

Introducción a vRealize Log Insight

24 de mayo de 2022
vRealize Log Insight 8.1

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

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

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

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

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

Contenido

Primeros pasos con vRealize Log Insight 4

1 Antes de instalar vRealize Log Insight 5

Formatos de archivos y archivos de registro admitidos en vRealize Log Insight 5

Requisitos de seguridad 6

Compatibilidad de productos 6

Requisitos mínimos 8

Planificar la implementación de vRealize Log Insight 10

Dimensionar el dispositivo virtual de vRealize Log Insight 12

Integrar vRealize Log Insight y vRealize Operations Manager 14

2 Ciclo de vida de un evento 15

Aspectos clave del ciclo de vida del evento 16

3 Instalar vRealize Log Insight 18

Implementar el dispositivo virtual vRealize Log Insight 18

Iniciar una nueva implementación de vRealize Log Insight 21

Unirse a una implementación existente 23

4 Programa de mejora de la experiencia de cliente 26

Primeros pasos con vRealize Log Insight

Introducción con vRealize Log Insight proporciona información acerca de la implementación y configuración de VMware® vRealize™ Log Insight™, incluida la información sobre cómo dimensionar el dispositivo virtual de vRealize Log Insight para recibir mensajes de registro.

Utilice esta información cuando desee planificar o instalar su implementación. Está destinada a administradores de sistemas Linux y Windows con experiencia que están familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Antes de instalar vRealize Log Insight

1

Para comenzar a utilizar vRealize Log Insight en su entorno, debe implementar el dispositivo virtual vRealize Log Insight y aplicar varias configuraciones básicas.

Este capítulo incluye los siguientes temas:

- Formatos de archivos y archivos de registro admitidos en vRealize Log Insight
- Requisitos de seguridad
- Compatibilidad de productos
- Requisitos mínimos
- Planificar la implementación de vRealize Log Insight
- Dimensionar el dispositivo virtual de vRealize Log Insight
- Integrar vRealize Log Insight y vRealize Operations Manager

Formatos de archivos y archivos de registro admitidos en vRealize Log Insight

Puede usar vRealize Log Insight para analizar los datos del registro estructurados o no estructurados.

vRealize Log Insight acepta datos de los siguientes orígenes:

- Orígenes que admiten el envío de corrientes de registros con el protocolo syslog.
- Orígenes que escriben archivos de registro y pueden ejecutar el agente vRealize Log Insight.
- Orígenes que pueden publicar datos de registro con HTTP o HTTPS a través de REST API. La documentación de la API está disponible en la interfaz de vRealize Log Insight en `https://<host_de_vRLI>/rest-api`.
- Datos históricos archivados por vRealize Log Insight.

El analizador de registros de vSphere le permite importar paquetes de registros de vSphere a 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.

Consulte cómo [importar un archivo de Log Insight en vRealize Log Insight](#) en *Administrar vRealize Log Insight*.

Requisitos de seguridad

Para asegurarse de que su entorno virtual esté protegido de los ataques externos, debe tener en cuenta ciertas reglas.

- Instale siempre vRealize Log Insight en una red de confianza.
- Guarde siempre los paquetes de soporte de vRealize Log Insight en una ubicación segura.

Los responsables de la toma de decisiones de TI, los arquitectos, los administradores y otras personas que deben familiarizarse con los componentes de seguridad de vRealize Log Insight deben leer los temas sobre seguridad de *Administrar vRealize Log Insight*.

Estos temas proporcionan referencias concisas a las funciones de seguridad de vRealize Log Insight. Los temas incluyen las interfaces externas del producto, puertos, mecanismos de autenticación y opciones para la configuración y la administración de las funciones de seguridad.

Para obtener información acerca de asegurar su entorno virtual, consulte la *Guía de seguridad VMware vSphere* y el centro de seguridad en el sitio web de VMware.

Compatibilidad de productos

vRealize Log Insight recopila los datos sobre el protocolo syslog y HTTP, puede conectarse con vCenter Server para recopilar eventos, tareas y datos de alarmas, y puede integrarse con vRealize Operations Manager para enviar eventos de notificación y habilitar la ejecución en contexto. Revise las *notas de la versión de VMware vRealize Log Insight* para conocer la última actualización sobre las versiones de productos admitidas.

Implementación del dispositivo virtual

Debe implementar el dispositivo virtual de vRealize Log Insight con vSphere. Utilice siempre vSphere Client para conectarse con vCenter Server. El dispositivo virtual de vRealize Log Insight debe implementarse en una versión de host ESX/ESXi 5.0 o posterior administrada con vCenter Server versión 5.0 o posterior.

Feeds de syslog

vRealize Log Insight recopila y analiza los datos de syslog a través de los siguientes puertos y protocolos:

- 514/UDP
- 514/TCP
- 1514/TCP (SSL)

Debe configurar los componentes del entorno, como sistemas operativos, aplicaciones, almacenamiento, firewalls y dispositivos de red para que inserten sus feeds de syslog en vRealize Log Insight.

Feeds de API

La API de consumo de vRealize Log Insight recopila datos a través de los siguientes puertos y protocolos.

- 9000/TCP
- 9543/TCP (SSL)

Integración de vSphere

Es posible configurar vRealize Log Insight para que extraiga datos para tareas, eventos y alarmas que se produjeron en una o más instancias de vCenter Server. vRealize Log Insight utiliza vSphere API para conectarse con los sistemas vCenter Server y recopilar datos.

Es posible configurar hosts de ESXi para reenviar los datos de syslog a vRealize Log Insight.

Para obtener información de compatibilidad con versiones específicas de vCenter Server y del ESXi, consulte [Matrices de interoperabilidad de productos VMware](#).

Para obtener más información sobre cómo conectarse a un entorno vSphere, consulte la sección sobre cómo [conectar vRealize Log Insight a un entorno vSphere](#).

Integración de vRealize Operations Manager

La vApp o la versión instalable de vRealize Log Insight y vRealize Operations Manager pueden integrarse de dos maneras independientes.

Todas las versiones compatibles de vCenter Operations Manager admiten tanto las notificaciones como la ejecución en contexto.

- vRealize Log Insight puede enviar eventos de notificación a vRealize Operations Manager.
Consulte [Configurar vRealize Log Insight para enviar eventos de notificación a vRealize Operations Manager](#).
- La ejecución en el menú contextual de vRealize Operations Manager puede mostrar acciones relacionadas con vRealize Log Insight.

Consulte [Habilitar ejecución en contexto para vRealize Log Insight en vRealize Operations Manager](#).

Requisitos mínimos

VMware distribuye vRealize Log Insight como dispositivo virtual en formato de archivo OVA. Para que el dispositivo se ejecute correctamente, deben estar disponibles diversos recursos y aplicaciones. Consulte los requisitos y la información más actualizada en las notas de la versión más recientes.

Hardware virtual

Durante la implementación del dispositivo virtual de vRealize Log Insight, puede seleccionar distintos tamaños desde la configuración preestablecida, según los requisitos de consumo para el 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, descrita en la siguiente tabla, consume los recursos mínimos sin dejar de estar admitida. También está disponible una configuración muy reducida, pero solo es apropiada para demostraciones.

Para ver los requisitos completos de recursos en función de los requisitos de consumo, consulte [Dimensionar el dispositivo virtual de vRealize Log Insight](#)

Tabla 1-1. Valores preestablecidos para configuraciones reducidas

Recursos	Requisito mínimo
Memoria	8 GB
vCPU	4
Espacio de almacenamiento	530 GB

Exploradores admitidos

Puede utilizar uno de estos exploradores para conectarse con la interfaz de usuario web de vRealize Log Insight. Las versiones más recientes del explorador también funcionan con vRealize Log Insight, pero no han sido validadas.

Importante Se deben habilitar las cookies en su explorador.

- Mozilla Firefox 45.0 y versiones posteriores
- Google Chrome 51.0 y versiones posteriores
- Safari 9.1 y versiones posteriores

- Internet Explorer 11.0 y versiones posteriores

Nota

- En el **modo de estándares** se debe establecer el modo de documento de Internet Explorer. No se admiten otros modos.
- **Modo Navegador:** no se admite la vista de compatibilidad.
- Para usar Internet Explorer con el cliente web vRealize Log Insight, el nivel de integridad del almacenamiento local de Windows se debe establecer como aparece a continuación.

Contraseñas de la cuenta

Tipo	Requisitos
Raíz	<p>A menos que se especifique una contraseña de raíz o se utilice una personalización para invitado durante la implementación de OVA, las credenciales predeterminadas para el usuario de raíz en el dispositivo virtual vRealize Log Insight son root/<blank>. Se le solicita cambiar la contraseña de la cuenta de raíz al acceder por primera vez a la consola del dispositivo virtual de vRealize Log Insight.</p> <p>Nota SSH está deshabilitado hasta que configura la contraseña raíz.</p>
Cuenta de usuario	<p>Las cuentas de usuario que se crean en vRealize Log Insight 3.3 y versiones posteriores requieren una contraseña segura. La contraseña debe tener al menos 8 caracteres de extensión y debe contener una letra mayúscula, una letra minúscula, un número y un carácter especial.</p>

Requisitos de integración

Producto	Requisito
vCenter Server	<p>Para extraer eventos, tareas e información de alarmas de un servidor vCenter Server, debe proporcionar un conjunto de credenciales de usuario para ese servidor vCenter Server. La función mínima requerida para registrar vRealize Log Insight y eliminarlo del registro con vCenter Server es Solo lectura. La función debe establecerse en el nivel de vCenter Server y propagarse a los objetos secundarios. Para configurar los hosts de ESXi que administra un servidor vCenter Server, vRealize Log Insight requiere privilegios adicionales.</p>
vSphere ESXi	<p>Se requiere vSphere ESXi 6.0 actualización 1 o posterior para establecer conexiones SSL con vRealize Log Insight.</p>
vRealize Operations Manager	<p>Para habilitar los eventos de notificación y la funcionalidad de ejecución en contexto en una instancia de vRealize Operations Manager, debe proporcionar las credenciales del usuario para esa instancia de vRealize Operations Manager.</p>

Requisitos del puerto de red

Los siguientes puertos de red deben estar accesibles en forma externa.

Puerto	Protocolo
22/TCP	SSH

Puerto	Protocolo
80/TCP	HTTP
443/TCP	HTTPS
514/UDP, 514/TCP	Syslog
1514/TCP	Consumo syslog a través de SSL únicamente
9000/TCP	API de consumo de vRealize Log Insight
9543/TCP	API de consumo (SSL) de vRealize Log Insight

Planificar la implementación de vRealize Log Insight

Puede implementar vRealize Log Insight con un solo nodo, un solo clúster o un clúster con reenviadores.

Nota No se admite el uso de equilibradores de carga externos con vRealize Log Insight, incluidos los clústeres de vRealize Log Insight.

Instalación mediante vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager automatiza las operaciones de instalación, configuración, actualización, revisión, administración de configuración, solución de desviaciones y mantenimiento de los productos en paquetes. Como alternativa a la instalación con vRealize Log Insight, puede instalar vRealize Log Insight mediante vRealize Suite Lifecycle Manager. Debe usar vRealize Suite Lifecycle Manager 1.2 o una versión posterior y vRealize Log Insight 4.5.1 o posterior. Consulte la [Documentación de vRealize Suite Lifecycle Manager](#) para obtener más información.

Nodos únicos

Una configuración básica de vRealize Log Insight incluye un solo nodo. Los orígenes de registro pueden ser aplicaciones, registros de SO, registros de máquinas virtuales, hosts, vCenter Server, conmutadores y enrutadores físicos o virtuales, hardware de almacenamiento, etc. Los flujos del registro se transportan al nodo vRealize Log Insight usando syslog (UDP, TCP, TCP+SSL) o CFAPI (el protocolo de consumo nativo vRealize Log Insight mediante HTTP o HTTPS), ya sea en forma directa mediante una aplicación, mediante un concentrador de syslog o mediante el agente de vRealize Log Insight instalado en el origen.

Como práctica recomendada para las implementaciones de un único nodo, se recomienda usar el equilibrador de carga integrado (ILB) de vRealize Log Insight y enviar las consultas y el tráfico de consumo al ILB. Si desea agregar nodos y crear un clúster para la implementación en el futuro, esto no supone una sobrecarga y simplifica la configuración.

Como práctica recomendada, no utilice nodos únicos para los entornos de producción.

Clústeres

Por lo general, los entornos de producción requieren el uso de clústeres. Los clústeres deben cumplir los requisitos siguientes:

- Todos los nodos de los clústeres deben ser del mismo tamaño y estar en el mismo centro de datos.
- El ILB usado con los clústeres requiere que todos los nodos estén en la misma red de Capa 2.
- Las máquinas virtuales de vRealize Log Insight se deben excluir de la protección de VMware NSX Distributed Firewall.

El motivo es que las IP virtuales de los clústeres usan Linux Virtual Server en modo retorno de servidor directo (LVS-DR) para equilibrar la carga. El retorno de servidor directo es más eficaz que enrutar todo el tráfico de respuesta a través de un único miembro del clúster. Sin embargo, también puede parecer tráfico falsificado, que NSX Distributed Firewall bloquea.

Dimensionamiento de clústeres

Una configuración de un solo clúster de vRealize Log Insight puede incluir de tres a 18 nodos y usa el ILB. Un clúster requiere un mínimo de tres nodos en buen estado para poder funcionar correctamente.

Los entornos de producción requieren que los nodos sean al menos de tamaño medio. Si se anticipa trabajando con un número elevado de consultas al mismo tiempo, incluidas las alertas, considere la posibilidad de usar nodos de gran tamaño. Para obtener más información sobre el tamaño, consulte [Dimensionar el dispositivo virtual de vRealize Log Insight](#).

A pesar de que el número mínimo de nodos en un clúster de vRealize Log Insight es de tres, si se produce un error de los nodos, un clúster con menos de tres nodos en buen estado no será plenamente funcional. Además, el número de nodos en buen estado en el clúster debe ser superior a la mitad de la cantidad total de nodos del clúster. Por ejemplo, si tiene un clúster de seis nodos y tres de los nodos dejan de estar disponibles, el clúster no será plenamente funcional hasta que elimine los nodos no funcionales del clúster. No se permite extraer y volver a introducir un nodo del clúster.

Clústeres con reenviadores

Una configuración de clúster de vRealize Log Insight con reenviadores incluye la indexación principal, el almacenamiento y un clúster de consultas con entre 3 y 18 nodos que usan el ILB. Aparece un mensaje de registro en una única ubicación dentro del clúster principal, al igual que sucede con un solo clúster.

El diseño se extiende a través de la adición de múltiples clúster de reenviadores en sitios remotos de clústeres. Cada clúster de reenviador se configura para reenviar todos sus mensajes de registro al clúster principal. Al mismo tiempo, los usuarios se conectan a dicho clúster, aprovechando CFAPI para la compresión y la resiliencia de la ruta de acceso de reenvío. Los clústeres de reenviadores configurados como parte superior del bastidor pueden configurarse con una retención local más grande.

Reenvío para redundancia

Este escenario de implementación de vRealize Log Insight incluye un clúster con reenviador que se extiende y espeja. Se usan dos clústeres principales para indexación, almacenamiento y consulta. Hay un clúster principal en cada centro de datos. Cada uno tiene una conexión front-end con un par de clústeres de reenviadores dedicados. Todos los orígenes de registro de todas las agregaciones de la parte superior del bastidor se concentran en los clústeres de reenviadores. Puede consultar independientemente los mismos registros en ambos clústeres de retención.

Equilibrador de carga integrado de vRealize Log Insight

Para equilibrar el tráfico correctamente entre los nodos de un clúster y para minimizar la sobrecarga administrativa, use el equilibrador de carga integrado (ILB) en todas las implementaciones. Esto garantiza que el tráfico de consumo entrante se acepte, aunque algunos nodos de vRealize Log Insight no estén disponibles.

Dimensionar el dispositivo virtual de vRealize Log Insight

De forma predeterminada, el dispositivo virtual de vRealize Log Insight usa los valores preestablecidos para configuraciones reducidas.

Implementación independiente

Puede cambiar la configuración del dispositivo para cumplir las necesidades del entorno del que pretende recopilar registros durante la implementación.

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.

Tamaño preestablecido	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
Mediano	75 GB por día	8	16 GB	1000	250	5000
Grande	225 GB por día	16	32 GB	1500	750	15.000

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.

El dimensionamiento se basa sobre los siguientes supuestos.

- Cada CPU virtual tiene una velocidad de al menos 2 GHz.
- Cada host ESXi envía hasta 10 mensajes por segundo con un tamaño promedio de 170 bytes por mensaje, lo que equivale aproximadamente a 150 MB al día por host.

Nota Para las instalaciones grandes, debe actualizar la versión del hardware virtual de la máquina virtual de vRealize Log Insight. vRealize Log Insight admite el hardware virtual versión 7 o posterior. El hardware virtual versión 7 puede admitir hasta 8 CPU virtuales. Por lo tanto, si va a aprovisionar 16 CPU virtuales, debe actualizar a la versión 8 o posterior del hardware virtual para ESXi 5.x. Utilice vSphere Client para actualizar el hardware virtual. Si desea actualizar el hardware virtual con la última versión, debe leer y comprender la información del artículo de la base de conocimientos de VMware [Actualización de una máquina virtual con la última versión de hardware \(1010675\)](#).

Implementación de clúster

Utilice una configuración mediana, o más grande, para los nodos principal y de trabajador en un clúster de vRealize Log Insight. La cantidad de eventos por segundo se incrementa en forma lineal con la cantidad de nodos. Por ejemplo, en un clúster de 3 a 18 nodos (los clústeres deben tener un mínimo de tres nodos), el consumo en un clúster de 18 nodos es de 270.000 eventos por segundo (EPS) o 4 TB de eventos por día.

Reducir el tamaño de la memoria

Utilice la versión del dispositivo **Extrapequeño** en un entorno de prueba o prueba de concepto, pero no en un entorno de producción. Esta configuración admite hasta 20 hosts ESXi (~200 eventos/segundo o ~3 GB/día).

Calculadora de tamaño de vRealize Log Insight

Puede disponer de una calculadora para ayudarle a determinar el tamaño de vRealize Log Insight, del uso del almacenamiento y la red. Esta calculadora sirve únicamente a modo de orientación. Un gran número de entradas de entorno son específicas del sitio, por lo que la calculadora utiliza necesariamente estimaciones en determinadas áreas. Consulte <https://www.vmware.com/go/loginsight/calculator>.

Nota El rendimiento general de vRealize Log Insight puede degradarse si los reenviadores se definen en el campo de texto con condiciones complejas o múltiples que impliquen expresiones regulares, por ejemplo "**text=~\"Eliminación de la máquina\"**". En estos casos, en concreto, cuando la carga general en el clúster es alta, el rendimiento puede retrasarse y los bloques de disco pueden acumularse en cada nodo del clúster.

Integrar vRealize Log Insight y vRealize Operations Manager

Para habilitar la integración entre vRealize Log Insight y vRealize Operations Manager, la configuración debe realizarse en ambos productos.

Procedimiento

- 1 Instale el paquete de administración de vRealize Log Insight en vRealize Operations Manager.

El paquete de administración de vRealize Log Insight es necesario para la funcionalidad de Ejecución en contexto entre los dos productos. El paquete de administración de vRealize Log Insight está disponible con el archivo de descarga de vRealize Operations Manager o en el sitio web de VMware Solution Exchange.

- 2 Configure vRealize Log Insight para conectarse a vRealize Operations Manager.
- 3 Configure alertas de vRealize Log Insight para reenviar información a vRealize Operations Manager.

Consulte [Configurar vRealize Log Insight para enviar eventos de notificación a vRealize Operations Manager](#) en la guía de *administración de vRealize Log Insight*.

- 4 Habilite la ejecución en contexto de vRealize Operations para consultar registros en vRealize Log Insight.

Consulte [Habilitar ejecución en contexto para vRealize Log Insight en vRealize Operations Manager](#) en la guía de *administración de vRealize Log Insight*.

Ciclo de vida de un evento

2

Comprender cómo vRealize Log Insight procesa mensajes y eventos resulta clave para un uso eficiente de vRealize Log Insight.

El ciclo de vida de un evento o mensaje de registro tiene varias etapas, incluyendo lectura, análisis, consumo, indexación, alertas, aplicación de consulta, archivado y eliminación.

Los mensajes y eventos van pasando por las siguientes etapas.

- 1 Se genera en un dispositivo (fuera de vRealize Log Insight).
- 2 Se selecciona y se envía a vRealize Log Insight siguiendo uno de estos procedimientos:
 - Con un agente de vRealize Log Insight que usa syslog o API de consumo
 - A través de un agente de terceros, como rsyslog, syslog-ng o log4j que usa syslog
 - Personalizando la escritura de API de consumo (por ejemplo, log4j.append)
 - Personalizando la escritura de syslog (por ejemplo, log4j.append)
- 3 vRealize Log Insight recibe el evento.
 - Si utiliza el equilibrador de carga integrado (ILB), el evento se envía a un nodo único que se encarga de procesarlo.
 - Si se rechaza el evento, el cliente maneja los rechazos con eliminaciones UDP, TCP con configuración de protocolos o CFAPI con una cola respaldada en disco.
 - Si se acepta el evento, se notifica al cliente.
- 4 El evento se envía a través de la canalización del consumo de vRealize Log Insight, en el que se producen los siguientes pasos:
 - Se crea un índice de palabras clave o se actualiza el existente. El índice se almacena en un formato del fabricante en un disco local.
 - Se aplica el aprendizaje automático a los eventos del clúster.
 - El evento se almacena en un formato del fabricante comprimido en el disco local en un depósito.
- 5 Se consulta el evento.
 - Se buscan coincidencias entre el índice de palabras clave y consultas globales y de palabras clave.

- Se buscan coincidencias de Regex con eventos comprimidos.
- 6 El evento se mueve a un depósito y se archiva.
 - Un depósito se sella y archiva cuando llega a 0,5 GB.
- 7 Se elimina el evento.
 - Los depósitos se eliminan en orden FIFO.

Más información

Para obtener más información, consulte el vídeo de las publicaciones técnicas de VMware sobre



el ciclo de vida de un evento de registro en vRealize Log Insight.

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_horp849x/uiConfId/50138843/)

Este capítulo incluye los siguientes temas:

- [Aspectos clave del ciclo de vida del evento](#)

Aspectos clave del ciclo de vida del evento

Existen aspectos clave de la administración y del almacenamiento de eventos durante su ciclo de vida que se deben conocer.

Almacenamiento de eventos

Cada evento se almacena en un depósito en disco individual. Cuando trabaje con depósitos, tenga en cuenta los siguientes comportamientos y características.

- Los depósitos pueden tener un tamaño máximo de 0,5 GB. Cuando un depósito llega a 0,5 GB, se sella y se ponen en cola para el archivado. Después de archivar un depósito sellado, se marca como archivado. Se puede retener un evento localmente y en los archivos al mismo tiempo.
- Los depósitos no se replican entre los nodos de vRealize Log Insight. Si pierde un nodo, perderá los datos que se encuentren en él.
- Todos los depósitos se almacenan en la partición `/storage/core`.
- vRealize Log Insight elimina los depósitos antiguos cuando el espacio disponible en la partición `/storage/core` es inferior al 3%. La eliminación sigue un modelo FIFO.

Nota Una partición `/storage/core` casi completa es habitual y previsible. Esa partición nunca debe alcanzar el 100 % dado que vRealize Log Insight administra la partición. Sin embargo, no intente almacenar datos en esa partición, ya que puede interferir con la eliminación de depósitos anteriores.

Administración de eventos

Al instalar y configurar el producto, resulta útil estar familiarizado con las siguientes características y comportamientos de los eventos de vRealize Log Insight y la administración de eventos.

- Tras eliminar un evento de forma local, ya no puede consultarse a menos que se importe desde el archivo usando la interfaz de la línea de comandos.
- Después de eliminar todos los eventos de un clúster de aprendizaje automático de vRealize Log Insight, se elimina el clúster.
- vRealize Log Insight vuelve a equilibrar todos los eventos entrantes de manera uniforme entre los nodos en el clúster. Por ejemplo, aunque un nodo se envíe de forma explícita a un evento, puede que no sea el nodo que consuma el evento.
- Los metadatos del evento se almacenan en un formato de propiedad en un nodo de vRealize Log Insight individual y no en una base de datos.
- Un evento puede existir localmente en un nodo y en el archivo.

Instalar vRealize Log Insight

3

vRealize Log Insight se entrega como un dispositivo virtual que implementa en su entorno vSphere.

Después de revisar [Dimensionar el dispositivo virtual de vRealize Log Insight](#), proceda a [Implementar el dispositivo virtual vRealize Log Insight](#). Independientemente de si tiene una implementación de nodo simple o de clúster, siga el procedimiento estándar para implementar OVF que se describe en esta sección.

Nota Puede utilizar vRealize Suite Lifecycle Manager 1.2 o una versión posterior para instalar vRealize Log Insight 4.5.1 y versiones posteriores. Consulte la [documentación de vRealize Suite](#) para obtener más información.

Este capítulo incluye los siguientes temas:

- [Implementar el dispositivo virtual vRealize Log Insight](#)
- [Iniciar una nueva implementación de vRealize Log Insight](#)
- [Unirse a una implementación existente](#)

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.

Requisitos previos

- 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.

Tamaño preestablecido	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
Mediano	75 GB por día	8	16 GB	1000	250	5000
Grande	225 GB por día	16	32 GB	1500	750	15.000

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 se expande 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 Seleccionar redes, configure los parámetros de redes para el dispositivo virtual vRealize Log Insight. Puede seleccionar el protocolo IPv4 o IPv6.

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.

Precaución 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.

En Aplicación, seleccione la casilla **Preferir direcciones IPv6** si desea ejecutar la máquina virtual en una red de pila dual.

Precaución No seleccione la casilla **Preferir direcciones IPv6** si desea usar IPv4 puro incluso con IPv6 admitido en la red. Seleccione la casilla solo si la red cuenta con una pila dual o una compatibilidad de pila pura para IPv6.

- 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 verifique 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://	<p>Error en la configuración de DHCP en el dispositivo virtual.</p> <ul style="list-style-type: none"> a Apague el dispositivo virtual vRealize Log Insight. b Haga clic con el botón derecho en el dispositivo virtual y seleccione Editar configuración. c Establezca una dirección IP estática para el dispositivo virtual.

Pasos siguientes

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

La interfaz web de vRealize Log Insight está disponible en <https://host-log-insight/>, donde *host-log-insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Iniciar una nueva implementación de vRealize Log Insight

Cuando accede a la interfaz web de vRealize Log Insight por primera vez tras implementar el dispositivo virtual o después de eliminar un nodo de trabajador de un clúster, debe completar los pasos de configuración inicial.

Todos los parámetros que modifique durante la configuración inicial también están disponibles en la interfaz de usuario web de Administración.

Para obtener información acerca de los datos de rastreo que vRealize Log Insight podría recopilar y enviar a VMware si participa en el Programa de mejora de la experiencia de cliente, consulte [Capítulo 4 Programa de mejora de la experiencia de cliente](#).

Requisitos previos

- En vSphere Client, observe la dirección IP del dispositivo virtual de vRealize Log Insight. Para obtener más información acerca de la ubicación de las direcciones IP, consulte [Implementar el dispositivo virtual vRealize Log Insight](#).
- Verifique que esté usando un explorador compatible. Consulte [Requisitos mínimos](#).
- Verifique que tenga una clave de licencia válida. Puede solicitar una clave de licencia permanente o de evaluación mediante su cuenta en My VMware™ en la página <https://my.vmware.com/>.

- Si desea usar credenciales locales, del servidor vCenter Server o de Active Directory para integrar vRealize Log Insight con vRealize Operations Manager, verifique que estos usuarios se importen en la interfaz de usuario personalizada de vRealize Operations Manager. Para obtener instrucciones sobre cómo configurar LDAP, vea la [documentación de vRealize Operations Manager](#).

Procedimiento

- 1 Utilice un explorador compatible para desplazarse hasta la interfaz de usuario web de vRealize Log Insight.

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

Se abre el asistente de configuración inicial.

- 2 Haga clic en **iniciar nueva implementación**.
- 3 Configure la contraseña para el usuario administrador y haga clic en **Guardar y continuar**.
Opcionalmente, puede proporcionar una dirección de correo electrónico para el usuario administrador.
- 4 Introduzca la clave de licencia, haga clic en **Agregar clave de licencia** y, a continuación, en **Guardar y continuar**.
- 5 En la página de configuración general, escriba la dirección de correo electrónico en la cual recibir las notificaciones del sistema de vRealize Log Insight.
- 6 Si utiliza enlaces web para enviar notificaciones a vRealize Operations Manager o a una aplicación de terceros, introduzca una lista de URL separada por espacios en el cuadro de texto **Enviar notificaciones del sistema de HTTP Post a**.
- 7 (opcional) Para salir del Programa de mejora de la experiencia de cliente, desmarque la opción **Participar en el Programa para la mejora de la experiencia del usuario de VMware**. Haga clic en **Guardar y continuar**.
- 8 En la página Configuración de hora, configure cómo se sincroniza la hora en el dispositivo virtual de vRealize Log Insight y haga clic en **Probar**.

Opción	Descripción
Servidor NTP (recomendado)	De manera predeterminada, se configura vRealize Log Insight para sincronizar la hora con los servidores NTP públicos. Si no es posible acceder a un servidor NTP externo debido a los ajustes del firewall, puede usar el servidor NTP interno de su organización. Utilice comas para separar los servidores NTP múltiples.
Host ESX/ESXi	Si no hay servidores NTP disponibles, puede sincronizar la hora con el host de ESXi donde implementó el dispositivo virtual de vRealize Log Insight.

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

- 10 (opcional) Para habilitar los correos electrónicos salientes de alertas y notificaciones del sistema, especifique las propiedades de un servidor SMTP.

Para verificar que la configuración del SMTP sea correcta, escriba una dirección de correo electrónico válida y haga clic en **Probar**. vRealize Log Insight envía un correo electrónico de prueba a la dirección que proporcionó.

- 11 (opcional) Para proporcionar un certificado SSL personalizado, cargue un archivo de certificado en el clúster en formato PEM. También puede ver los detalles del certificado existente.

El sistema agrega el certificado a los almacenes de confianza de todos los nodos del clúster y lo guarda para su uso posterior.

Para obtener información sobre los requisitos previos del certificado SSL personalizado, consulte [Instalar un certificado SSL personalizado](#).

- 12 Haga clic en **Guardar y continuar**.

Resultados

Después de que se reinicia el proceso de vRealize Log Insight, se abre la pestaña **Paneles** de vRealize Log Insight.

Pasos siguientes

- Desplácese hasta la pestaña **Administración**. Desde la página **Integración de vSphere**, configure vRealize Log Insight para que extraiga tareas, eventos y alertas de instancias de vCenter Server y configure hosts ESXi para enviar feeds de syslog a vRealize Log Insight.
- Asigne una licencia permanente a vRealize Log Insight. Consulte [Asignar una licencia permanente a Log Insight](#) en *Administrar vRealize Log Insight*.
- Configure el adaptador de vRealize Log Insight en vRealize Operations Manager para habilitar el inicio en contexto. Consulte *Configurar vRealize Log Insight con vRealize Operations Manager* en la *Guía de configuración de vRealize Operations Manager*.
- Instale el agente de Windows de vRealize Log Insight para recopilar eventos de los canales de eventos de Windows, de los directorios de Windows y de los archivos de registro de texto plano. Consulte [Instalar agentes de Windows](#) en *Trabajar con agentes de vRealize Log Insight*.

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 de clúster, vRealize Log Insight proporciona los nodos principal y de

trabajador. Los nodos principal y de trabajador son responsables de un subconjunto de datos. Los nodos principales pueden consultar todos los subconjuntos de datos y agregar los resultados. Es posible que necesite más nodos para satisfacer las necesidades del sitio. Puede utilizar de tres a 18 nodos en un clúster. Esto significa que un clúster completamente funcional debe tener un mínimo de tres nodos en buen estado. La mayoría de los nodos en un clúster de mayor tamaño deben estar en buen estado. Por ejemplo, si se produce un error en tres nodos de un clúster de seis nodos, ninguno de los nodos funcionará plenamente mientras no se eliminen los nodos erróneos.

Requisitos previos

- 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.

Pasos siguientes

- Agregue más nodos de trabajador según sea necesario. El clúster debe tener un mínimo de tres nodos.

Programa de mejora de la experiencia de cliente

4

Este producto participa en el Programa de mejora de la experiencia de cliente (CEIP) de VMware.

Los detalles sobre los datos recopilados a través del CEIP y los propósitos para los que VMware los utiliza se establecen en el centro de seguridad y confianza, disponible en <https://www.vmware.com/solutions/trustvmware/ceip.html>.

Para unirse al CEIP de este producto o abandonarlo, consulte la sección "Unirse al programa de la experiencia de cliente de VMware o abandonarlo" en *Administrar vRealize Log Insight*.