientes
Dispositivo vRealize Log Insight	Servidor de correo	465	TCP	SMTPS: servicio de correo a través de SSL para alertas salientes
Dispositivo vRealize Log Insight	Servidor DNS	53	TCP, UDP	DNS: servicio de resolución de nombres
Dispositivo vRealize Log Insight	Servidor AD	389	TCP, UDP	Active Directory
Dispositivo vRealize Log Insight	Servidor AD	636	TCP	Active Directory a través de SSL
Dispositivo vRealize Log Insight	Servidor AD	3268	TCP	Catálogo global de Active Directory
Dispositivo vRealize Log Insight	Servidor AD	3269	TCP	SSL de Catálogo global de Active Directory
Dispositivo vRealize Log Insight	Servidor AD	88	TCP, UDP	Kerberos

Origen	Destino	Puerto	Protocolo	Descripción del servicio
Dispositivo vRealize Log Insight	vCenter Server	443	TCP	Servicio web de vCenter Server
Dispositivo vRealize Log Insight	Dispositivo vRealize Operations Manager	443	TCP	Servicio web de vRealize Operations
Dispositivo vRealize Log Insight	Administrador del registro de terceros	514	TCP, UDP	Datos de syslog
Dispositivo vRealize Log Insight	Administrador del registro de terceros	9000	CFAPI	Tráfico de la API de consumo de Log Insight saliente (CFAPI) configurado como un destino de reenvío
Dispositivo vRealize Log Insight	Administrador del registro de terceros	9543	CFAPI	Tráfico de la API de consumo de Log Insight saliente (CFAPI) configurado como un destino de reenvío cifrado (SSL/TLS)

Puertos que se pueden bloquear

Los siguientes puertos están abiertos, pero vRealize Log Insight no lo utiliza. Estos puertos se pueden bloquear con un firewall sin problemas.

Destino	Puerto	Protocolo	Descripción del servicio
Dispositivo vRealize Log Insight	111	TCP, UDP	Servicio RPCbind que convierte números de programa RPC en direcciones universales
Servicio Tomcat del dispositivo de vRealize Log Insight	9007	TCP	Servicios Tomcat

Supervisar el estado de los agentes de Windows y Linux de vRealize Log Insight

7

Puede supervisar el estado de los agentes de Windows y Linux de vRealize Log Insight y visualizar las estadísticas actuales de su operación.

Solo los agentes que estén configurados para enviar datos a través de CFAPI aparecen en la página Agentes. Los agentes que se configuran para enviar datos a través de syslog aparecen en la página Hosts, al igual que otros orígenes de syslog.

NOTA: Si cambia una IP de host para un servidor de vRealize Log Insight en la configuración del agente, el agente restablece el estado de la página a cero.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **View Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Administración, haga clic en **Agentes**.

Qué hacer a continuación

Puede utilizar la información de la página Agentes para supervisar el funcionamiento de los agentes de Windows y Linux de vRealize Log Insight instalados.

Habilitar la actualización automática de los agentes desde el servidor



Puede habilitar la actualización automática para todos los agentes desde el servidor de vRealize Log Insight.

La actualización automática aplica la última actualización disponible a todos los agentes conectados al servidor. Puede deshabilitar la función de actualización automática para cada servidor. Para ello, edite el archivo `liagent.ini` del agente. Para obtener más información, consulte *Trabajar con agentes de vRealize Log Insight*.

La actualización automática está deshabilitada para el servidor de forma predeterminada.

Prerequisitos

Los agentes deben tener un estado activo y la versión 4.3 o una versión posterior.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Haga clic en **Agentes** en el menú de la izquierda.
- 3 Haga clic en el botón de alternancia **Habilitar actualización automática para todos los agentes** en la página Agentes.

Los agentes conectados a este servidor se actualizan cuando existe una actualización.

Trabajar con grupos de agentes

Usando el servidor de vRealize Log Insight, puede configurar agentes desde el interior de la interfaz de usuario de la aplicación. Los agentes sondean el servidor de vRealize Log Insight en forma regular para determinar si hay disponibles configuraciones nuevas.

Puede agrupar los agentes que requieren la misma configuración. Por ejemplo, puede agrupar todos los agentes de Windows de vRealize Log Insight en forma separada de los agentes de Linux de vRealize Log Insight.

En el menú **Todos los agentes**, se enumeran automáticamente todos los grupos de agentes existentes de los paquetes de contenidos. Los agentes enumerados se relacionan con paquetes de contenido que ya ha instalado (por ejemplo, el paquete de contenido vSphere) que utilizan grupos de agentes.

Los grupos del paquete de contenido son de solo lectura.

Solo las secciones de configuración que comienzan con `[winlog]`, `[filelog]` y `[parser]` se utilizan en los paquetes de contenido. Las secciones adicionales no se exportan como parte de un paquete de contenido. Solo los comentarios de línea simple (las líneas que comienzan con `;`) de las secciones `[winlog]`, `[filelog]` y `[parser]` se preservan en un paquete de contenido.

Consulte *Trabajar con agentes de vRealize Log Insight* para obtener información sobre la configuración de agentes, que incluye información sobre la combinación de configuraciones entre los ajustes locales y del lado del servidor.

- [Fusión de configuraciones de grupos de agentes](#)

Con grupos de agentes, los agentes pueden ser parte de múltiples grupos y pueden pertenecer al grupo predeterminado *Todos los agentes*, lo cual permite la configuración centralizada.

- [Crear un grupo de agentes](#)

Puede crear un grupo de agentes que estén configurados con los mismos parámetros.

- [Editar un grupo de agentes](#)

Puede editar el nombre y la descripción de un grupo de agentes, cambiar los filtros y editar la configuración.

- [Añadir un grupo de agentes de paquetes de contenidos como grupo de agentes](#)

Puede añadir un grupo de agentes que se definió como parte de un paquete de contenidos a sus grupos activos y aplicar una configuración de agentes al grupo.

- [Eliminar un grupo de agentes](#)

Puede eliminar un grupo de agentes para eliminarlo de la lista de grupos activos.

Fusión de configuraciones de grupos de agentes

Con grupos de agentes, los agentes pueden ser parte de múltiples grupos y pueden pertenecer al grupo predeterminado *Todos los agentes*, lo cual permite la configuración centralizada.

La fusión ocurre del lado del servidor, y la configuración resultante se fusiona con la configuración del lado del agente. La configuración fusionada es el resultado de las siguientes reglas.

- Las configuraciones de grupos individuales tienen mayor prioridad y sustituyen los parámetros de todas las configuraciones de grupos de agentes.
- La configuración del grupo Todos los agentes sustituye a la configuración local.
- No se puede configurar secciones con el mismo nombre en grupos diferentes excepto con el grupo Todos los agentes. Sin embargo, las secciones de los grupos individuales tienen mayor prioridad.

NOTA: Para evitar la pérdida de agentes, los parámetros **nombre de host** y **puerto** de una configuración de agentes no se pueden cambiar de forma centralizada desde el servidor.

La configuración fusionada se guarda en el archivo `liagent-effective.ini` del lado del agente.

Crear un grupo de agentes

Puede crear un grupo de agentes que estén configurados con los mismos parámetros.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Administración, haga clic en **Agentes**.
- 3 En el menú **Todos los agentes**, haga clic en **Nuevo grupo**.
- 4 Proporcione un nombre exclusivo y una descripción para el grupo de agentes y haga clic en **Nuevo grupo**.

El grupo de agentes se crea y aparece en la lista **Todos los agentes** pero no se guarda.

- 5 Especifique uno o más de los siguientes filtros para el grupo de agentes.

Los filtros pueden contener caracteres comodín como * y ?.

- Dirección IP
- nombre de host

- versión
- SO

Por ejemplo, puede seleccionar el filtro del SO `contains` y especificar el valor `windows` para identificar todos los agentes de Windows para configuración.

- 6 Especifique los valores de configuración de agentes en el área Configuración de agentes y haga clic en **Guardar nuevo grupo**.

La configuración de agentes se aplicará después del siguiente intervalo de sondeo.

Editar un grupo de agentes

Puede editar el nombre y la descripción de un grupo de agentes, cambiar los filtros y editar la configuración.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Administración, haga clic en **Agentes**.
- 3 En el menú **Todos los agentes**, seleccione el nombre del grupo de agentes adecuado y haga clic en el icono del lápiz para editarlo.
- 4 Realice los cambios.

Elemento para editar	Acción
Nombre o Descripción	Realice los cambios necesarios y haga clic en Guardar .
Filtros o Configuración	Realice los cambios necesarios y haga clic en Guardar grupo .

Añadir un grupo de agentes de paquetes de contenidos como grupo de agentes

Puede añadir un grupo de agentes que se definió como parte de un paquete de contenidos a sus grupos activos y aplicar una configuración de agentes al grupo.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Administración, haga clic en **Agentes**.
- 3 En el menú **Todos los agentes**, seleccione una plantilla de agente para la lista Plantillas disponibles.
- 4 Haga clic en **Copiar plantilla** para copiar el grupo de agentes de paquetes de contenidos en sus grupos activos.
- 5 Haga clic en **Copiar**.
- 6 Seleccione los filtros necesarios y haga clic en **Guardar nuevo grupo**.

El grupo de agentes de paquetes de contenidos se añadirá a los grupos activos y los agentes se configurarán de acuerdo con los filtros especificados.

Eliminar un grupo de agentes

Puede eliminar un grupo de agentes para eliminarlo de la lista de grupos activos.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Administración, haga clic en **Agentes**.
- 3 In el menú **Todos los agentes**, seleccione el nombre del grupo de agentes que desea eliminar haciendo clic en el icono X que está junto al nombre.
- 4 Haga clic en **Eliminar**.

El grupo de agentes queda eliminado de los grupos activos.

Configurar y utilizar vRealize Log Insight Importer

10

vRealize Log Insight Importer es una herramienta de línea de comandos que se utiliza para importar registros sin conexión de datos del historial de máquinas locales al servidor vRealize Log Insight.

vRealize Log Insight es una herramienta de análisis de registros en tiempo real que transmite eventos de syslog o eventos de agentes a vRealize Log Insight, pero es posible que, en ocasiones, sea necesario importar registros que se recopilaban en el pasado. Con vRealize Log Insight Importer puede importar paquetes de soporte y registros archivados para recopilar datos que se recopilaban a lo largo de un período. Puede analizar los registros de los paquetes de compatibilidad recopilados desde vRealize Log Insight o de cualquier producto VMware.

vRealize Log Insight Importer incluye las siguientes funciones y utilidades.

- vRealize Log Insight Importer envía datos mediante API de consumo.
- Admite la recopilación de registros de archivos (filelog), incluida la recopilación recursiva de directorios.
- Importer puede leer los datos de archivos zip, tar o gz.
- Puede especificar que los datos se lean de forma recursiva desde un archivo anidado, como un archivo zip anidado, o especificar un directorio dentro de un archivo.
- 7-Zip no es compatible.

Uso de vRealize Log Insight Importer

Asegúrese de que vRealize Log Insight tenga acceso al servidor NFS en el que están almacenados los datos archivados. Si no es posible acceder al servidor NFS debido a un error de red o a errores en el servidor NFS, los datos archivados podrían no importarse correctamente. Tenga en cuenta que se aplican las siguientes restricciones cuando trabaje con vRealize Log Insight Importer.

Cuando los registros se extraen de un paquete durante el consumo, se determina automáticamente un nombre del paquete de registro y se agrega como una etiqueta de paquete a los registros extraídos. El nombre de etiqueta corresponde al nombre de archivo del registro o al nombre de directorio en el caso de los orígenes de directorios. Las etiquetas diferencian a los paquetes en un servidor vRealize Log Insight.

Esta etiqueta reemplaza las etiquetas con el mismo nombre que se especifican en el archivo de manifiesto. La etiqueta se puede reemplazar por una etiqueta de línea de comandos que usa el mismo nombre.

Se aplican las siguientes limitaciones:

- vRealize Log Insight Importer no busca espacio de disco disponible en el dispositivo virtual de vRealize Log Insight. Por lo tanto, los registros archivados podrían no importarse correctamente si el dispositivo virtual se queda sin espacio de disco.
- vRealize Log Insight no muestra la información de progreso durante la importación de registros. Mientras se lleva a cabo la importación de los datos archivados, la consola no muestra información sobre el tiempo que queda para finalizar la importación ni sobre la cantidad de datos que ya se han importado.

Sistemas operativos compatibles

La herramienta vRealize Log Insight Importer es compatible con los siguientes sistemas operativos:

- Windows de 32 bits y de 64 bits
- Linux de 32 bits y de 64 bits

La versión de Linux no se puede ejecutar en un sistema Apple Macintosh.

Este capítulo cubre los siguientes temas:

- [Acerca del archivo de manifiesto de vRealize Log Insight Importer](#)
- [Instalar, configurar y ejecutar vRealize Log Insight Importer](#)
- [Ejemplos de configuración de archivos de manifiesto de vRealize Log Insight Importer](#)
- [Parámetros de configuración de vRealize Log Insight Importer](#)

Acerca del archivo de manifiesto de vRealize Log Insight Importer

vRealize Log Insight Importer utiliza un archivo de configuración de manifiesto para determinar el formato de registro y especificar la ubicación de los datos para importar. El archivo de manifiesto tiene el mismo formato que el archivo de configuración `liagent.ini` y es similar en su estructura.

Puede crear sus propios archivos de manifiesto para importar archivos de registro arbitrarios. A pesar de que crear un archivo de manifiesto es opcional, si utiliza un archivo de manifiesto, no es necesario conocer la ruta de acceso absoluta a los archivos de datos.

Si no crea un archivo de manifiesto, vRealize Log Insight Importer utiliza el manifiesto predeterminado que recopila todos los archivos `.txt` y `.log` (`include=*.log*;*.txt*`) y aplica el analizador automático (extrae la marca de tiempo + kvp) en los registros extraídos.

Si se utiliza el archivo de configuración `liagent.ini` como archivo de manifiesto, vRealize Log Insight Importer extrae solamente las secciones `[filelog]` como un manifiesto. Todas las opciones de la sección `[filelog]` se admiten en vRealize Log Insight Importer.

Para obtener información sobre opciones adicionales admitidas en la sección [filelog] y ejemplos de configuración, consulte la documentación de agentes de vRealize Log Insight en la *Guía de administración de agentes de vRealize Log Insight*.

Para crear un archivo de manifiesto

Puede copiar y pegar los contenidos del archivo de configuración de agente en un nuevo archivo .txt. Para identificar una ruta de acceso dinámica, elimine el carácter "/" de inicio antes de la ruta de acceso del directorio.

Especificar la ruta de acceso del directorio

El directorio especificado en la sección [filelog] puede ser relativo al origen o absoluto. Para especificar una ruta de acceso relativa, no incluya la barra diagonal inicial bajo Linux; de lo contrario, vRealize Log Insight Importer tratará la ruta de acceso como absoluta.

Para indicar patrones de nombre en el valor de la clave de directorio, puede utilizar los caracteres * y **.

- Utilice * como marcador de posición para un directorio individual. Utilícelo para indicar un nivel de anidamiento con un nombre de carpeta arbitrario. Por ejemplo, utilice `directory = log_folder_*` para indicar cualquier carpeta que comience con la cadena `log_folder_`.
- Utilice ** para indicar un nivel de anidamiento arbitrario con cualquier nombre de carpeta. Por ejemplo, puede utilizar `directory = **/log` para indicar cualquier carpeta con el nombre `log` en cualquier nivel de anidamiento dentro del directorio de origen.

Instalar, configurar y ejecutar vRealize Log Insight Importer

Puede instalar vRealize Log Insight Importer en Windows o Linux. También puede instalar vRealize Log Insight Importer en un servidor vRealize Log Insight y ejecutarlo desde el servidor.

Prerequisitos

- Verifique que pueda acceder al sitio de [descargas de VMware](#) para descargar vRealize Log Insight Importer.
- Revise [Acerca del archivo de manifiesto de vRealize Log Insight Importer](#) y cree un archivo de manifiesto para usarlo con el importador. Para obtener más información, consulte [Ejemplos de configuración de archivos de manifiesto de vRealize Log Insight Importer](#).
- Revise [Parámetros de configuración de vRealize Log Insight Importer](#) para identificar los parámetros opcionales requeridos y disponibles.
- Si utiliza el parámetro `honor_timestamp`, verifique que posea las credenciales de inicio de sesión apropiadas.
- Si importa un paquete de soporte, deberá configurar el `honor_timestamp`, el nombre de usuario y la contraseña.

Procedimiento

- 1 Descargue el paquete de instalación de vRealize Log Insight Importer en el sitio de [descargas de VMware](#) e instale la herramienta en su sistema. Los paquetes de instalación incluyen el instalador MSI para Windows y paquetes de instalación POSIX (RPM, DEB y BIN) para Linux.

La herramienta vRealize Log Insight Importer se instala en las siguientes ubicaciones.

Sistema operativo	Nombre de archivo	Ubicación de instalación
Windows	loginsight-importer.exe	C:\Program Files (x86)\VMware\Log Insight Importer
Linux	loginsight-importer	/usr/lib/loginsight-importer

NOTA:

- Después de la instalación, el directorio de instalación de Importer se agrega a la variable de entorno PATH en Windows, y un vínculo simbólico al ejecutable `loginsight-importer` se agrega a `/usr/bin/` en Linux. Así el cliente puede llamar a `loginsight-importer` desde un shell sin especificar un prefijo de ruta de acceso.
- Cuando instala vRealize Log Insight Importer, también se instalan varios archivos de manifiesto de productos de VMware. Puede utilizar estos archivos o modificarlos de acuerdo a sus necesidades cuando ejecute vRealize Log Insight Importer. Estos archivos de manifiesto se encuentran en `C:\Program Files (x86)\VMware\Log Insight Importer\Manifests` en Windows y en `/usr/lib/loginsight-importer/manifests` en Linux.
- Si desinstala el paquete `.bin`, necesitará también eliminar el vínculo simbólico de `/usr/bin/loginsight_importer`.

- 2 Inicie la herramienta vRealize Log Insight Importer introduciendo el siguiente comando en un símbolo del sistema.

```
/usr/bin/loginsight-importer.exe
```

- 3 Introduzca el nombre del archivo de manifiesto cuando se le solicite.
- 4 Defina los parámetros de configuración y presione **Intro**.
vRealize Log Insight Importer comienza a extraer las entradas de registro de los directorios especificados en los parámetros. Se muestra el número total de archivos procesados, los mensajes de registros extraídos, los mensajes de registro enviados y el tiempo transcurrido.
- 5 Después de completar la importación, pulse **Ctrl+C** en Windows o Linux para salir de la herramienta.

Qué hacer a continuación

En la pestaña de análisis interactivo de vRealize Log Insight, puede actualizar la vista para enumerar los eventos de registro importados. Si importó un paquete de soporte y utilizó el honor_timestamp, el panel de control también debería mostrar los eventos a través del tiempo.

Ejemplos de configuración de archivos de manifiesto de vRealize Log Insight Importer

Los archivos de manifiesto de vRealize Log Insight Importer de muestra proporcionan ejemplos de configuraciones de parámetros.

El valor de la clave de directorio debe ser relativo al origen o absoluto. El siguiente ejemplo demuestra cómo recopilar registros de archivos con una extensión `.log` que residen dos niveles más bajos que el directorio de origen y el nombre con el que finaliza la última carpeta es la cadena `_log`.

```
[filelog|importer_test]
directory=**_log
include=*.log
event_marker=^\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2} [A-Z]{4} LOG
```

El siguiente ejemplo demuestra cómo recopilar todos los archivos con la extensión `.log` de todas las subcarpetas del directorio de origen, incluido el propio origen.

```
[filelog|sbimporter_test_channel]
directory = **
include = *.log
```

El siguiente ejemplo demuestra cómo recopilar registros de todos los archivos en el directorio de origen (pero no de las subcarpetas), excepto los archivos que tienen una extensión `.ini`. Interpretamos los archivos como codificados en UTF-16LE.

```
[filelog|quotes_channe3]
directory=
charset=UTF-16LE
exclude=*.ini
tags={"Provider" : "Apache"}
```

El siguiente ejemplo demuestra cómo recopilar registros de todos los archivos con la extensión `.log` en el directorio de origen (pero no de las subcarpetas). Se analiza la marca de tiempo de los eventos en el archivo de registro mediante el analizador de formato de registro común (Common Log Format, CLF) y se aplica la marca de tiempo histórica extraída. El formato de registro analizado por el analizador de CLF es `2015-03-25 22:11:46,786 | DEBUG | pool-jetty-76 | AuthorizationMethodInterceptor | Authorizing method: public abstract.`

```
[filelog|vcd-container-debug]
directory=
include=*.log
parser=vcd

[parser|vcd]
base_parser=clf
format=%Y-%m-%d %H:%M:%S%f)t %M
```

Parámetros de configuración de vRealize Log Insight Importer

La configuración de vRealize Log Insight Importer incluye parámetros obligatorios y opcionales.

Parámetros obligatorios	Descripción
<code>--source <ruta de acceso></code>	Especifica la ruta de acceso del directorio del paquete de soporte o la ruta de acceso del archivo zip, gzip o tar del paquete. El valor se agrega a todos los mensajes que se envían como el valor de la etiqueta <code>bundle</code> .
<code>--server <nombre de host></code>	Nombre de host o dirección IP del servidor de destino.
Opciones	Descripción
<code>--port <puerto></code>	Puerto para la conexión. Si no se configura, se utiliza el puerto 9000 para las conexiones que no son SSL y se utiliza el puerto 9543 para las conexiones SSL.
<code>--logdir <ruta de acceso></code>	Especifica la ruta de acceso del directorio de registros. Si no se configura, la ruta de acceso es: <code>\$ (LOCALAPPDATA)\VMware\Log Insight Importer\log</code> en Windows y <code>~/loginsight-importer/log</code> en Linux.
<code>--manifest <ruta de acceso de archivo></code>	Especifica la ruta de acceso del archivo del manifiesto (formato <code>.ini</code>). Si no se configura este parámetro, se utiliza el archivo <code>importer.ini</code> en el directorio de origen. Si el archivo <code>importer.ini</code> no existe o no se encuentra en el directorio de origen, vRealize Log Insight Importer aplicará el manifiesto predeterminado (codificado de forma rígida) y recopilará todos los archivos <code>.txt</code> y <code>.log</code> (incluyendo <code>*.log*;*.txt*</code>), y también aplicará el análisis automático (extrae marca de tiempo + kvp).
<code>--no_ssl</code>	No utilice SSL para las conexiones. Este parámetro no debe configurarse para las conexiones autenticadas (por ejemplo, si se utiliza <code>--honor_timestamp</code>).
<code>--ssl_ca_path <ruta de acceso></code>	Ruta de acceso del archivo del paquete de certificados raíz de confianza.
<code>--tags <etiquetas></code>	Configure etiquetas para todos los eventos enviados. Por ejemplo, <code>--tags "{ \"tag1\" : \"value1\", \"tag2\": \"value2\"}"</code> NOTA: La opción <code>tags</code> puede aceptar el valor <code>nombre de host</code> como nombre de etiqueta. Se utiliza el valor de la etiqueta <code>nombre de host</code> de la línea de comandos en lugar del FQDN de la máquina que realiza el envío como valor del campo <code>nombre de host</code> para todos los eventos extraídos por vRealize Log Insight Importer. Esto es opuesto al parámetro de etiquetas en el archivo de manifiesto y los campos extraídos por los analizadores, que ignoran el campo <code>nombre de host</code> . El nombre del paquete de registro, ya sea un nombre de archivo o un nombre de directorio en el caso de orígenes de directorios, se determina automáticamente y se agrega como una etiqueta <code>paquete</code> a todos los registros extraídos de ese paquete específico durante el consumo. Esta etiqueta le ayuda a diferenciar los paquetes en el servidor vRealize Log Insight. Una etiqueta <code>paquete</code> reemplaza las etiquetas con el mismo nombre en el archivo de manifiesto. Sin embargo, se puede reemplazar por etiquetas de la línea de comandos si existe una con el nombre <code>paquete</code> .
<code>--username <nombre de usuario></code>	Nombre de usuario para la autenticación. Se requiere si <code>--honor_timestamp</code> se encuentra configurado.

Opciones	Descripción
<code>--password <contraseña></code>	Contraseña para la autenticación. Se requiere si <code>--honor_timestamp</code> se encuentra configurado. El par de nombre de usuario y contraseña deshabilita la desviación horaria permitida en el servidor vRealize Log Insight, por lo que es posible importar datos con una marca de tiempo histórica.
<code>--honor_timestamp</code>	<p>Aplica la marca de tiempo extraída. Los analizadores configurados extraen la marca de tiempo de las entradas de registro y <code>--honor_timestamp</code> aplica la marca de tiempo extraída.</p> <ul style="list-style-type: none"> ■ Si la marca de tiempo se extrae mediante analizadores configurados, se aplicará esa marca de tiempo a los eventos. ■ Si existe un evento en el archivo de registros, sin una marca de tiempo extraída, se aplicará la marca de tiempo extraída correctamente del evento anterior en el mismo archivo de registro. ■ Si no se encuentra o no se analiza ninguna marca de tiempo en el archivo, se aplicará el valor de <code>MTIME</code> del archivo de registro como marca de tiempo. <p>NOTA: Si no se proporcionó un archivo de manifiesto, el manifiesto con codificación rígida predeterminado que vRealize Log Insight Importer utilizará tendrá el analizador de registros automáticos habilitado. En tal caso, vRealize Log Insight Importer extrae la marca de tiempo de las entradas de registro si se usa el parámetro <code>--honor_timestamp</code>.</p>
<code>--debug_level <1 2></code>	Aumenta el nivel de detalle del archivo de registro. Este parámetro solamente se debe cambiar al realizar procesos de solución de problemas. En condiciones de funcionamiento normal, esta marca no debe usarse.
<code>--help</code>	Muestra la ayuda y sale.

Supervisar vRealize Log Insight

Puede supervisar el dispositivo virtual de vRealize Log Insight y los hosts y dispositivos que envían eventos de registro a vRealize Log Insight.

Este capítulo cubre los siguientes temas:

- [Revisar el estado del dispositivo virtual vRealize Log Insight](#)
- [Supervisar hosts que envían eventos de registro](#)

Revisar el estado del dispositivo virtual vRealize Log Insight

Puede revisar los recursos disponibles y las consultas activas en el dispositivo virtual vRealize Log Insight, y ver las estadísticas actuales acerca del funcionamiento de vRealize Log Insight.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **System Monitor**.
- 3 Si vRealize Log Insight se ejecuta como un clúster, haga clic en **Mostrar recursos para** y escoja el nodo que desea supervisar.

- 4 Haga clic en los botones de la página Supervisión del sistema para ver la información que necesita.

Opción	Descripción
Recursos	<p>Vea información acerca de la CPU, la memoria, las IOPS (actividad de lectura y escritura), y el uso del almacenamiento en el dispositivo virtual vRealize Log Insight.</p> <p>Los gráficos de la derecha representan los datos históricos de las últimas 24 horas y se actualizan a intervalos de 5 minutos. Los gráficos de la izquierda muestran información de los últimos 5 minutos y se actualizan cada tres segundos.</p>
Consultas activas	Vea información acerca de las consultas que están actualmente activas en vRealize Log Insight.
Estadísticas	<p>Vea las estadísticas sobre las operaciones y tasas de consumo de registros.</p> <p>Para ver estadísticas más detalladas, haga clic en Mostrar estadísticas avanzadas.</p>

Qué hacer a continuación

Puede utilizar la información de la página Supervisión del sistema para administrar los recursos del dispositivo virtual vRealize Log Insight.

Supervisar hosts que envían eventos de registro

Puede visualizar una lista de todos los hosts y dispositivos que envían eventos de registro a vRealize Log Insight y supervisarlos.

Las entradas en las tablas de los hosts caducan tres meses después del último evento registrado.

Prerequisitos

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Administración, haga clic en **Hosts**.

NOTA: Si ha configurado un servidor vCenter Server para que envíe eventos y alarmas pero no ha configurado los diferentes hosts ESXi para que envíen los registros, la columna Nombre de host enumera el servidor vCenter Server y los hosts ESXi individuales como el origen en lugar de enumerar solo el servidor vCenter Server.

Integración de vRealize Log Insight con productos VMware

12

vRealize Log Insight puede integrarse con otros productos VMware para usar eventos y datos de registro, y proporcionar mejor visibilidad de eventos que suceden en un entorno virtual.

Integración con VMware vSphere

Los usuarios administradores de vRealize Log Insight pueden configurar vRealize Log Insight para que se conecte con sistemas vCenter Server en intervalos de dos minutos, y recopile datos de eventos, alarmas y tareas de estos sistemas vCenter Server. Además, vRealize Log Insight puede configurar hosts ESXi a través de vCenter Server. Consulte [Conectar vRealize Log Insight a un entorno vSphere](#).

Integración con VMware vRealize Operations Manager

Es posible integrar vRealize Log Insight con la vApp de vRealize Operations Manager y la versión instalable de vRealize Operations Manager. La integración con la versión instalable requiere cambios adicionales en la configuración de vRealize Operations Manager. Para obtener información sobre la configuración de la versión instalable de vRealize Operations Manager para la integración con vRealize Log Insight, consulte la *Guía de introducción a Log Insight*.

vRealize Log Insight y vRealize Operations Manager pueden integrarse en dos formas independientes.

Eventos de notificación Los usuarios administradores de vRealize Log Insight pueden configurar vRealize Log Insight para que envíe eventos de notificación a vRealize Operations Manager en función de las consultas que cree. Consulte [Configurar vRealize Log Insight para enviar eventos de notificación a vRealize Operations Manager](#).

Ejecución en contexto Ejecutar en contexto es una función de vRealize Operations Manager que le permite iniciar una aplicación externa a través de una URL en un contexto específico. El contexto se define por el elemento de la UI activo y la selección de objetos. Ejecutar en contexto permite al adaptador de vRealize Log Insight añadir elementos de menú a numerosas vistas

diferentes dentro de la interfaz de usuario personalizada y la interfaz de usuario de vSphere de vRealize Operations Manager. Consulte [Habilitar ejecución en contexto para vRealize Log Insight en vRealize Operations Manager](#).

NOTA: Los eventos de notificación no dependen de la configuración de la ejecución en contexto. Puede enviar eventos de notificación de vRealize Log Insight a vRealize Operations Manager, incluso si no habilita la función de inicio en contexto.

Si el entorno cambia, los usuarios administradores de vRealize Log Insight pueden cambiar, añadir o eliminar sistemas vSphere de vRealize Log Insight, cambiar o eliminar la instancia de vRealize Operations Manager a la que se envían las notificaciones de alerta, y cambiar las contraseñas que se usan para conectarse a sistemas vSphere y vRealize Operations Manager.

Este capítulo cubre los siguientes temas:

- [Conectar vRealize Log Insight a un entorno vSphere](#)
- [Configure vRealize Log Insight para extraer eventos, tareas y alarmas desde la instancia de vCenter Server.](#)
- [Uso de vRealize Operations Manager con vRealize Log Insight](#)
- [Paquete de contenido de vRealize Operations Manager para vRealize Log Insight](#)

Conectar vRealize Log Insight a un entorno vSphere

Antes de configurar vRealize Log Insight para que recopile datos de alarmas, eventos y tareas desde su entorno vSphere, debe conectar vRealize Log Insight a uno o más sistemas vCenter Server.

vRealize Log Insight puede recopilar dos tipos de datos desde las instancias de vCenter Server y los hosts ESXi que administran.

- Los eventos, tareas y alertas son datos estructurados con un significado específico. Si están configurados, vRealize Log Insight extrae eventos, tareas y alertas de las instancias de vCenter Server registradas.
- Los registros contienen datos desestructurados que se pueden analizar en vRealize Log Insight. Los hosts de ESXi o las instancias de vCenter Server Appliance pueden introducir sus registros en vRealize Log Insight mediante syslog.

Prerequisitos

- Para el nivel de integración que desea lograr, verifique que tenga las credenciales de usuario con privilegios suficientes para realizar la configuración necesaria en el sistema de vCenter Server y los hosts de ESXi.

Nivel de integración	Privilegios requeridos
Recopilación de eventos, tareas y alarmas	<ul style="list-style-type: none"> ■ System.View <p>NOTA: System.View es un privilegio definido por el sistema. Cuando añade una función personalizada y no le asigna privilegios, la función se crea como de solo lectura con tres privilegios definidos por el sistema: System.Anonymous, System.View y System.Read.</p>
Configuración de syslog en los hosts de ESXi	<ul style="list-style-type: none"> ■ Host.Configuración.Modificación de ajustes ■ Host.Configuración.Configuración de red ■ Host.Configuración.Configuración avanzada ■ Host.Configuración.Perfil de seguridad y firewall

NOTA: Debe configurar el permiso de la carpeta de nivel superior dentro del inventario de vCenter Server y verificar que esté marcada la casilla **Propagar a objetos secundarios**.

- Compruebe que conoce la dirección IP o el nombre de dominio del sistema vCenter Server.
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Integración, haga clic en **vSphere**.
- 3 Escriba la dirección IP y las credenciales para un vCenter Server, y haga clic en **Probar conexión**.
Se recomienda utilizar las credenciales de la cuenta de servicio.
- 4 (Opcional) Para registrar otro vCenter Server, haga clic en **Añadir vCenter Server** y repita los pasos 3 a 5.

NOTA: No registre sistemas vCenter Server con nombres o direcciones IP duplicados. vRealize Log Insight no comprueba la existencia de nombres de vCenter Server duplicados. Deberá comprobar que la lista de sistemas vCenter Server registrados no contiene entradas duplicadas.

- 5 Click **Save**.

Qué hacer a continuación

- Comience a recopilar datos de eventos, tareas y alarmas desde la instancia de vCenter Server que registró. Consulte [Configure vRealize Log Insight para extraer eventos, tareas y alarmas desde la instancia de vCenter Server](#).

- Comience a recopilar los feeds de syslog desde los hosts ESXi que administra el vCenter Server. Consulte [Configurar un host ESXi para que reenvíe eventos de registro a vRealize Log Insight](#).

vRealize Log Insight como servidor de Syslog

vRealize Log Insight incluye un servidor syslog integrado que está activo de manera constante cuando se ejecuta el servicio vRealize Log Insight.

El servidor syslog escucha puertos 514/TCP, 1514/TCP y 514/UDP, y está preparado para consumir mensajes de registro que se envían desde otros hosts. Los mensajes que consume el servidor syslog pueden buscarse en la interfaz de usuario web de vRealize Log Insight prácticamente en tiempo real. La longitud máxima del mensaje de syslog que acepta vRealize Log Insight es 10 KB.

Configurar un host ESXi para que reenvíe eventos de registro a vRealize Log Insight

Los hosts ESXi o las instancias de vCenter Server Appliance generan datos de registro no estructurados que se pueden analizar en vRealize Log Insight.

Use la interfaz de administración de vRealize Log Insight para configurar los hosts ESXi en un vCenter Server registrado a fin de incorporar los datos de syslog a vRealize Log Insight.

ADVERTENCIA: Ejecutar tareas paralelas de configuración podría provocar una configuración incorrecta de syslog en los hosts ESXi de destino. Compruebe que no haya otro usuario administrativo configurando los hosts ESXi que usted intenta configurar.

Un clúster vRealize Log Insight puede utilizar un equilibrador de carga integrado para distribuir ESXi y feeds de syslog de vCenter Server Appliance entre los nodos individuales del clúster.

Para obtener información sobre el filtrado de mensajes de syslog en hosts ESXi antes de que los mensajes se envíen a vRealize Log Insight, consulte el tema *Configurar filtrado de registros en hosts ESXi* en la sección [Instalación de ESXi](#) de la guía de **Instalación y configuración de vSphere**.

Para obtener información sobre la configuración de feeds de syslog desde un vCenter Server Appliance, consulte [Configurar vCenter Server para que reenvíe eventos de registro a vRealize Log Insight](#).

NOTA: vRealize Log Insight puede recibir datos de syslog desde hosts ESXi de la versión 5.5 y superiores.

Prerequisitos

- Compruebe que el vCenter Server que administra el host ESXi esté registrado con su instancia de vRealize Log Insight. O bien, puede registrar el host ESXi y configurar vCenter Server en una sola operación.
- Verifique que tenga credenciales de usuario con privilegios suficientes como para configurar syslog en los hosts de ESXi.
 - **Host.Configuración.Configuración avanzada**

- **Host.Configuración.Perfil de seguridad y firewall**

NOTA: Debe configurar el permiso de la carpeta de nivel superior dentro del inventario de vCenter Server y verificar que esté marcada la casilla **Propagar a objetos secundarios**.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Integración, haga clic en **vSphere**.
- 3 Localice la instancia de vCenter Server que administra el host ESXi desde la que desea recibir feeds de syslog.
- 4 Seleccione la casilla de verificación **Configurar hosts ESXi para que envíen registros a Log Insight**.

De forma predeterminada, vRealize Log Insight configura todos los hosts ESXi disponibles de la versión 5.5 y superiores para que envíen sus registros mediante UDP.
- 5 (Opcional) Para modificar los valores de configuración predeterminados, haga clic en **Opciones avanzadas**.
 - Para cambiar el protocolo de todos los hosts ESXi, seleccione **Configurar todos los host ESXi**, elija un protocolo y haga clic en **Aceptar**.
 - Para configurar solo el registro de hosts ESX específicos o cambiar el protocolo de hosts ESXi seleccionados, siga estos pasos:
 - a Seleccione **Configurar hosts ESXi específicos**.
 - b Elija uno o varios hosts de la lista **Filtrar por host**.
 - c Establezca el valor del protocolo.
 - d Haga clic en **Aceptar**.
- 6 (Opcional) Si utiliza clústeres, abra el menú desplegable del cuadro de texto **Destino** y seleccione el nombre de host o la dirección IP del equilibrador de carga que distribuye feeds de syslog.
- 7 Click **Save**.

Modificar una configuración de host ESXi para reenviar eventos de registro a vRealize Log Insight

Los hosts ESXi o las instancias de vCenter Server Appliance generan datos de registro no estructurados que se pueden analizar en vRealize Log Insight.

Use la interfaz de administración de vRealize Log Insight para configurar los hosts ESXi en un vCenter Server registrado a fin de incorporar los datos de syslog a vRealize Log Insight.

ADVERTENCIA: Ejecutar tareas paralelas de configuración podría provocar una configuración incorrecta de syslog en los hosts ESXi de destino. Compruebe que no haya otro usuario administrativo configurando los hosts ESXi que usted intenta configurar.

Tras realizarse la configuración inicial, puede habilitar una opción para configurar automáticamente un host ESXi con el protocolo predeterminado cuando se agrega a un clúster.

Un clúster vRealize Log Insight puede utilizar un equilibrador de carga integrado para distribuir ESXi y feeds de syslog de vCenter Server Appliance entre los nodos individuales del clúster.

Para obtener información sobre el filtrado de mensajes de syslog en hosts ESXi antes de que los mensajes configurados se envíen a vRealize Log Insight, consulte el tema *Configurar filtrado de registros en hosts ESXi* en la sección [Instalación de ESXi](#) de la guía de **Instalación y configuración de vSphere**.

Para obtener información sobre la configuración de feeds de syslog desde un vCenter Server Appliance, consulte [Configurar vCenter Server para que reenvíe eventos de registro a vRealize Log Insight](#).

NOTA: vRealize Log Insight puede recibir datos de syslog desde hosts ESXi de la versión 5.5 y superiores.

Prerequisitos

- Compruebe que el vCenter Server que administra el host ESXi esté registrado con su instancia de vRealize Log Insight.
- Verifique que tenga credenciales de usuario con privilegios suficientes como para configurar syslog en los hosts de ESXi.
 - **Host.Configuración.Configuración avanzada**
 - **Host.Configuración.Perfil de seguridad y firewall**

NOTA: Debe configurar el permiso de la carpeta de nivel superior dentro del inventario de vCenter Server y verificar que esté marcada la casilla **Propagar a objetos secundarios**.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Integración, haga clic en **vSphere**.
- 3 Seleccione la casilla de verificación **Configurar hosts ESXi para que envíen registros a Log Insight**.
- 4 Haga clic en **Opciones avanzadas**.
- 5 Para cambiar el protocolo de los hosts ESXi seleccionados, siga estos pasos:
 - a Elija uno o varios hosts de la lista **Filtrar por host**.
 - b Establezca el valor del protocolo.
 - c Si desea tener un host ESXi configurado automáticamente con el protocolo predeterminado cuando se añade a un clúster vRealize Log Insight, seleccione **Configurar automáticamente todos los host ESXi**.
 - d Haga clic en **Configurar**.

- 6 (Opcional) Si utiliza clústeres, puede especificar un equilibrador de carga: abra el menú desplegable para el cuadro de texto **Destino** en la pantalla **Integración de vSphere** y seleccione el nombre de host o la dirección IP para el equilibrador de cargas.

Eventos de notificación de vRealize Log Insight en vRealize Operations Manager

Puede configurar vRealize Log Insight para que envíe eventos de notificación a vRealize Operations Manager en función de las consultas de alertas que cree.

Cuando configure una alerta de notificación en vRealize Log Insight, seleccione un recurso en vRealize Operations Manager que esté asociado a los eventos de notificación. Consulte [Añadir una consulta de alerta en Log Insight para enviar eventos de notificación a vRealize Operations Manager](#).

A continuación, aparecen las secciones de la interfaz de usuario de vRealize Operations Manager donde aparecen los eventos de notificación.

- Inicio > panel **Recomendaciones** > widget **Principales alertas de estado de descendientes**
- Inicio > pestaña **Alertas**
- En todos los paneles personalizados donde haya widgets con eventos de notificación

Para obtener más información sobre dónde se muestran eventos de notificación, consulte el [Centro de documentación de VMware vRealize Operations Manager](#).

Configurar vCenter Server para que reenvíe eventos de registro a vRealize Log Insight

La integración de vSphere recopila tareas y eventos de vCenter Server, pero no los registros internos de nivel inferior de cada componente de vCenter Server. Estos registros los utiliza el paquete de contenido de vSphere.

La configuración de vCenter Server 6.5 y versiones posteriores debe realizarse a través de la interfaz de administración de vCenter Server Appliance. Para obtener más información sobre cómo reenviar eventos de registro de vCenter Server, consulte la documentación de vSphere acerca del redireccionamiento de archivos de registro de vCenter Server Appliance a otra máquina.

En el caso de las versiones anteriores de vSphere, aunque vCenter Server Appliance incluye un daemon de syslog que podría usarse para enrutar registros, el método preferido consiste en instalar un agente de vRealize Log Insight.

Para obtener información sobre cómo instalar agentes de vRealize Log Insight, consulte la *Guía de administración del agente de vRealize Log Insight* en el [Centro de información de vRealize Log Insight](#).

El paquete de contenido de vSphere contiene grupos de agentes que definen qué archivos de registro específicos se deben recopilar de las instalaciones de vCenter Server. La configuración puede consultarse en `https://LogInsightServerFqdn0rIP/contentpack?contentPackId=com.vmware.vsphere`.

Para obtener información sobre cómo trabajar con grupos de agentes, consulte [Capítulo 9 Trabajar con grupos de agentes](#)

Para obtener información sobre las ubicaciones de los archivos de registro de vCenter Server, consulte <http://kb.vmware.com/kb/1021804> y <http://kb.vmware.com/kb/1021806>.

Configure vRealize Log Insight para extraer eventos, tareas y alarmas desde la instancia de vCenter Server .

Los eventos, tareas y alertas son datos estructurados con un significado específico. Puede configurar vRealize Log Insight para que recopile datos de alarmas, eventos y tareas desde uno o más sistemas de vCenter Server.

Use la UI de administración para configurar vRealize Log Insight para que se conecte con los sistemas vCenter Server. La información se extrae de los sistemas vCenter Server mediante el uso de la API de servicios web de vSphere y aparece como un paquete de contenidos vSphere en la interfaz de usuario web de vRealize Log Insight.

NOTA: vRealize Log Insight puede extraer datos de alarmas, eventos y tareas únicamente desde vCenter Server 5.1 y superiores.

Prerequisitos

Compruebe que tiene credenciales de usuario con privilegios de **System.View**.

NOTA: Debe configurar el permiso de la carpeta de nivel superior dentro del inventario de vCenter Server y verificar que esté marcada la casilla **Propagar a objetos secundarios**.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 En Integración, haga clic en **vSphere**.
- 3 Localice la instancia de vCenter Server desde donde desea recopilar los datos y marque la casilla de verificación **Recopilar eventos, tareas y alarmas de vCenter Server**.
- 4 Click **Save**.

vRealize Log Insight se conecta con el vCenter Server cada dos minutos y consume toda la información nueva desde el último sondeo exitoso.

Qué hacer a continuación

- Analice los eventos de vSphere usando el paquete de contenidos de vSphere o las consultas personalizadas.
- Habilite las alertas de paquetes de contenidos de vSphere o las alertas personalizadas.

Uso de vRealize Operations Manager con vRealize Log Insight

Requisitos de la integración con vRealize Operations Manager

Para integrar vRealize Log Insight con vRealize Operations Manager, debe especificar credenciales para vRealize Log Insight para autenticarse en vRealize Operations Manager. vRealize Operations Manager admite cuentas de usuario locales y múltiples orígenes LDAP.

Para determinar el nombre de usuario para una cuenta de usuario local:

- 1 Abra la interfaz web de vRealize Operations Manager.
- 2 Seleccione **Control de acceso**.
- 3 Identifique o cree el usuario de integración. El campo Tipo de origen es **Usuario local**.
- 4 El nombre de usuario que debe introducirse dentro de la interfaz de usuario de administración de vRealize Log Insight es el contenido del campo **Nombre de usuario**.

Para determinar el formato del nombre de usuario para la cuenta de usuario LDAP que se debe proporcionar en vRealize Log Insight, siga estas instrucciones:

- 1 Abra la interfaz web de vRealize Operations Manager.
- 2 Seleccione Control de acceso.
- 3 Identifique o cree el usuario de integración. Tenga en cuenta los campos **Nombre de usuario** y **Tipo de origen**. Por ejemplo, un usuario con el nombre **integration@example.com** del origen **Active Directory: ad**.
- 4 Seleccione **Orígenes de autenticación**.
- 5 Identifique el origen de autenticación correspondiente al **Tipo de origen** del Paso 3. Tenga en cuenta el campo **Nombre mostrado del origen**. Por ejemplo, "ad".
- 6 El nombre de usuario que debe introducirse dentro de la interfaz de usuario de administración de vRealize Log Insight se combina desde el Paso 3 y el Paso 5, en el formato **Nombre_de_usuario@Nombre_para_mostrar_de_origen**. Por ejemplo, **integration@example.com@ad**.

Prerequisitos

Compruebe que la cuenta de usuario de integración tiene permisos para manipular objetos en vRealize Operations Manager. Consulte [Permisos necesarios mínimos de una cuenta de usuario local o de Active Directory](#).

Permisos necesarios mínimos de una cuenta de usuario local o de Active Directory

Para integrar vRealize Log Insight con vRealize Operations Manager, debe especificar credenciales para vRealize Log Insight para autenticarse en vRealize Operations Manager. Para poder manipular objetos en vRealize Operations Manager, una cuenta de usuario debe tener los permisos necesarios correspondientes.

Licencia de vRealize Operations Manager

Si asigna a un usuario permisos de ejecución en contexto, el usuario también puede configurar la integración de alertas. Use la información de la tabla de integración de alertas para asignar permisos únicamente para la integración de alertas.

Tabla 12-1. Integración de alertas

Acción	Permisos y objetos que seleccionar
Crear una función personalizada con los permisos de la lista.	<ol style="list-style-type: none"> 1 Administración -> Administración de clases de recursos [Seleccionar todo] 2 Administración -> Administración de recursos [Seleccionar todo] 3 Administración -> API REST <ol style="list-style-type: none"> a Todas las demás API de lectura y escritura b Acceso de lectura a API
Asignar la función anterior al usuario local o de Active Directory (sea nuevo o ya existente) y seleccionar objetos/jerarquías de objetos para asignarlos.	<ol style="list-style-type: none"> 1 Instancia de adaptador -> vRealizeOpsMgrAPI [Seleccionar todo] 2 Hosts y clústeres de vSphere [Seleccionar todo] 3 Red de vSphere [Seleccionar todo] 4 Almacenamiento de vSphere [Seleccionar todo]

Para que la integración de la ejecución en contexto funcione, es necesario un usuario con privilegio de administrador. Si se habilitan tanto las alertas como la ejecución en contexto, se necesita un usuario con privilegios de administrador.

Acción	Permisos y objetos que seleccionar
Asignar la función de administrador a una cuenta de usuario.	<p>En la pestaña Objetos de la página Asignar grupos y permisos:</p> <ol style="list-style-type: none"> 1 Para Seleccionar función, elija Administrador. 2 Seleccione Asignar esta función al usuario. 3 Seleccione Permitir el acceso a todos los objetos en el sistema.

Configurar vRealize Log Insight para enviar eventos de notificación a vRealize Operations Manager

Puede configurar vRealize Log Insight para que envíe notificaciones de alerta a vRealize Operations Manager.

Es posible integrar vRealize Log Insight con la vApp de vRealize Operations Manager y la versión instalable de vRealize Operations Manager. La integración con la versión instalable requiere cambios adicionales en la configuración de vRealize Operations Manager. Para obtener información sobre la configuración de la versión instalable de vRealize Operations Manager para la integración con vRealize Log Insight, consulte la *Guía de introducción a Log Insight*.

Integrar alertas de vRealize Log Insight con vRealize Operations Manager le permite ver toda la información acerca de su entorno en una única interfaz de usuario.

Puede enviar eventos de notificación desde múltiples instancias de vRealize Log Insight a una única instancia de vRealize Operations Manager. Puede habilitar la ejecución en contexto para una única instancia de vRealize Log Insight por instancia de vRealize Operations Manager.

vRealize Log Insight usa REST API de vRealize Operations Manager para crear recursos y relaciones en vRealize Operations Manager a fin de configurar el adaptador de ejecución en contexto.

Prerequisitos

- Cree una cuenta de usuario de integración en vRealize Operations Manager con los permisos requeridos. Para obtener más información, consulte [Requisitos de la integración con vRealize Operations Manager](#).
- Verifique que conozca la dirección IP o el nombre del host de la instancia de vRealize Operations Manager de destino.
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

NOTA: En un entorno en el que se ejecuta un clúster vRealize Operations Manager con un equilibrador de carga configurado, puede usar la dirección IP del equilibrador de carga si está disponible.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Integration, select **vRealize Operations Manager**.
- 3 Escriba la dirección IP o el nombre de host del nodo principal o del equilibrador de carga, si hay uno configurado. Use una credencial de usuario de vRealize Operations Manager y haga clic en **Probar conexión**. vRealize Log Insight utiliza las credenciales para incorporar los eventos de notificación a vRealize Operations Manager. Asegúrese de que el usuario configurado tenga los permisos mínimos necesarios para que la integración funcione. Consulte [Permisos necesarios mínimos de una cuenta de usuario local o de Active Directory](#).

- 4 En el panel de vRealize Operations Manager, seleccione **Habilitar integración de alertas**.
- 5 Click **Save**.

Qué hacer a continuación

- Consulte las páginas pertinentes en la interfaz de usuario de vRealize Operations Manager para ver los eventos de notificación que vRealize Log Insight envía.

Habilitar ejecución en contexto para vRealize Log Insight en vRealize Operations Manager

Puede configurar vRealize Operations Manager para mostrar elementos de menú relacionados con vRealize Log Insight ejecutar vRealize Log Insight con una consulta específica del objeto.

Es posible integrar vRealize Log Insight con la vApp de vRealize Operations Manager y la versión instalable de vRealize Operations Manager.

La integración con la instalación de vApp y la versión instalable (Windows, Linux) requiere cambios adicionales en la configuración de vRealize Operations Manager. Consulte el tema sobre cómo instalar vRealize Log Insight Management Pack (Adaptador) en vRealize Operations Manager 6.x y en versiones posteriores en el [Centro de información de vRealize Log Insight 4.0](#).

Tenga en cuenta que vRealize vRealize Log Insight Management Pack está preinstalado en vRealize Operations Manager 6.0 y en las versiones posteriores y no es necesario realizar ningún cambio de configuración.

La versión instalable de vRealize Operations Manager (versión de Windows) se dejó de producir a partir de la versión 6.5 de vRealize Operations Manager.

IMPORTANTE: Una instancia de vRealize Operations Manager admite la ejecución en contexto para una sola instancia de vRealize Log Insight. Dado que vRealize Log Insight no comprueba si otras instancias ya están registradas en vRealize Operations Manager, puede anular la configuración de otro usuario.

Prerequisitos

- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verifique que conozca la dirección IP o el nombre del host de la instancia de vRealize Operations Manager de destino.
- Verifique que cuenta con las credenciales de usuario necesarias. Consulte [Permisos necesarios mínimos de una cuenta de usuario local o de Active Directory](#).
- Si utiliza vRealize Operations Manager 6.5 o una versión posterior, use el procedimiento para habilitar la ejecución en contexto en el [Centro de información de vRealize Operations Manager 6.5](#).

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Integration, select **vRealize Operations Manager**.
- 3 Escriba la dirección IP o FQDN del nodo principal o del equilibrador de carga (si hay uno configurado) de vRealize Operations Manager y haga clic en **Probar conexión**.

NOTA: Para la funcionalidad de ejecución en contexto, debe proporcionar un usuario de vRealize Operations Manager con privilegios de administrador.

- 4 Click **Save**.

vRealize Log Insight configura la instancia de vRealize Operations Manager. Esta operación puede demorar unos minutos.

Los elementos relacionados con vRealize Log Insight aparecen en los menús de vRealize Operations Manager.

Qué hacer a continuación

Ejecute una consulta de vRealize Log Insight desde la instancia de vRealize Operations Manager. Consulte [Ejecución en contexto de vRealize Log Insight](#)

Ejecución en contexto de vRealize Log Insight

Cuando la ejecución en contexto se habilita para vRealize Log Insight, se crea un recurso de vRealize Log Insight en vRealize Operations Manager.

El identificador de recursos incluye la dirección IP de la instancia de vRealize Log Insight, y vRealize Operations Manager lo utiliza para abrir vRealize Log Insight.

Ejecución en contexto de vRealize Operations Manager 6.5 y versiones posteriores

Para obtener más información sobre cómo habilitar la ejecución en contexto, consulte el [Centro de información de vRealize Operations Manager](#).

Ejecución en contexto de la interfaz de usuario de vSphere de vRealize Operations Manager 6.4 y versiones anteriores

Las opciones de ejecución en contexto que están relacionadas con vRealize Log Insight aparecen en el menú desplegable **Acciones** de la interfaz de usuario de vSphere. Puede usar estos elementos de menú para abrir vRealize Log Insight, y buscar eventos de registro de un objeto en vRealize Operations Manager.

La acción de ejecución en contexto disponible depende del objeto que seleccione en el inventario de vRealize Operations Manager. El intervalo de tiempo de las consultas se limita a 60 minutos antes de hacer clic en una opción de ejecución en contexto.

Tabla 12-3. Objetos en la UI de vRealize Operations Manager y sus opciones y acciones de ejecución en contexto correspondientes

Objeto seleccionado en vRealize Operations Manager	Opción de ejecución en contexto en el menú desplegable Acciones	Acción en vRealize Operations Manager	Acción en vRealize Log Insight
Mundo	Abrir vRealize Log Insight	Abre vRealize Log Insight.	vRealize Log Insight muestra la pestaña Análisis interactivo .
vCenter Server	Abrir vRealize Log Insight	Abre vRealize Log Insight.	vRealize Log Insight muestra la pestaña Análisis interactivo .
Centro de datos	Buscar registros en vRealize Log Insight	Abre vRealize Log Insight y transmite los nombres de recursos de todos los sistemas del host en el objeto del centro de datos seleccionado.	vRealize Log Insight muestra la pestaña Análisis interactivo y realiza una consulta para buscar eventos de registro que incluyen nombres de hosts dentro del centro de datos.
Clúster	Buscar registros en vRealize Log Insight	Abre vRealize Log Insight y transmite los nombres de recursos de todos los sistemas del host en el objeto Clúster seleccionado.	vRealize Log Insight muestra la pestaña Análisis interactivo y realiza una consulta para buscar eventos de registro que incluyen nombres de hosts dentro del clúster.
Sistema host	Buscar registros en vRealize Log Insight	Abre vRealize Log Insight y transmite el nombre de recursos del objeto Host seleccionado.	vRealize Log Insight muestra la pestaña Análisis interactivo y realiza una consulta para buscar eventos de registro que incluyen el nombre del sistema Host seleccionado.
Virtual Machine (Máquina virtual)	Buscar registros en vRealize Log Insight	Abre vRealize Log Insight y transmite la dirección IP de la máquina virtual seleccionada y el nombre de recurso del sistema del host relacionado.	vRealize Log Insight muestra la pestaña Análisis interactivo y realiza una consulta para buscar eventos de registro que incluyen la dirección IP de la máquina virtual, y el nombre del host en el que reside la máquina virtual.

En la pestaña **Alertas**, si selecciona una alerta y selecciona **Buscar registros en Log Insight** en el menú contextual, el intervalo de tiempo de la consulta se limita a una hora antes de activarse la alerta. Por ejemplo, si una alerta se activa a las 2:00 p.m., la consulta en vRealize Log Insight muestra todos los mensajes de registro que sucedieron entre las 1:00 p.m. y las 2:00 p.m. Esto ayuda a identificar eventos que puedan haber activado la alerta.

Puede abrir vRealize Log Insight desde gráficos métricos en vRealize Operations Manager. El intervalo de tiempo de la consulta que vRealize Log Insight ejecuta coincide con el intervalo de tiempo del gráfico métrico.

NOTA: La hora que ve en los gráficos métricos vRealize Log Insight y vRealize Operations Manager puede ser diferente si la configuración de hora de los dispositivos virtuales es diferente.

Ejecución en contexto en la interfaz de usuario de vRealize Operations Manager 6.4 y versiones anteriores

El icono de ejecución en contexto  aparece en varias páginas de la interfaz de usuario, pero vRealize Log Insight solamente se puede ejecutar desde las páginas que muestran eventos de notificación de vRealize Log Insight:

- La página Descripción general de alertas.
- La página Resumen de alertas de una alerta de notificación de vRealize Log Insight.
- Los widgets Alertas en sus paneles, cuando se selecciona una alerta de notificación de vRealize Log Insight.

Cuando selecciona un evento de notificación de vRealize Log Insight en la interfaz de usuario personalizada, puede elegir entre dos acciones de ejecución en contexto.

Tabla 12-4. Opciones y acciones de ejecución en contexto en la UI de vRealize Operations Manager

Opción de ejecución en contexto en vRealize Operations Manager	Acción en vRealize Operations Manager	Acción en vRealize Log Insight
Abrir vRealize Log Insight	Abre vRealize Log Insight.	vRealize Log Insight muestra la pestaña Paneles y carga el panel Descripción general de vSphere.
Buscar registros en vRealize Log Insight	Abre vRealize Log Insight y transmite el identificador de la consulta que activa el evento de notificación.	vRealize Log Insight muestra la pestaña Análisis interactivo y realiza la consulta que activó el evento de notificación.

Cuando selecciona una alerta que se ha originado a partir de vRealize Log Insight, el menú de ejecución en contexto incluye el elemento de menú **Buscar VM y registros de host en vRealize Log Insight**. Si selecciona este elemento de menú, vRealize Operations Manager abre vRealize Log Insight y transmite los identificadores del objeto que activó la alerta. vRealize Log Insight usa los identificadores de recursos para realizar una búsqueda en los eventos de registro disponibles.

Ejecución en contexto bidireccional

La ejecución en contexto también estará disponible de vRealize Log Insight a vRealize Operations Manager.

Si integra vRealize Log Insight con vRealize Operations Manager, puede realizar una ejecución en contexto desde un evento de vRealize Log Insight; solo hay que seleccionar el icono de engranaje a la izquierda del evento y seleccionar la opción para verlo en vRealize Operations Manager.

Para obtener información sobre la ejecución en contexto de vRealize Operations Manager a vRealize Log Insight, consulte [Ejecución en contexto de vRealize Log Insight](#).

Procedimiento

- 1 En vRealize Log Insight, vaya a la pestaña **Análisis interactivo**.

- 2 Localice un evento que tenga campos de asignación de inventario y mantenga el puntero sobre él.
- 3 Haga clic en el icono de engranaje y seleccione **Abrir análisis** en vRealize Operations Manager desde el menú desplegable.

Se abrirá una nueva pestaña del explorador que le dirigirá a la instancia de vRealize Operations Manager integrada con vRealize Log Insight. Cuando se autentique, se le dirigirá a la sección **Entorno > Análisis** de vRealize Operations Manager con el objeto seleccionado.

NOTA: Si hay varias instancias de vRealize Log Insight conectadas a la misma instancia de vRealize Operations Manager, solamente la última instancia de vRealize Log Insight integrada con vRealize Operations Manager dispone de la característica de ejecución en contexto. Esto también significa que la característica de ejecución en contexto quedará invalidada cada vez que una instancia de vRealize Log Insight se integre con una instancia de vRealize Operations Manager que estuvo integrada anteriormente con otra instancia de vRealize Log Insight.

Deshabilitar inicio en contexto para vRealize Log Insight en vRealize Operations Manager

Puede desinstalar el adaptador de vRealize Log Insight de la instancia de vRealize Operations Manager para eliminar elementos de menú relacionados con vRealize Log Insight desde la interfaz de usuario de vRealize Operations Manager.

Puede usar la UI de administración de vRealize Log Insight para deshabilitar la ejecución en contexto. Si no tiene acceso a vRealize Log Insight, o si la instancia de vRealize Log Insight se elimina antes de deshabilitar la conexión con vRealize Operations Manager, puede eliminar del registro vRealize Log Insight de la UI de administración de vRealize Operations Manager. Consulte la Ayuda en el portal de administración de vRealize Operations Manager.

ADVERTENCIA: Una instancia de vRealize Operations Manager admite la ejecución en contexto para una sola instancia de vRealize Log Insight. Si se ha registrado otra instancia de vRealize Log Insight después de registrar la instancia que desea deshabilitar, la segunda instancia anula la configuración de la primera sin enviarle notificación.

Prerequisitos

- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedimiento

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Integration, select **vRealize Operations Manager**.
- 3 Anule la selección de la casilla de verificación **Habilitar ejecución en contexto**.
- 4 Click **Save**.

vRealize Log Insight configura la instancia de vRealize Operations Manager para eliminar el adaptador de vRealize Log Insight. Esta operación puede demorar unos minutos.

Agregar un dominio y una ruta de búsqueda de DNS

Puede agregar un dominio y una ruta de búsqueda de DNS para mejorar las coincidencias de inventario de vRealize Operations Manager.

Agregar un dominio y una ruta de búsqueda de DNS permite mejorar las coincidencias cuando una etiqueta de máquina virtual y un dominio de búsqueda resuelven la dirección IP del host que envía mensajes de registro a vRealize Log Insight. Por ejemplo, si tiene una máquina virtual denominada linux_01 en vRealize Operations Manager y el nombre del host linux_01.company.com resuelve en 192.168.10.10, entonces añadir un dominio de búsqueda permite que vRealize Log Insight reconozca y empareje ese recurso.

Procedimiento

- 1 Lleve a cabo un apagado de invitado del dispositivo virtual vRealize Log Insight.
- 2 Con la máquina virtual apagada, seleccione **Editar ajustes**.
- 3 Seleccione la pestaña **Opciones**.
- 4 En **Opciones de vApp > Opciones avanzadas**, haga clic en **Propiedades**.
- 5 Busque las claves `vami.searchpath.VMware_vCenter_Log_Insight` y `vami.domain.VMware_vCenter_Log_Insight`.
Si no existen, créelas.
- 6 Defina el dominio y la ruta de búsqueda de DNS.
- 7 Encienda el dispositivo virtual.

Qué hacer a continuación

Después de que vRealize Log Insight se inicie, inicie sesión y vea el contenido del archivo `/etc/resolv.conf` para validar la configuración de DNS. Prácticamente al final de este archivo es donde deben figurar las opciones de búsqueda y dominio.

Eliminar el adaptador de vRealize Log Insight

Cuando habilita la ejecución en contexto en una instancia de vRealize Operations Manager 6.2 y posterior, vRealize Log Insight crea una instancia del adaptador de vRealize Log Insight en la instancia de vRealize Operations Manager.

La instancia del adaptador permanece en la instancia de vRealize Operations Manager hasta que desinstala vRealize Log Insight. Como consecuencia, los elementos del menú de ejecución en contexto continúan mostrándose en los menús de acción y apuntan a una instancia de vRealize Log Insight que ya no existe.

Para deshabilitar la funcionalidad de ejecución en contexto en vRealize Operations Manager, debe quitar el adaptador de vRealize Log Insight de la instancia de vRealize Operations Manager.

El usuario puede usar la utilidad de la línea de comando cURL para enviar llamadas REST a vRealize Operations Manager.

NOTA: Estos pasos solo son necesarios si la ejecución en contexto está habilitada.

Prerequisitos

- Verifique que cURL esté instalado en su sistema. Tenga en cuenta que esta herramienta está preinstalada en el dispositivo virtual devRealize Operations Manager y los pasos se pueden realizar desde el dispositivo con una dirección IP 127.0.0.1.
- Verifique que conozca la dirección IP o el nombre del host de la instancia de vRealize Operations Manager de destino.
- Según la licencia de vRealize Operations Manager que posea, compruebe que dispone de las credenciales de usuario mínimas necesarias para desinstalar el paquete de administración. Consulte [Permisos necesarios mínimos de una cuenta de usuario local o de Active Directory](#).

Procedimiento

- 1 En cURL, ejecute la siguiente consulta en el dispositivo virtual de vRealize Operations Manager para buscar el adaptador de vRealize Log Insight.

```
curl -k -u "admin" https://ipaddress/suite-api/api/adapterkinds/LogInsight/resourcekinds/LogInsightLogServer/resources
```

Donde *admin* es el nombre de inicio de sesión del administrador y *ipaddress* es la dirección IP (o nombre de host) de la instancia de vRealize Operations Manager. Se le pedirá que introduzca la contraseña para el usuario: *admin*.

En la salida de cURL, busque el valor de GUID asignado al identificador: `<ops:resource creationTime="{TIMESTAMP}" identifier="{GUID}">`. Es posible usar este valor de GUID en el comando a continuación que elimina la instancia del adaptador.

- 2 Ejecute el siguiente comando para quitar el adaptador de vRealize Log Insight.

```
curl -k -u "admin" -X DELETE https://ipaddress/suite-api/api/adapters/{GUID}
```

Donde *admin* es el nombre de inicio de sesión del administrador y *ipaddress* es la dirección IP (o nombre de host) de la instancia de vRealize Operations Manager. Se le pedirá que introduzca la contraseña para el usuario: *admin*.

Los elementos de ejecución en contexto de vRealize Log Insight se eliminan de los menús en vRealize Operations Manager. Para obtener más información acerca de ejecución en contexto, vea el tema *Ejecución en contexto de vRealize Log Insight* en la ayuda del producto de vRealize Log Insight.

Paquete de contenido de vRealize Operations Manager para vRealize Log Insight

El paquete de contenido de vRealize Operations Manager para vRealize Log Insight incluye paneles, campos extraídos, consultas almacenadas y alertas que se utilizan para analizar todos los registros redireccionados desde una instancia de vRealize Operations Manager.

El paquete de contenido de vRealize Operations Manager proporciona una manera de analizar todos los registros redireccionados desde una instancia de vRealize Operations Manager. El paquete de contenido incluye paneles, consultas y alertas para proporcionar capacidades de diagnóstico y solución de problemas al administrador de vRealize Operations Manager. Los paneles se agrupan conforme a los principales componentes de vRealize Operations Manager, como Análisis, UI y Adaptadores, para brindar una mejor capacidad de administración. Puede habilitar distintas alertas para enviar eventos de notificación en vRealize Operations Manager y correos electrónicos a los administradores.

Puede descargar el paquete de contenido de vRealize Operations Manager desde https://solutionexchange.vmware.com/store/loginsight?src=Product_Product_LogInsight_YES_US.

Vea [Trabajar con paquetes de contenido](#).

Consideraciones de seguridad para vRealize Log Insight

13

Use las funciones de vRealize Log Insight para proteger su entorno ante ataques.

Este capítulo cubre los siguientes temas:

- [Puertos e interfaces externas](#)
- [Archivos de configuración de vRealize Log Insight](#)
- [Clave pública, certificado y almacén de claves de vRealize Log Insight](#)
- [Archivo de licencia y CLUF de vRealize Log Insight](#)
- [Archivos de registro de vRealize Log Insight](#)
- [Cuentas de usuario de vRealize Log Insight](#)
- [Recomendaciones de firewall de vRealize Log Insight](#)
- [Actualizaciones y revisiones de seguridad](#)

Puertos e interfaces externas

vRealize Log Insight usa servicios, puertos e interfaces externas específicos que son necesarios.

Puertos de comunicación

vRealize Log Insight usa los protocolos y puertos de comunicación enumerados en este tema. Los puertos necesarios se organizan en función de si se necesitan para los orígenes, para la interfaz de usuario, entre clústeres o para servicios externos, o bien si se pueden bloquear con un firewall. Algunos puertos se usan solamente si se habilita la integración correspondiente.

NOTA: vRealize Log Insight no admite clústeres WAN (también denominados geoclústeres, clústeres de alta disponibilidad o clústeres remotos). Todos los nodos de un clúster deben implementarse en la misma LAN de capa 2. Además, los puertos descritos en esta sección deben estar abiertos entre nodos para una correcta comunicación.

El tráfico de red de vRealize Log Insight tiene distintos orígenes.

Estación de trabajo administrativa	La máquina que usa un administrador de sistema para administrar el dispositivo virtual de vRealize Log Insight de manera remota.
Estación de trabajo del usuario	La máquina en la que un usuario de vRealize Log Insight usa un explorador para acceder a la interfaz web de vRealize Log Insight.
Sistema que envía registros	El endpoint que envía registros a vRealize Log Insight para análisis y búsqueda. Por ejemplo, los endpoints incluyen hosts ESXi, máquinas virtuales o cualquier sistema con una dirección IP.
Log Insight Agents	El agente que reside en una máquina Windows o Linux, y envía eventos del sistema operativo e inicia sesión en vRealize Log Insight a través de API.
Dispositivo vRealize Log Insight	Cualquier dispositivo virtual de vRealize Log Insight, principal o de trabajador, donde residen los servicios de vRealize Log Insight. El sistema operativo base del dispositivo es SUSE 11 SP3.

Puertos necesarios para orígenes que envían datos

Los siguientes puertos deben estar abiertos al tráfico de red desde orígenes que envían datos a vRealize Log Insight, tanto para conexiones desde fuera del clúster como para conexiones de carga equilibrada entre nodos del clúster.

Origen	Destino	Puerto	Protocolo	Descripción del servicio
Sistema que envía registros	Dispositivo vRealize Log Insight	514	TCP, UDP	Tráfico de syslog saliente configurado como un destino de reenvío
Sistema que envía registros	Dispositivo vRealize Log Insight	1514, 6514	TCP	Datos de syslog a través de SSL
Agentes de vRealize Log Insight	Dispositivo vRealize Log Insight	9000	TCP	API de consumo de Log Insight
Agentes de vRealize Log Insight	Dispositivo vRealize Log Insight	9543	TCP	API de consumo de Log Insight a través de SSL

Puertos necesarios para la interfaz de usuario

Los siguientes puertos deben estar abiertos al tráfico de red que necesite utilizar la interfaz de usuario de vRealize Log Insight, tanto para conexiones fuera del clúster como para conexiones de carga equilibrada entre nodos del clúster.

Origen	Destino	Puerto	Protocolo	Descripción del servicio
Estación de trabajo administrativa	Dispositivo vRealize Log Insight	22	TCP	SSH: conectividad shell segura
Estación de trabajo del usuario	Dispositivo vRealize Log Insight	80	TCP	HTTP: interfaz web
Estación de trabajo del usuario	Dispositivo vRealize Log Insight	443	TCP	HTTPS: interfaz web

Puertos necesarios entre nodos de clúster

Los siguientes puertos solo deben estar abiertos en un nodo principal de vRealize Log Insight para el acceso de red desde los nodos de trabajador para máxima seguridad. Además, se deben tener en cuenta los puertos usados para los orígenes y el tráfico de la interfaz de usuario que tienen carga equilibrada entre los nodos del clúster.

Origen	Destino	Puerto	Protocolo	Descripción del servicio
Dispositivo vRealize Log Insight	Dispositivo vRealize Log Insight	7000	TCP	Replicación y consulta de Cassandra
Dispositivo vRealize Log Insight	Dispositivo vRealize Log Insight	9042	TCP	Servicio de Cassandra para clientes de protocolos nativos
Dispositivo vRealize Log Insight	Dispositivo vRealize Log Insight	9160	TCP	Servicio de Cassandra para clientes Thrift
Dispositivo vRealize Log Insight	Dispositivo vRealize Log Insight	59778, 16520-16580	TCP	Servicio Thrift de vRealize Log Insight

Puertos necesarios para servicios externos

Los siguientes puertos deben estar abiertos para permitir el tráfico de red saliente desde los nodos del clúster de vRealize Log Insight hasta servicios remotos.

Origen	Destino	Puerto	Protocolo	Descripción del servicio
Dispositivo vRealize Log Insight	Servidor NTP	123	UDP	NTPD: proporciona sincronización de hora NTP NOTA: El puerto está abierto solo si elige usar la sincronización de hora NTP
Dispositivo vRealize Log Insight	Servidor de correo	25	TCP	SMTP: servicio de correo para alertas salientes

Origen	Destino	Puerto	Protocolo	Descripción del servicio
Dispositivo vRealize Log Insight	Servidor de correo	465	TCP	SMTPTS: servicio de correo a través de SSL para alertas salientes
Dispositivo vRealize Log Insight	Servidor DNS	53	TCP, UDP	DNS: servicio de resolución de nombres
Dispositivo vRealize Log Insight	Servidor AD	389	TCP, UDP	Active Directory
Dispositivo vRealize Log Insight	Servidor AD	636	TCP	Active Directory a través de SSL
Dispositivo vRealize Log Insight	Servidor AD	3268	TCP	Catálogo global de Active Directory
Dispositivo vRealize Log Insight	Servidor AD	3269	TCP	SSL de Catálogo global de Active Directory
Dispositivo vRealize Log Insight	Servidor AD	88	TCP, UDP	Kerberos
Dispositivo vRealize Log Insight	vCenter Server	443	TCP	Servicio web de vCenter Server
Dispositivo vRealize Log Insight	Dispositivo vRealize Operations Manager	443	TCP	Servicio web de vRealize Operations
Dispositivo vRealize Log Insight	Administrador del registro de terceros	514	TCP, UDP	Datos de syslog
Dispositivo vRealize Log Insight	Administrador del registro de terceros	9000	CFAPI	Tráfico de la API de consumo de Log Insight saliente (CFAPI) configurado como un destino de reenvío
Dispositivo vRealize Log Insight	Administrador del registro de terceros	9543	CFAPI	Tráfico de la API de consumo de Log Insight saliente (CFAPI) configurado como un destino de reenvío cifrado (SSL/TLS)

Puertos que se pueden bloquear

Los siguientes puertos están abiertos, pero vRealize Log Insight no lo utiliza. Estos puertos se pueden bloquear con un firewall sin problemas.

Destino	Puerto	Protocolo	Descripción del servicio
Dispositivo vRealize Log Insight	111	TCP, UDP	Servicio RPCbind que convierte números de programa RPC en direcciones universales
Servicio Tomcat del dispositivo de vRealize Log Insight	9007	TCP	Servicios Tomcat

Archivos de configuración de vRealize Log Insight

Algunos archivos de configuración contienen ajustes que afectan la seguridad de vRealize Log Insight.

NOTA: La cuenta raíz tiene acceso a todos los recursos relacionados con la seguridad. La protección de esta cuenta es fundamental para la seguridad de vRealize Log Insight.

Tabla 13-1. Archivos de configuración de Log Insight

File (Archivo)	Descripción
/usr/lib/loginsight/application/etc/loginsight-config-base.xml	La configuración del sistema predeterminada para vRealize Log Insight.
/storage/core/loginsight/config/loginsight-config.xml#number	La configuración del sistema modificada (a partir de la predeterminada) para vRealize Log Insight.
/usr/lib/loginsight/application/etc/jaas.conf	La configuración para la integración de Active Directory.
/usr/lib/loginsight/application/etc/3rd_config/server.xml	La configuración del sistema para el servidor Apache Tomcat.
/storage/var/loginsight/apache-tomcat/conf/tomcat-users.xml	La configuración del sistema para el servidor Apache Tomcat.
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/server.xml	La configuración del sistema para el servidor Apache Tomcat.
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/tomcat-users.xml	Información de usuario para el servidor Apache Tomcat.

Clave pública, certificado y almacén de claves de vRealize Log Insight

La clave pública, el certificado y el almacén de claves de vRealize Log Insight se encuentran en el dispositivo virtual de vRealize Log Insight.

NOTA: La cuenta raíz tiene acceso a todos los recursos relacionados con la seguridad. La protección de esta cuenta es fundamental para la seguridad de vRealize Log Insight.

- /usr/lib/loginsight/application/etc/public.cert
- /usr/lib/loginsight/application/etc/loginsight.pub
- /usr/lib/loginsight/application/etc/3rd_config/keystore

- /usr/lib/loginsight/application/etc/truststore
- /usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/keystore

Archivo de licencia y CLUF de vRealize Log Insight

El archivo de contrato de licencia de usuario final (CLUF) y licencia se encuentran en el dispositivo virtual de vRealize Log Insight.

NOTA: La cuenta raíz tiene acceso a todos los recursos relacionados con la seguridad. La protección de esta cuenta es fundamental para la seguridad de vRealize Log Insight.

File (Archivo)	Ubicación
Licencia	/usr/lib/loginsight/application/etc/license/loginsight_dev.dlf
Licencia	/usr/lib/loginsight/application/etc/license/loginsight_cpu.dlf
Licencia	/usr/lib/loginsight/application/etc/license/loginsight_osi.dlf
Archivo de clave de licencia	/usr/lib/loginsight/application/etc/license/loginsight_license.bak
Contrato de licencia de usuario final	/usr/lib/loginsight/application/etc/license/release/eula.txt

Archivos de registro de vRealize Log Insight

Los archivos que incluyen mensajes del sistema se encuentran en el dispositivo virtual de vRealize Log Insight.

File (Archivo)	Descripción
/storage/var/loginsight/alert.log	Se usa para rastrear información sobre las alertas definidas por el usuario que se activaron.
/storage/var/loginsight/apache-tomcat/logs/*.log	Se usa para rastrear eventos del servidor Apache Tomcat.
/storage/var/loginsight/cassandra.log	Se usa para rastrear almacenamiento de configuración y replicación del clúster en Apache Cassandra.
/storage/var/loginsight/plugins/vsphere/li-vsphere.log	Se usa para rastrear eventos en relación con la integración con vSphere Web Client.
/storage/var/loginsight/loginsight_daemon_stdout.log	Se usa para la salida estándar del daemon de vRealize Log Insight.
/storage/var/loginsight/phonehome.log	Se usa para rastrear información sobre la recopilación de datos de traza enviados a VMware (si se habilita).
/storage/var/loginsight/pi.log	Se usa para rastrear eventos de inicio o detención de la base de datos.
/storage/var/loginsight/runtime.log	Se usa para rastrear toda la información de tiempo de ejecución relacionada con vRealize Log Insight.
/var/log/firstboot/stratavm.log	Se usa para rastrear los eventos que suceden en el primer arranque y configuración del dispositivo virtual de vRealize Log Insight.

File (Archivo)	Descripción
/storage/var/loginsight/systemalert.log	Se usa para rastrear información sobre las notificaciones del sistema que envía vRealize Log Insight. Cada alerta se enumera como una entrada JSON.
/storage/var/loginsight/systemalert_worker.log	Se usa para rastrear información sobre las notificaciones del sistema que envía un nodo de trabajo de vRealize Log Insight. Cada alerta se enumera como una entrada JSON.
/storage/var/loginsight/ui.log	Se usa para rastrear eventos relacionados con la interfaz de usuario de vRealize Log Insight.
/storage/var/loginsight/ui_runtime.log	Se usa para rastrear eventos de tiempo de ejecución relacionados con la interfaz de usuario de vRealize Log Insight.
/storage/var/loginsight/upgrade.log	Se usa para rastrear eventos que suceden durante la actualización de vRealize Log Insight.
/storage/var/loginsight/usage.log	Se usa para rastrear todas las consultas.
/storage/var/loginsight/vcenter_operations.log	Se usa para rastrear eventos relacionados con la integración de vRealize Operations Manager.
/storage/var/loginsight/watchdog_log*	Se usa para rastrear los eventos de tiempo de ejecución del proceso de vigilancia, que es responsable de reiniciar vRealize Log Insight si se apaga por algún motivo.

Mensajes de registro relacionados con la seguridad

El archivo `ui_runtime.log` incluye mensajes de registro de auditorías del usuario en el siguiente formato.

- [2013-05-17 20:40:18.716+0000] [http-443-5 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Name: admin | Role: admin]
- [2013-05-17 20:39:51.395+0000] [http-443-5 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged out: Name: admin | Role: admin]
- [2013-09-18 12:39:34.823-0700] [http-9443-3 WARN /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean][Bad username/password attempt (username: myusername)]
- [2013-09-18 12:40:08.761-0700] [http-9443-3 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Active Directory User: SAM=myusername, Domain=vmware.com,UPN=myusername@vmware.com]
- [2013-09-18 12:40:20.232-0700] [http-9443-3 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged out: Active Directory User: SAM=myusername, Domain=vmware.com,UPN=myusername@vmware.com]

- [2013-09-18 12:40:36.933-0700] [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Local User: Name=myusername, Role=user]
- [2013-09-18 12:40:40.429-0700] [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged out: Local User: Name=myusername, Role=user]
- [2013-11-13 23:26:21.569+0000] [http-443-4 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: Active Directory User: SAM=username, Domain=vmware.com, UPN=username@vmware.com]
- [2013-11-14 22:44:11.017+0000] [http-443-6 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: Local User: Name=username, Role=admin]
- [2013-12-05 21:03:36.751+0000] [http-443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed users: [Active Directory User: SAM=username, Domain=vmware.com, UPN=username@vmware.com]]
- [2013-12-05 21:04:16.707+0000] [http-443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed users: [Local User: Name=username, Role=admin]]
- [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new group: (domain=vmware.com, group=VMware Employees, role=user)]
- [2013-12-05 13:07:04.108-0800] [http-9443-2 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed groups: [(domain=vmware.com, group=VMware Employees, role=user)]]

Cuentas de usuario de vRealize Log Insight

Debe configurar un sistema y una cuenta raíz para administrar vRealize Log Insight.

Usuario raíz de vRealize Log Insight

vRealize Log Insight usa actualmente la cuenta de usuario raíz como el usuario de servicio. No se crean otros usuarios.

A menos que configure la propiedad de contraseña raíz durante la implementación, la contraseña raíz predeterminada está en blanco. Debe cambiar la contraseña raíz cuando inicia sesión en la consola de vRealize Log Insight por primera vez.

SSH está deshabilitado hasta que se configura la contraseña raíz predeterminada.

La contraseña raíz debe cumplir los siguientes requisitos.

- Debe tener al menos 8 caracteres

- Debe incluir al menos una letra mayúscula, una letra minúscula, un dígito y un carácter especial
- No debe repetir el mismo carácter cuatro veces

Usuario administrador de vRealize Log Insight

Cuando inicia el dispositivo virtual de vRealize Log Insight por primera vez, vRealize Log Insight crea la cuenta del usuario administrador para su interfaz de usuario web.

La contraseña predeterminada para administración está en blanco. Debe cambiar la contraseña administrativa en la interfaz de usuario web durante la configuración inicial de vRealize Log Insight.

Soporte de Active Directory

vRealize Log Insight admite la integración con Active Directory. Cuando se configura, vRealize Log Insight puede autenticar o autorizar a un usuario en Active Directory.

Consulte [Habilitar la autenticación de usuarios a través de Active Directory](#).

Privilegios asignados a usuarios predeterminados

El usuario del servicio vRealize Log Insight tiene privilegios raíz.

El usuario administrador de la interfaz de usuario web tiene los privilegios de administrador solo para la interfaz de usuario web de vRealize Log Insight.

Recomendaciones de firewall de vRealize Log Insight

Para proteger información sensible recopilada por vRealize Log Insight, coloque el servidor o servidores en un segmento de red de administración protegido por un firewall del resto de su red interna.

Puertos requeridos

Es necesario que los siguientes puertos estén abiertos al tráfico de red de orígenes que envían datos a vRealize Log Insight.

Puerto	Protocolo
514/UDP, 514/TCP	Syslog
1514/TCP, 6514/TCP	Syslog-TLS (SSL)
9000/TCP	API de consumo de vRealize Log Insight
9543/TCP	API de consumo de vRealize Log Insight: TLS (SSL)

Es necesario que los siguientes puertos estén abiertos al tráfico de red que debe usar la UI de vRealize Log Insight.

Puerto	Protocolo
80/TCP	HTTP
443/TCP	HTTPS

El siguiente conjunto de puertos solo debe estar abierto en un nodo principal de vRealize Log Insight para el acceso de red desde los nodos de trabajador para máxima seguridad.

Puerto	Protocolo
16520:16580/TCP	Thrift RPC
59778/TCP	log4j server
12543/TCP	database server

Actualizaciones y revisiones de seguridad

El dispositivo virtual de vRealize Log Insight utiliza SUSE Linux Enterprise Server 11 (x86_64), versión 11, nivel de revisión 3, como sistema operativo invitado.

VMware lanzará revisiones para abordar los problemas de seguridad.

Antes de aplicar una actualización o revisión al sistema operativo invitado, considere las dependencias. Consulte [Capítulo 6 Puertos e interfaces externas](#).

Copia de seguridad, restauración y recuperación de desastres

14

Para proteger contra el costoso tiempo de inactividad del centro de datos, lleve a cabo las siguientes prácticas recomendadas para realizar copias de seguridad, restauración y recuperación de desastres de vRealize Log Insight.

Este capítulo cubre los siguientes temas:

- [Información general sobre copias de seguridad, restauración y recuperación de desastres](#)
- [Utilizar direcciones IP estáticas y FQDN](#)
- [Planificación y preparación](#)
- [Copia de seguridad de nodos y clústeres](#)
- [Agentes de Linux o Windows de copia de seguridad](#)
- [Restaurar nodos y clúster](#)
- [Cambiar configuraciones tras la restauración](#)
- [Verificar restauraciones](#)
- [Recuperación de desastres](#)

Información general sobre copias de seguridad, restauración y recuperación de desastres

VMware entrega una cartera integral y completa de soluciones de continuidad operativa y recuperación en caso de desastres (Business Continuity and Disaster Recovery, BCDR) que proporcionan alta disponibilidad, protección de datos y recuperación de desastres.

Use la información sobre copias de seguridad, restauración y recuperación de desastres que aparece en este documento para los componentes de vRealize Log Insight, incluidos el nodo principal, el nodo de trabajo y el reenviador.

- Para obtener más información sobre los miembros de los clústeres de trabajo y principal, los datos de registro y la personalización, consulte [Copia de seguridad de nodos y clústeres](#).
- Para obtener más información sobre la configuración local del agente de Linux o Windows, consulte [Agentes de Linux o Windows de copia de seguridad](#).

La información que contiene este documento no se aplica a las siguientes herramientas y productos. Debe consultar varios recursos para obtener información acerca de dichas herramientas y productos.

- Herramientas de terceros que se utilizan específicamente para copias de seguridad, restauración y recuperación de desastres. Para obtener más información, consulte la documentación del proveedor.
- vSphere Data Protection, Site Recovery Manager y Symantec NetBackup. Para obtener información adicional sobre las soluciones BCDR de VMware, consulte <http://www.vmware.com/business-continuity/business-continuity> y la documentación de [VMware vCloud Suite](#).
- Herramientas de copia de seguridad, restauración y recuperación de desastres para productos que se integran con vRealize Log Insight.
 - vRealize Operations Manager
 - Servidor vSphere Web Client
 - Hosts ESXi

Utilizar direcciones IP estáticas y FQDN

Puede utilizar direcciones IP estáticas y FQDN para evitar riesgos durante las operaciones de copia de seguridad, restauración y recuperación ante desastres.

Direcciones IP estáticas para los nodos del clúster de vRealize Log Insight y el equilibrador de carga

Cuando utiliza las direcciones IP estáticas para todos los nodos de un clúster de vRealize Log Insight, elimina la necesidad de actualizar las direcciones IP de los nodos del clúster cuando se modifican las direcciones IP.

vRealize Log Insight incluye todas las direcciones IP de los nodos en cada archivo de configuración de los nodos de clúster, tal como se describe en el [artículo 2123058 de la base de conocimientos](#).

Todos los productos que se integran con vRealize Log Insight (ESXi, vSphere, vRealize Operations) utilizan el nombre de dominio completo (FQDN) o la dirección IP del nodo principal del clúster como destino de syslog. Esos productos pueden usar el FQDN o la dirección IP del equilibrador de carga, si está configurado, como el objetivo de syslog. Las direcciones IP estáticas reducen el riesgo de actualizar constantemente la dirección IP objetivo de syslog en varias ubicaciones.

Proporcione direcciones IP estáticas y direcciones IP virtuales opcionales para el equilibrador de carga. Al configurar un equilibrador de carga integrado, proporcione el FQDN opcional para la dirección IP virtual. El FQDN se utiliza cuando la dirección IP no está disponible por algún motivo.

FQDN para el nodo de trabajador y los nodos de clúster de vRealize Log Insight

Cuando utiliza un FQDN para todos los nodos en el clúster de vRealize Log Insight, puede ahorrar tiempo en los cambios de configuración posteriores a la restauración y de la recuperación siempre que se pueda resolver el mismo FQDN en el sitio de la recuperación.

Para el nodo principal (equilibrador de carga cuando se utilice), se requiere un FQDN de resolución completa. De lo contrario, los hosts ESXi no envían los mensajes de syslog a vRealize Log Insight ni a ningún destino remoto.

Para las notificaciones del sistema, vRealize Log Insight utiliza nombres de host FQDN, si están disponibles, en lugar de direcciones IP.

Se puede asumir, en forma razonable, que solo las direcciones IP subyacentes se modifican después de las operaciones posteriores a la copia de seguridad y restauración o de recuperación de desastre. El uso de FQDN elimina la necesidad de modificar la dirección de destino de syslog (FQDN del nodo principal o FQDN del equilibrador de carga interno) en todos los dispositivos externos que envían registros al clúster de vRealize Log Insight.

Verifique que las solicitudes de unión de un nodo de trabajador de vRealize Log Insight utilicen el FQDN del nodo principal de vRealize Log Insight.

El valor del host del nodo principal que aparece en el archivo de configuración de cada uno de los nodos se basa en el valor utilizado por el primer nodo de trabajador que envía una solicitud de unión. El uso del FQDN del nodo principal para la solicitud de unión evita realizar cambios manuales en el valor del host del nodo principal después de la recuperación ante desastres. De lo contrario, los nodos de trabajador no pueden volver a unirse al nodo principal hasta que se actualice el nombre del host del nodo principal en los archivos de configuración de todos los nodos del clúster restablecido.

Planificación y preparación

Antes de implementar un procedimiento de copia de seguridad, de restauración o de recuperación de desastres, revise la información de planificación y preparación que contiene este tema.

Las siguientes recomendaciones deben incluirse en un plan de copia de seguridad, restauración y recuperación ante desastres.

Operaciones de copia de seguridad de prueba

Realice una prueba de funcionamiento de las operaciones de copia de seguridad, restauración y recuperación ante desastres en un entorno de prueba o simulación antes de realizar estas operaciones en un entorno de producción real.

Realice una copia de seguridad completa de todo el clúster de vRealize Log Insight. No confíe en los procedimientos automáticos para realizar las copias de seguridad de los diferentes archivos y configuraciones.

Verificar las revisiones

Verifique que se implementen las revisiones y que se corrijan los errores y advertencias antes de efectuar las operaciones de copia de seguridad, restauración y recuperación ante desastres. Las herramientas para copia de seguridad, restauración y recuperación ante desastres generalmente proporcionan validaciones visuales y pasos para garantizar que se creen correctamente las configuraciones para copia de seguridad, restauración y recuperación ante desastres.

Programar copias de seguridad

Según la configuración del clúster, la primera operación de copia de seguridad suele ser una copia de seguridad completa. Reserve una buena cantidad de tiempo para completar la primera copia de seguridad. Las copias de seguridad sucesivas, que pueden ser incrementales o completas, terminan en forma relativamente más rápida si se comparan con la operación de la primera copia de seguridad.

Herramientas y documentación adicionales

Verifique que esté siguiendo la documentación para asignar recursos para las herramientas de copia de seguridad, restauración y recuperación ante desastres de vRealize Log Insight.

Verifique que esté siguiendo las prácticas recomendadas específicas de las herramientas y las recomendaciones para las herramientas de copia de seguridad, restauración y recuperación ante desastres de terceros.

En el caso de máquinas virtuales implementadas mediante productos VMware, utilice herramientas adicionales que puedan proporcionar configuraciones y características especiales para admitir la copia de seguridad, la restauración y la recuperación ante desastres.

Reenviadores y clústeres

En el caso de los reenviadores, aplique los pasos de copia de seguridad, restauración y recuperación ante desastres para el clúster principal de vRealize Log Insight. Consulte [Restaurar nodos y clúster](#).

En función de los requisitos del cliente, puede tener uno o varios reenviadores de vRealize Log Insight. Además, los reenviadores pueden instalarse como nodo independiente o como clúster. A efectos de las operaciones de copia de seguridad, restauración y recuperación ante desastres, los reenviadores de vRealize Log Insight son idénticos a los nodos del clúster primario de vRealize Log Insight y se manejan de igual manera.

Copia de seguridad de nodos y clústeres

Es una práctica recomendada configurar una replicación o copias de seguridad programadas para los nodos y clústeres de vRealize Log Insight.

vRealize Log Insight no admite las instantáneas inactivas. Si intenta crear una snapshot inactiva, se crea la snapshot pero no se aplica la condición de inactividad. Para obtener más información, consulte el artículo de la base de conocimientos de VMware que aborda el problema que se produce cuando [los dispositivos virtuales Log Insight no responden durante las snapshot inactivas](#).

Prerequisitos

- Compruebe que no haya problemas de configuración en los sitios de origen y destino antes de llevar a cabo las operaciones de copia de seguridad o replicación.
- Compruebe que la asignación de recursos en el clúster no esté al máximo de su capacidad.

En configuraciones con cargas razonables de consumo y consulta, el consumo e intercambio de memoria puede alcanzar casi el 100% de la capacidad durante las operaciones de copia de seguridad y de replicación. Debido a que la memoria está casi al límite de su capacidad en un entorno activo, parte del pico de uso de la memoria se debe al uso del clúster de vRealize Log Insight. Además, las operaciones programadas de copia de seguridad y de replicación pueden influir considerablemente en el pico de uso de memoria.

En algunos casos, los nodos de trabajador se desconectan momentáneamente durante 1 a 3 minutos antes de reunirse con los nodos principales, posiblemente debido al consumo intensivo de memoria.

- Reduzca la regulación de la memoria en los nodos de vRealize Log Insight llevando a cabo una de las siguientes acciones:
 - Asigne memoria adicional a las configuraciones recomendadas de vRealize Log Insight.
 - Programe las copias de seguridad recurrentes durante las horas valle.

Procedimiento

- 1 Habilite la copia de seguridad o la replicación regulares de los reenviadores de vRealize Log Insight utilizando los mismos procedimientos que usa para el servidor de vRealize Log Insight.
- 2 Compruebe que la frecuencia de las copias de seguridad y los tipos de copias de seguridad estén correctamente seleccionados en función de los recursos disponibles y los requisitos específicos del cliente.
- 3 Si los recursos no constituyen un problema y si cuentan con el soporte de la herramienta, habilite las copias de seguridad simultáneas de los nodos de clúster para acelerar el proceso de copia de seguridad.
- 4 Lleve a cabo una copia de todos los nodos al mismo tiempo.

Qué hacer a continuación

Supervisión: mientras la copia de seguridad está en progreso, revise los problemas de entorno o de rendimiento en la configuración de vRealize Log Insight. La mayoría de las herramientas de copia de seguridad, restauración y recuperación de desastres ofrecen funciones de supervisión.

Durante el proceso de copia de seguridad, revise todos los registros relevantes en el sistema de producción porque es posible que la interfaz de usuario no muestre todos los problemas.

Agentes de Linux o Windows de copia de seguridad

Para realizar una copia de seguridad de los agentes, realice una copia de seguridad de la información y la configuración en el lado del servidor. No se requiere una copia de seguridad por separado del nodo agente.

Los agentes se suelen instalar en sistemas Linux o Windows que también se usan para otras aplicaciones o servicios, y que se pueden incluir en procesos de copias de seguridad. Para el proceso de recuperación, basta con una copia de seguridad a nivel de bloque o de archivo del equipo que incluya la instalación completa del agente y su configuración. Los agentes admiten la configuración local y la configuración proporcionada por el servidor.

Si el agente está configurado completamente desde el servidor vRealize Log Insight, sin ningún cambio local en el archivo de configuración `liagent.ini`, no es necesario que cree una copia de seguridad de la instalación del agente. En su lugar, realice una instalación nueva del agente y lleve a cabo un proceso de recuperación de la copia de seguridad del servidor.

Si el agente tiene una configuración local personalizada, realice una copia de seguridad del archivo `liagent.ini` y restáurelo junto con una nueva instalación del agente. Si utiliza los nodos agente para más que para instalar el software agente, y si esos nodos necesitan una copia de seguridad completa, siga el mismo procedimiento de copia de seguridad que para cualquier otra máquina virtual.

Si la configuración del agente se lleva a cabo en el lado del cliente (en los agentes) y si los nodos agente se utilizan únicamente para instalar el software del agente de vRealize Log Insight, realizar una copia de seguridad del archivo de configuración del agente es suficiente.

Prerequisitos

Compruebe que la configuración del agente se encuentra en el lado del servidor de vRealize Log Insight.

Procedimiento

- 1 Realice una copia de seguridad del archivo `liagent.ini`.
- 2 Reemplace el archivo en el agente recuperado o en la máquina Linux o Windows con el archivo de copia de seguridad.

Restaurar nodos y clúster

Los nodos deben restablecerse en un orden específico y algunas situaciones de restauración pueden requerir cambios de configuración manual.

Según la herramienta utilizada para la restauración, puede restablecer las máquinas virtuales con el mismo host, con un host diferente en el mismo centro de datos o con un host diferente en un centro de datos remoto de destino. Consulte [Cambiar configuraciones tras la restauración](#)

Prerequisitos

- Verifique que los nodos restaurados estén en estado desconectado.

- Verifique que las instancias de clúster estén apagadas antes de restablecer el clúster en un sitio nuevo.
- Verifique que no se produzca comportamiento de procesador dividido cuando se utilicen las mismas direcciones IP y FQDN en el sitio de recuperación.
- Verifique que ninguno esté utilizando, accidentalmente, un clúster que funciona parcialmente en el sitio primario.

Procedimiento

- 1 Restablezca el nodo principal en primer lugar antes de restablecer los nodos de trabajador.
- 2 Restablezca los nodos de trabajador en cualquier orden.
- 3 (Opcional) Restablezca los reenviadores si están configurados.

Asegúrese de restablecer el servidor de vRealize Log Insight (el nodo principal y todos los nodos de trabajador en una agrupación de clúster) se restablezcan antes de restablecer los reenviadores.

- 4 Restablezca los agentes recuperados.

Qué hacer a continuación

- Al restablecer un clúster de vRealize Log Insight, si se usan las mismas direcciones IP, verifique que todas las direcciones IP del nodo restablecido y FQDN estén asociados con su equivalentes originales.

Por ejemplo, el siguiente escenario fallaría. En un clúster de tres nodos con los nodos A, B y C, el nodo A se restablece con la dirección IP B, el nodo B se restablece con la dirección IP C y el nodo C se restablece con la dirección IP A.

- Si se utilizan las mismas direcciones IP solo para un subgrupo de nodos restablecidos, verifique que para estos nodos, todas las imágenes restablecidas estén asociadas con sus direcciones IP originales.
- La mayoría de las herramientas de recuperación ante desastres y restauración de la copia de seguridad proporcionan una vista de supervisión para observar el progreso de las operaciones de restauración por fallos o advertencias. Tome las medidas apropiadas con cualquier problema identificado.
- Si se requieren cambios de configuración manual antes de restablecer el sitio por completo, siga las pautas de [Cambiar configuraciones tras la restauración](#).
- Cuando la restauración finaliza en forma exitosa, realice un control rápido del clúster que se restauró.

Cambiar configuraciones tras la restauración

El objetivo de la recuperación y las personalizaciones de IP durante la configuración de la copia de seguridad determinan qué cambios de configuración manual son necesarios. Debe aplicar cambios de configuración a al menos un nodo de vRealize Log Insight antes de que el sitio restaurado sea completamente funcional.

Restaurar en el mismo host

Restaurar un clúster de vRealize Log Insight en el mismo host es simple y puede realizarse con cualquier herramienta.

Prerequisitos

Revise la información importante sobre [Planificación y preparación](#).

Procedimiento

- 1 Apague el clúster existente antes de iniciar la operación de restauración. De manera predeterminada, se utilizan las mismas direcciones IP y FQDN para los nodos del clúster restaurado.
- 2 (Opcional) Proporcione un nombre nuevo para el clúster.

Durante el proceso de restauración, la copia original del clúster se sobrescribe con la versión restaurada a menos que se proporcione un nombre nuevo a la máquina virtual.
- 3 (Opcional) Si fuera posible, verifique que todos los ajustes de red, IP y FQDN que se utilizan para el entorno de producción se conserven en el sitio restaurado y recuperado.

Qué hacer a continuación

Después de una restauración exitosa y revisión de estado, elimine la copia anterior para conservar recursos y evitar situaciones de procesador dividido accidentales si un usuario enciende la copia anterior.

Restablecer a un host diferente

Cuando realiza una restauración a un host diferente, debe efectuar cambios de configuración en el clúster de vRealize Log Insight.

En vRealize Log Insight 3.0 y versiones posteriores no se admiten oficialmente los cambios en la configuración realizados directamente desde la consola del dispositivo. Consulte el [artículo 2123058 de la base de conocimientos](#) para obtener más información acerca de cómo realizar estos cambios mediante la interfaz de usuario web.

Estos cambios en la configuración son específicos de las compilaciones de vRealize Log Insight que pueden usarse con cualquier herramienta de recuperación de copias de seguridad.

La recuperación en un host diferente requiere efectuar cambios de configuración manuales en el clúster de vRealize Log Insight. Puede asumir que los nodos de vRealize Log Insight restaurados tienen distintas direcciones IP y FQDN que los equivalentes de origen desde los cuales se hizo una copia de seguridad.

Prerequisitos

Revise la información importante sobre [Planificación y preparación](#).

Procedimiento

- 1 Enumere todas las direcciones IP nuevas y FQDN que se asignaron a cada nodo de vRealize Log Insight.
- 2 Realice los siguientes cambios de configuración en el nodo principal. Para ello, siga los pasos descritos en el [artículo 2123058 de la base de conocimientos](#).
 - a En la sección de configuración de vRealize Log Insight, busque líneas similares a las siguientes.

```
<distributed overwrite-children="true">
  <daemon host="prod-es-vrli1.domain.com" port="16520" token="c4c4c6a7-f85c-4f28-
a48f-43aeea27cd0e">
    <service-group name="standalone" />
  </daemon>
  <daemon host="192.168.1.73" port="16520" token="a5c65b52-aff5-43ea-8a6d-38807ebc6167">
    <service-group name="workernode" />
  </daemon>
  <daemon host="192.168.1.74" port="16520" token="a2b57cb5-a6ac-48ee-8e10-17134e1e462e">
    <service-group name="workernode" />
  </daemon>
</distributed>
```

El código muestra tres nodos. El primer nodo es el nodo principal, que muestra `<service-group name=standalone>`, y los dos nodos restantes son los nodos de trabajador, que muestran `<service-group name="workernode">`.

- b Para el nodo principal, en el entorno recientemente recuperado, verifique que se pueda volver a utilizar la entrada DNS que se utilizó en el entorno de recuperación previa.
 - Si es posible reutilizar la entrada de DNS, actualice solo la entrada DNS para que apunte a la nueva dirección IP del nodo principal.
 - Si no es posible reutilizar la entrada DNS, reemplace la entrada del nodo principal con un nuevo nombre de DNS (que apunta a la nueva dirección IP).
 - Si no es posible asignar el nombre de DNS, como última opción, actualice la entrada de la configuración con la nueva dirección IP.
- c Asimismo, actualice las direcciones IP del nodo de trabajador para reflejar las nuevas direcciones IP.

- d En el mismo archivo de configuración, verifique que tenga las entradas que representan NTP, SMTP y las secciones de la base de datos y los adicionadores.

```
<ntp>
  <ntp-servers value="ntp1.domain.com, ntp2.domain.com" />
</ntp>

<smtp>
  <server value="smtp.domain.com" />
  <default-sender value="source.domain.com@domain.com" />
</smtp>

<database>
  <password value="xserttt" />
  <host value="vrli-node1.domain.com" />
  <port value="12543" />
</database>
```

- Si los valores del servidor NTP configurado ya no son válidos en el nuevo entorno, actualice los valores en la sección `<ntp>...</ntp>`
 - Si los valores del servidor SMTP configurado ya no son válidos en el nuevo entorno, actualice los valores en la sección `<smtp>...</smtp>`.
 - Opcionalmente, modifique el valor de transmisor-predeterminado en la sección SMTP. El valor puede ser cualquier valor, pero como práctica sugerida, representa el origen desde donde se envía el correo electrónico.
 - En la sección `<database>...</database>`, modifique el valor del host para que apunte a la dirección IP o al FQDN del nodo principal.
- e En el mismo archivo de configuración, actualice la sección de configuración ILB de vRealize Log Insight.

```
<load-balancer>
  <leadership-lease-renewal-secs value="5" />
  <high-availability-enabled value="true" />
  <high-availability-ip value="10.158.128.165" />
  <high-availability-fqdn value="LB-FQDN.eng.vmware.com" />
  <layer4-enabled value="true" />
  <ui-balancing-enabled value="true" />
</load-balancer>
```

- f En la sección `<load-balancer>...</load-balancer>`, actualice el valor `high-availability-ip` si es diferente de la configuración actual.
- g Asegúrese de actualizar también el FQDN del equilibrador de carga.

- h Reinicie desde la pestaña Clúster de la página Administración en la interfaz de usuario web. Por cada nodo de la lista, seleccione su nombre de host o dirección IP para abrir el panel de detalles y haga clic en **Reiniciar Log Insight**.

Los cambios de configuración se aplican automáticamente a todos los nodos del clúster.

- i Espere 2 minutos después de que se inicie el servicio de vRealize Log Insight para dar tiempo suficiente a que se inicie el servicio Cassandra antes de poner en línea los nodos de trabajador.

Qué hacer a continuación

Verifique que los nodos de vRealize Log Insight restaurados han sido asignados a distintas direcciones IP y FQDN que los equivalentes de origen desde los cuales se tomó una copia de seguridad.

Verificar restauraciones

Debe verificar que todos los clúster de vRealize Log Insight restablecidos sean completamente funcionales.

Prerequisitos

Confirme que el proceso de copia de seguridad y restauración esté completo antes de verificar las configuraciones del nodo y del clúster.

Procedimiento

- 1 Inicie sesión en vRealize Log Insight usando la dirección IP o el FQDN (si está configurado) del equilibrador de carga interna (ILB).
- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Verifique lo siguiente:
 - a Verifique que pueda acceder a todos los nodos del clúster individual usando las direcciones IP respectivas o FQDN.
 - b Verifique el estado de los nodos del clúster desde la página del clúster y asegúrese de que el ILB, si está configurado, también esté en un estado activo.
 - c Verifique la integración de vSphere. Si es necesario, reconfigure la integración. La reconfiguración es necesaria cuando el FQDN o la dirección IP del ILB o del nodo principal se modifican tras la recuperación.
 - d Verifique la integración de vRealize Operations Manager y reconfigúrela nuevamente si fuera necesario.
 - e Verifique que todos los paquetes de contenido y las funciones de la UI estén funcionando en forma apropiada.
 - f Verifique que los agentes y reenviadores de vRealize Log Insight estén funcionando en forma apropiada si están configurados.
- 4 Verifique que las otras funciones clave de vRealize Log Insight estén funcionando según lo esperado.

Qué hacer a continuación

Realice los ajustes necesarios a su plan de copia de seguridad y recuperación para tratar los problemas que puedan haberse identificado durante sus operaciones de copia de seguridad, restauración y verificación.

Recuperación de desastres

Es fundamental tener un plan bien documentado y comprobado para devolver un clúster a su estado operativo rápidamente.

La selección del tipo de replicación es esencial durante la configuración de una máquina virtual para la recuperación de desastres. Considere el Objetivo de punto de recuperación (RPO), el Objetivo de tiempo de recuperación (RTO) y el costo y la escalabilidad al tomar decisiones sobre un tipo de replicación.

En un escenario de recuperación de desastres, a veces no puede restaurar en el mismo sitio si el sitio primario está completamente inactivo. No obstante, en función de la opción que elija, son necesarios algunos pasos manuales para restaurar por completo y devolver el clúster de vRealize Log Insight a un estado en ejecución.

A menos que el clúster de vRealize Log Insight esté completamente inactivo e inaccesible, verifique que las instancias del clúster estén apagadas antes de restaurar el clúster en el nuevo sitio.

Durante una interrupción de energía o un desastre, recupere el clúster de vRealize Log Insight lo antes posible.

Solución de problemas de vRealize Log Insight

15

Puede resolver los problemas comunes relacionados con la administración de vRealize Log Insight antes de llamar a los servicios de atención al cliente de VMware.

Este capítulo cubre los siguientes temas:

- [vRealize Log Insight no tiene espacio en disco](#)
- [Los datos archivados podrían no importarse correctamente](#)
- [Usar la consola del dispositivo virtual para crear un paquete de soporte de vRealize Log Insight](#)
- [Restablecer la contraseña del usuario administrador](#)
- [Restablecer la contraseña del usuario de raíz](#)
- [No se pudo entregar alertas a vRealize Operations Manager](#)
- [Imposible iniciar sesión usando las credenciales de Active Directory](#)
- [SMTP no funciona con la opción STARTTLS habilitada](#)
- [Error en la actualización al no poder validar la firma del archivo .pak](#)
- [Error en la actualización por error interno del servidor](#)

vRealize Log Insight no tiene espacio en disco

Un nodo principal o de trabajador de vRealize Log Insight puede quedarse sin espacio en disco si usa un disco virtual pequeño, y el almacenamiento no está habilitado.

Problema

vRealize Log Insight no tiene espacio en disco si el índice de registros entrantes excede el 3 por ciento del espacio de almacenamiento por minuto.

Origen

En situaciones normales, vRealize Log Insight nunca deja de tener espacio en disco dado que comprueba cada minuto si el espacio libre es menor del 3 por ciento. Si el espacio libre en el dispositivo virtual de vRealize Log Insight cae por debajo del 3 por ciento, se retiran los depósitos de datos antiguos.

No obstante, si el disco es pequeño y el índice de consumo de registros es tan alto que el espacio libre (3 por ciento) se completa en 1 minuto, vRealize Log Insight se queda sin espacio en disco.

Si el archivo está habilitado, vRealize Log Insight archiva el depósito antes de retirarlo. Si el espacio libre se completa antes de archivar el depósito antiguo y retirarlo, vRealize Log Insight se queda sin espacio en disco.

Solución

- ◆ Aumente la capacidad de almacenamiento del dispositivo virtual de vRealize Log Insight. Consulte [Aumentar la capacidad de almacenamiento del dispositivo virtual de vRealize Log Insight](#).

Los datos archivados podrían no importarse correctamente

Los datos archivados podrían no importarse correctamente si el dispositivo virtual vRealize Log Insight se queda sin espacio de disco.

Problema

La utilidad de importación del repositorio de vRealize Log Insight no comprueba si hay espacio de disco disponible en el dispositivo virtual vRealize Log Insight. Por lo tanto, los registros archivados podrían no importarse correctamente si el dispositivo virtual se queda sin espacio en disco.

Solución

Aumente la capacidad de almacenamiento del dispositivo virtual vRealize Log Insight y vuelva a iniciar la importación. [Aumentar la capacidad de almacenamiento del dispositivo virtual de vRealize Log Insight](#). Se duplicará la información que se importó correctamente antes de producirse el error.

Usar la consola del dispositivo virtual para crear un paquete de soporte de vRealize Log Insight

Si no es posible acceder a la interfaz de usuario web de vRealize Log Insight, puede descargar el paquete de soporte con la consola del dispositivo virtual o después de establecer una conexión SSH con el dispositivo virtual de vRealize Log Insight.

Prerequisitos

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- If you plan to connect to the vRealize Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.

Procedimiento

- 1 Establezca una conexión SSH con vRealize Log Insight vApp e inicie sesión como usuario raíz.
- 2 Para generar el paquete de soporte, ejecute `loginsight-support`.

Para generar un paquete de soporte e incluir solo los archivos que se han modificado dentro de un cierto período de tiempo, ejecute el comando `loginsight-support` con la restricción `--days`. Por ejemplo, `--days=1` solo incluye archivos que se han modificado dentro de 1 día.

La información de soporte se recopila y se almacena en un archivo *.tar.gz que tiene la siguiente convención de denominación: loginsight-support-YYYY-MM-DD_HHMMSS.xxxxx.tar.gz, donde xxxxx es el identificador del proceso bajo el cual se ejecuta el proceso de loginsight-support.

Qué hacer a continuación

Reenvíe el paquete de soporte al servicio de soporte de VMware conforme a lo solicitado.

Restablecer la contraseña del usuario administrador

Si un usuario administrador olvida la contraseña a la interfaz de usuario web, no será posible acceder a la cuenta.

Problema

Si vRealize Log Insight solo tiene un usuario administrador y olvida la contraseña, no se podrá administrar la aplicación. Si un usuario administrador es el único usuario de vRealize Log Insight, la interfaz de usuario web completa queda inaccesible.

Origen

vRealize Log Insight no proporciona una interfaz de usuario para que los usuarios administradores restablezcan sus propias contraseñas si no recuerdan sus contraseñas actuales.

NOTA: Los usuarios administradores que pueden iniciar sesión pueden restablecer la contraseña de otros usuarios administradores. Restablezca la contraseña de usuario administrador solo cuando no se conozca ninguna otra contraseña de las cuentas de usuario administrador.

Solución

Prerequisitos

- Verifique que tiene las credenciales del usuario raíz para iniciar sesión en el dispositivo virtual de vRealize Log Insight. Consulte [Configurar la contraseña SSH raíz para el dispositivo virtual vRealize Log Insight](#)
- Para habilitar conexiones SSH, verifique que el puerto 22 de TCP esté abierto.

Procedimiento

- 1 Establezca una conexión SSH con el dispositivo virtual de vRealize Log Insight e inicie sesión como usuario raíz.
- 2 Escriba `li-reset-admin-passwd.sh` y presione **Entrar**.

El script restablece la contraseña del usuario administrador, genera una contraseña nueva y la muestra en la pantalla.

Qué hacer a continuación

Inicie sesión en la interfaz de usuario web de vRealize Log Insight con la contraseña nueva y modifique la contraseña del usuario administrador.

Restablecer la contraseña del usuario de raíz

Si olvida la contraseña del usuario de raíz, no podrá establecer las conexiones SSH ni utilizar la consola del dispositivo virtual de vRealize Log Insight.

Problema

Si no puede establecer las conexiones SSH ni utilizar la consola del dispositivo virtual de vRealize Log Insight, no podrá realizar algunas de las tareas de administración ni restablecer la contraseña del usuario administrador.

Solución

Son varios los motivos por los que no pueda iniciar sesión como usuario raíz:

- No cambió la contraseña predeterminada. vRealize Log Insight establece de forma predeterminada una contraseña vacía para el usuario raíz y, además, impide el acceso a SSH. Cuando defina la contraseña, se permitirá el acceso a SSH para el usuario raíz.
- Configuró una clave SSH durante la implementación del dispositivo virtual de vRealize Log Insight. Si se especificó una clave SSH a través de OVF, la autenticación de contraseña estará deshabilitada. Inicie sesión con la clave SSH configurada o consulte los pasos para solucionar el problema que aparecen más abajo.
- Escribió mal la contraseña varias veces y ahora está temporalmente bloqueado. Si así es, no podrá iniciar sesión con la contraseña hasta que transcurra el período de bloqueo. Puede esperar o reiniciar el dispositivo virtual.

Procedimiento

- 1 En vSphere Client, realice un apagado de invitado del dispositivo virtual de vRealize Log Insight.
- 2 Con la máquina virtual apagada, seleccione **Editar ajustes**.
- 3 Seleccione la pestaña **Opciones**.
- 4 En **Opciones de vApp > Opciones avanzadas**, seleccione **Propiedades**.
- 5 Busque y modifique la clave `vm.rootpw`.

Si no ve una clave `vm.rootpw`, agregue una nueva.

Si usa claves SSH en lugar de la autenticación con contraseña, edite o añada la clave `vm.sshkey`.
- 6 Escriba una contraseña.

Si no usa la autenticación con contraseña, puede agregar en su lugar una clave SSH.
- 7 Encienda el dispositivo virtual.

Qué hacer a continuación

Cuando vRealize Log Insight se inicie, confirme que puede iniciar sesión como usuario raíz.

No se pudo entregar alertas a vRealize Operations Manager

vRealize Log Insightle notifica si un evento de alerta no se puede enviar a vRealize Operations Manager. vRealize Log Insight intenta enviar de nuevo la alerta cada minuto hasta que el problema se resuelva.

Problema

Aparece una señal roja con un signo de exclamación en la barra de herramientas de vRealize Log Insight cuando no se pudo entregar una alerta a vRealize Operations Manager.

Origen

Los problemas de conectividad evitan que vRealize Operations Manager vRealize Log Insight envíe notificaciones de alerta a vRealize Operations Manager.

Solución

- Haga clic en el icono rojo para abrir la lista de mensajes de error, y desplácese hacia abajo para ver el último mensaje.

La señal roja desaparecerá de la barra de herramientas cuando abra la lista de mensajes de error o cuando se resuelva el problema.

- Para solucionar el problema de conectividad con vRealize Operations Manager, intente lo siguiente.
 - Compruebe que la vApp vRealize Operations Manager no esté desconectada.
 - Compruebe que puede conectarse con vRealize Operations Manager mediante el botón **Probar conexión** en la sección **vRealize Operations Manager** de la página **Administración** de la interfaz de usuario web de vRealize Log Insight.
 - Compruebe que cuenta con las credenciales correctas iniciando sesión directamente en vRealize Operations Manager.
 - Revise los registros de vRealize Log Insight y vRealize Operations Manager para encontrar mensajes relacionados con problemas de conectividad.
 - Compruebe que no se filtren alertas en la interfaz de usuario vSphere de vRealize Operations Manager.

Imposible iniciar sesión usando las credenciales de Active Directory

No puede iniciar sesión en la interfaz de usuario web de vRealize Log Insight cuando utiliza las credenciales de Active Directory.

Problema

No es posible iniciar sesión en vRealize Log Insight usando sus credenciales de usuario de dominio de Active Directory a pesar de que un administrador ha añadido su cuenta de Active Directory a vRealize Log Insight.

Origen

Las causas más comunes son las contraseñas que han caducado, credenciales incorrectas, problemas de conectividad o falta de sincronización entre el dispositivo virtual de vRealize Log Insight y los relojes de Active Directory.

Solución

- Verifique que sus credenciales sean válidas, que la contraseña no haya caducado y que no esté bloqueada su cuenta de Active Directory.
- Si no ha especificado un dominio para usar con la autenticación de Active Directory, verifique que tenga una cuenta en el dominio predeterminado almacenada en la última configuración de vRealize Log Insight en `/storage/core/loginsight/config/loginsight-config.xml#[number]`, donde el [número] es el mayor.
- Busque el archivo de configuración más actualizado: `/storage/core/loginsight/config/loginsight-config.xml#[number]` donde [number] es el mayor.
- Verifique que vRealize Log Insight tenga conectividad con el servidor Active Directory.
 - Vaya a la sección **Autenticación** de la página **Administración** de la interfaz de usuario web de vRealize Log Insight, introduzca sus credenciales de usuario y haga clic en el botón **Probar conexión**.
 - Revise vRealize Log Insight `/storage/var/loginsight/runtime.log` para ver los mensajes relacionados con los problemas de DNS.
- Verifique que los relojes de Active Directory y vRealize Log Insight estén sincronizados.
 - Revise vRealize Log Insight `/storage/var/loginsight/runtime.log` para ver los mensajes relacionados con la desviación del reloj.
 - Utilice un servidor NTP para sincronizar los relojes de Active Directory y vRealize Log Insight.

SMTP no funciona con la opción STARTTLS habilitada

Cuando configura el servidor SMTP con la opción STARTTLS habilitada, los correos electrónicos de prueba fallan. Añada su certificado SSL para el servidor SMTP al almacén de confianza de Java para resolver el problema.

Prerequisitos

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- If you plan to connect to the vRealize Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.

Procedimiento

- 1 Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
- 2 Copie el certificado SSL para el servidor SMTP en vApp de vRealize Log Insight.
- 3 Ejecute el siguiente comando:

```
`/usr/java/latest/bin/keytool -import -alias certificado_nombre -file ruta_acceso_al_certificado -keystore /usr/java/latest/lib/security/cacerts`
```

NOTA: Se insertan las comillas exteriores usando el símbolo de comillas invertidas que se encuentra en la misma tecla que la tilde en el teclado. No utilice comillas simples.

- 4 Introduzca la contraseña predeterminada **changeit**.
- 5 Ejecute el comando `service loginsight restart`.

Qué hacer a continuación

Desplácese hasta **Administración > Smtip** y utilice **Enviar correo electrónico de prueba** para probar sus ajustes. Consulte [Configurar el servidor SMTP para vRealize Log Insight](#)

Error en la actualización al no poder validar la firma del archivo .pak

Error en la actualización de vRealize Log Insight debido a un archivo .pak dañado, licencia caduca o espacio insuficiente en el disco.

Problema

Error en la actualización de vRealize Log Insight. Se muestra el mensaje de error `Error en la actualización. Error en la actualización: no se pudo validar la firma del archivo PAK.`

Origen

El error podría producirse por los siguientes motivos:

- El archivo cargado no es un archivo .pak.
- El archivo .pak cargado no está completo.
- La licencia de vRealize Log Insight ha caducado.
- El sistema del archivo de raíz del dispositivo virtual de vRealize Log Insight no tiene espacio suficiente en el disco.

Solución

- Verifique que esté cargando un archivo .pak.
- Verifique el md5sum del archivo .pak y compárelo con el sitio de descarga de VMware.
- Verifique que se configure al menos una licencia válida en vRealize Log Insight.
- Inicie sesión en el dispositivo virtual de vRealize Log Insight y ejecute `df -h` para revisar el espacio disponible en el disco.

NOTA: No coloque archivos en el sistema de archivos de raíz del dispositivo virtual de vRealize Log Insight.

Error en la actualización por error interno del servidor

La actualización de vRealize Log Insight falla con un error interno del servidor a causa de un problema de conexión.

Problema

Error en la actualización de vRealize Log Insight. Se muestra el mensaje de error `Error en la actualización. Error interno del servidor.`

Origen

Se produjo un problema de conexión entre el cliente y el servidor. Por ejemplo, cuando intenta actualizar desde un cliente que está en una WAN.

Solución

- ◆ Actualice LI desde un cliente en la misma LAN que el servidor.