

Trabajar con agentes de 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

Trabajar con agentes de vRealize Log Insight	5
1 Descripción general de los agentes de vRealize Log Insight	6
2 Tipos de combinaciones de rotaciones de registros	8
3 Instalar o actualizar los agentes de vRealize Log Insight	9
Descargar los archivos de instalación del agente	10
Instalar agentes de Windows	11
Instalar o actualizar el agente de Windows de vRealize Log Insight con el asistente de instalación	11
Instalar o actualizar el agente de Windows de vRealize Log Insight desde la línea de comandos	12
Implementar Log Insight Windows Agent en varias máquinas	14
Instalar o actualizar el paquete de RPM del agente de Linux de vRealize Log Insight	19
Instalar o actualizar el paquete DEB del agente de Linux de vRealize Log Insight	20
Personalización de su agente de instalación para Linux Debian	21
Instalar el paquete binario de Log Insight Linux Agent	24
Opciones de línea de comandos para la instalación de agentes de vRealize Log Insight en Linux	26
Actualización automática para los agentes de vRealize Log Insight	27
Habilitar o deshabilitar la actualización automática para agentes individuales	27
4 Configurar agentes de vRealize Log Insight	29
Configurar Log Insight Windows Agent	30
Configuración predeterminada del Log Insight Windows Agent	30
Recopilar eventos de canales de eventos de Windows	33
Recopilar eventos de un archivo de registro	38
Reenviar eventos a Log Insight Windows Agent	43
Configurar Log Insight Linux Agent	43
Configuración predeterminada del agente de Linux de vRealize Log Insight	44
Recopilar eventos de un archivo de registro	46
Filtrado de eventos de agentes de vRealize Log Insight	54
Reenviar información desde un agente de vRealize Log Insight	56
Configurar el servidor vRealize Log Insight de destino	57
Especificar el destino de un agente	60
Configuración centralizada de agentes vRealize Log Insight	63
Un ejemplo de fusión de configuración	65
Uso de valores comunes para la configuración del agente	67

[Analizar registros](#) 68

[Configurar analizadores de registros](#) 69

5 Desinstalar agentes de vRealize Log Insight 100

[Desinstalar el Log Insight Windows Agent](#) 100

[Desinstalar el paquete RPM del agente de Linux de Log Insight](#) 100

[Desinstalar el paquete DEB del agente de Linux de Log Insight](#) 101

[Desinstalar el paquete bin del agente de Linux de Log Insight](#) 101

[Desinstalar manualmente el paquete bin del agente de Linux de Log Insight](#) 102

6 Solución de problemas de agentes de vRealize Log Insight 104

[Crear un paquete de soporte para el Log Insight Windows Agent](#) 104

[Crear un paquete de soporte para el Log Insight Linux Agent](#) 105

[Definir el nivel de detalles de registro en los Log Insight Agents](#) 105

[La UI de administración no muestra a Log Insight Agents](#) 106

[Los agentes de vRealize Log Insight no envían eventos](#) 107

[Añadir una regla de excepción saliente para Log Insight Windows Agent](#) 108

[Permitir conexiones salientes desde Log Insight Windows Agent en un firewall de Windows](#) 109

[Implementación masiva de Log Insight Windows Agent no finaliza correctamente](#) 110

[Los Log Insight Agents rechazan certificados autofirmados](#) 111

[El servidor de vRealize Log Insight rechaza la conexión para el tráfico no cifrado](#) 112

Trabajar con agentes de vRealize Log Insight

Trabajar con agentes de vRealize Log Insight describe el modo de instalar y configurar los agentes de Windows y Linux de vRealize™ Log Insight™. También incluye consejos para solucionar problemas.

Esta información está destinada a quienes desean instalar, configurar o solucionar los problemas de Log Insight Agents. Está redactada para administradores de sistemas Windows o Linux con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Para obtener información acerca del modo de crear clases de configuración para agentes con el servidor vRealize Log Insight, consulte *Administrar vRealize Log Insight*.

Descripción general de los agentes de vRealize Log Insight

1

Un agente de vRealize Log Insight recopila eventos de los archivos de registro y los reenvía a un servidor de vRealize Log Insight o a cualquier destino externo de syslog.

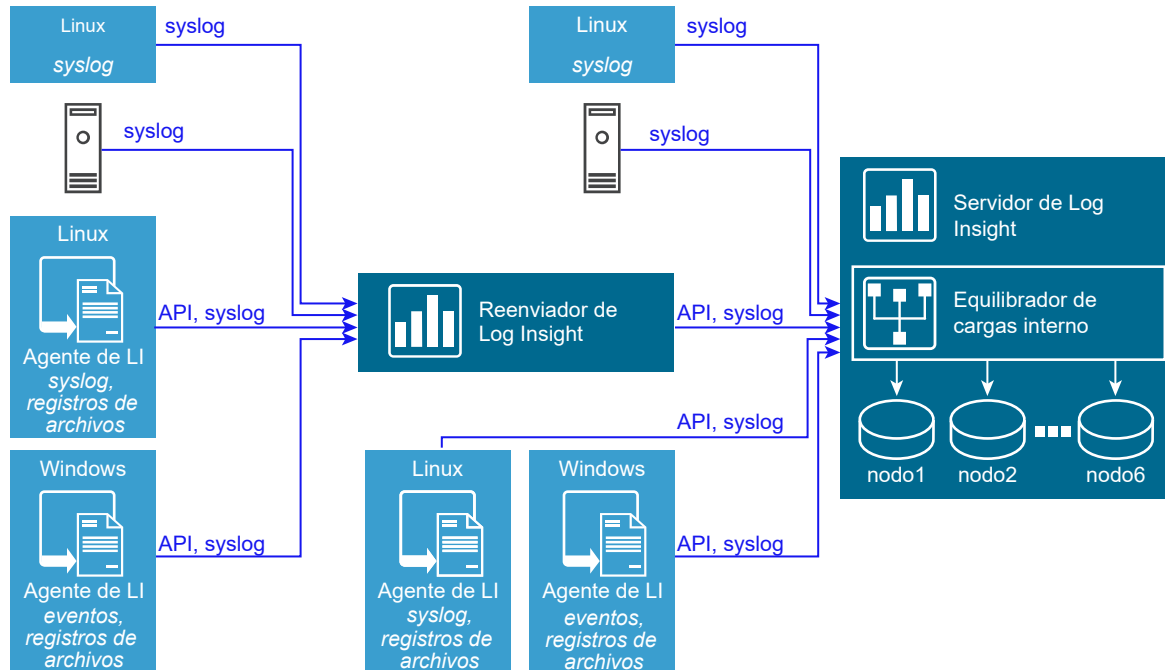
Los agentes admiten syslog y la API de consumo de vRealize Log Insight (protocolo cfapi) y se pueden utilizar con plataformas Linux o Windows. Configure los agentes mediante la interfaz web, con el archivo liagent.ini en el servidor y en el cliente, o bien como parte de la instalación.

Los agentes incluyen las siguientes funciones:

- Implementación única o en grupo
- Actualización automática.
- Análisis que funcionan en los mensajes de registro y extraen datos estructurados. Puede configurar analizadores para el recopilador FileLog o WinLog, o bien ambos.
- Soporte para mensajes con varias líneas
- Soporte nativo para varias combinaciones de rotación de registros
- Una API de consumo extendida que incluye compresión del cliente, cifrado y capacidad de agregar metadatos a eventos

El servidor de vRealize Log Insight admite una administración centralizada de la configuración y la creación y la administración de grupos de agentes.

La siguiente figura muestra los elementos de la configuración de una implementación de agente.



Un reenviador de vRealize Log Insight es una instancia dedicada de un servidor de vRealize Log Insight cuyo trabajo principal es enviar eventos a un destino remoto. Normalmente, las instancias de servidor usadas como reenviador no se usan para consultas. El reenviador usa un equilibrador de carga interno, pero se estructura como un servidor de vRealize Log Insight.

Los agentes escriben sus propios registros de las operaciones. En Windows, estos registros se encuentran en el directorio `C:\ProgramData\VMware\Log Insight Agent\logs`. En Linux, la ruta de acceso del registro de operaciones es `/var/log/loginsight-agent/liagent_*.log`. Los archivos de registro se rotan cuando un agente se reinicia o cuando el archivo alcanza 10 MB de tamaño. En la rotación se mantiene un límite combinado de 50 MB de archivos. No puede recopilar registros de agente con el agente de vRealize Log Insight.

Los agentes se usan para recopilar registros en tiempo real. Utilice vRealize Log Insight Importer para importar recopilaciones de registros históricos, incluidos paquetes de soporte técnico.

Se proporcionan descargas de instalación diferentes para Linux y Windows.

En sistemas Windows, el agente se ejecuta como un servicio Windows y se inicia inmediatamente tras la instalación. El agente supervisa los archivos de registro de aplicaciones y los canales de eventos de Windows, que recopilan grupos relacionados con eventos de sistema de Windows. Los eventos recopilados se reenvían a los servidores de vRealize Log Insight o a destinos de syslog de terceros.

En sistemas Linux, el agente se ejecuta como un daemon y se inicia inmediatamente tras la instalación. El agente de Linux de vRealize Log Insight recopila los eventos de los archivos de registro de equipos Linux y los reenvía al servidor de vRealize Log Insight o a destinos de syslog. Están disponibles los paquetes de instalación binarios de Linux, Red Hat y Debian.

Esquemas de rotación de registros admitidas por los agentes de vRealize Log Insight

2

Los agentes de vRealize Log Insight admiten varias combinaciones de rotaciones de registros.

La rotación de registros garantiza que los archivos de registro no aumenten de forma descontrolada. Existen varias combinaciones de rotación de registros, cada una diseñada para un conjunto particular de casos prácticos. vRealize Log Insight incluye soporte nativo para las siguientes combinaciones.

Tabla 2-1. Combinaciones de rotaciones de registros que admiten los agentes de vRealize Log Insight

Combinación de rotación de registros	Descripción
<code>create-new</code>	Se crean nuevos archivos de registro cuando se alcanza un límite de tiempo o de tamaño. El proceso del registrador deja de escribir en el archivo de registro actual y envía los resultados del registro a un archivo que se acaba de crear. Esto no afecta al resto de archivos ni les cambia el nombre.
<code>rename-recreate</code>	Una utilidad externa como <code>logrotate</code> cambia el nombre del archivo de registro cuando se alcanza un límite de tamaño o tiempo. El proceso del registrador crea entonces un archivo de registro con el nombre anterior.
<code>copy-truncate</code>	Una utilidad externa como <code>logrotate</code> copia el archivo de registro cuando se alcanza un límite de tamaño o tiempo. El proceso de registro cambia el nombre del archivo copiado y trunca el archivo original para que su tamaño pase a ser 0. El proceso del registrador puede seguir escribiendo registros en el archivo original.

Instalar o actualizar los agentes de vRealize Log Insight

3

Los agentes de vRealize Log Insight se instalan o se actualizan en equipos Windows o Linux, incluidos aquellos con sistemas externos de administración del registro.

Los agentes recopilan eventos y los reenvían al servidor de vRealize Log Insight. Durante la instalación, puede especificar los parámetros de la configuración del servidor, del puerto y del protocolo, o puede mantener la configuración predeterminada.

Puede actualizar los agentes con los mismos métodos que usa para la instalación, o bien puede utilizar la actualización automática. La actualización automática propaga la actualización a los agentes cuando implementa una nueva versión de vRealize Log Insight. Para obtener más información, consulte la sección [Actualización automática para los agentes de vRealize Log Insight](#). La actualización no está disponible para los paquetes binarios de Linux.

Compatibilidad de hardware

Para instalar y ejecutar un agente de vRealize Log Insight, el hardware debe admitir los parámetros mínimos necesarios para que los hosts y los equipos sean compatibles con arquitecturas x86 y x86_64, y con los conjuntos de instrucciones MMX, SSE, SSE2 y SSE3.

Compatibilidad con la plataforma

Sistema operativo	Arquitectura del procesador
Windows 7, Windows 8, Windows 8.1 y Windows 10	x86_64, x86_32
Windows Server 2008, Windows Server 2008 R2,	x86_64, x86_32
Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 y Windows Server 2019	x86_64
RHEL 5, RHEL 6, RHEL 7 y RHEL 8	x86_64, x86_32
SuSE Enterprise Linux (SLES) 11 SP3 y SLES 12 SP1	x86_64
Ubuntu 14.04 LTS, Ubuntu 16.04 LTS y Ubuntu 18.04	x86_64
VMware Photon, versión 1 revisión 2, versión 2 y versión 3	x86_64

Notas de Linux

Si implementa una instalación predeterminada del agente de Linux de Log Insight para un usuario sin privilegios de raíz, la configuración predeterminada puede presentar problemas con la recopilación de datos. El agente no registra advertencias para indicar que la suscripción al canal no ha sido correcta, y los archivos de la recopilación no tienen permisos de lectura. El mensaje `No se puede acceder al archivo de registro. Vuelva a intentarlo más tarde` se agrega al registro de forma repetitiva. Es posible comentar la configuración predeterminada que está causando el problema o modificar los permisos del usuario.

Si utiliza un paquete rpm o DEB para instalar los agentes de Linux, el script `init.d` denominado `liagentd` se instala como parte de la instalación del paquete. El paquete `bin` agrega el script, pero no lo registra. Puede registrar manualmente el script.

Para comprobar que la instalación se realizó correctamente, ejecute el comando (`/sbin/`) `service liagentd status`.

Este capítulo incluye los siguientes temas:

- [Descargar los archivos de instalación del agente](#)
- [Instalar agentes de Windows](#)
- [Instalar o actualizar el paquete de RPM del agente de Linux de vRealize Log Insight](#)
- [Instalar o actualizar el paquete DEB del agente de Linux de vRealize Log Insight](#)
- [Personalización de su agente de instalación para Linux Debian](#)
- [Instalar el paquete binario de Log Insight Linux Agent](#)
- [Opciones de línea de comandos para la instalación de agentes de vRealize Log Insight en Linux](#)
- [Actualización automática para los agentes de vRealize Log Insight](#)

Descargar los archivos de instalación del agente

El primer paso para configurar un agente de vRealize Log Insight es descargar el paquete de instalación del agente para la plataforma correspondiente.

Todos los paquetes descargados de la página del agente del servidor de vRealize Log Insight incluyen el nombre de host de destino anexo al nombre del paquete. El nombre de host del servidor se aplica durante una instalación inicial para los agentes MSI, RPM, y DEB. Si ya aparece un nombre de host en el archivo de configuración o si se está ejecutando el paquete mediante el parámetro del nombre de host, el nombre de host del servidor integrado se ignora.

Procedimiento

- 1 Desplácese hasta la pestaña **Administración** de la interfaz de usuario web de vRealize Log Insight.
- 2 En la sección Administración, haga clic en **Agentes**.

- 3 Desplácese hasta la parte inferior de la pantalla y haga clic en **Descargar agente de Log Insight**.
- 4 Descargue un paquete de instalación seleccionándolo en el menú emergente y haciendo clic en **Guardar**.

Opción	Descripción
Windows MSI	Paquete de instalación para una plataforma Windows (32 o 64 bits)
Linux RPM	Paquete de instalación para las siguientes plataformas: Linux Red Hat, openSUSE (32 bits o 64 bits) o VMware Photon Platform
Linux DEB	Paquete de instalación para una plataforma Linux Debian (32 o 64 bits)
Linux BIN	Paquete de instalación automática para Linux (32 o 64 bits). No es necesario un sistema de administración de paquetes.

Pasos siguientes

Use los archivos descargados para implementar el agente de vRealize Log Insight.

Instalar agentes de Windows

Puede instalar un agente en un equipo único utilizando un asistente de instalación o una línea de comandos, o bien puede implementar varias instancias de un agente utilizando un script.

Actualizar agentes de Windows

Puede actualizar un agente de Windows si aplica un archivo de actualización con uno de los métodos que puede usar para realizar la instalación. También puede usar la función de actualización automática para actualizar los agentes en segundo plano.

Instalar o actualizar el agente de Windows de vRealize Log Insight con el asistente de instalación

Puede instalar o actualizar un agente de Windows en un único equipo con el asistente de instalación.

Requisitos previos

- Verifique que tenga una copia del archivo `.msi` del agente de Windows de vRealize Log Insight. Consulte [Descargar los archivos de instalación del agente](#).
- Verifique que tenga los permisos para efectuar las instalaciones y los servicios de inicio en la máquina de Windows.

Procedimiento

- 1 Inicie sesión en la máquina de Windows en la que instalará el agente de Windows de vRealize Log Insight.

- 2 Cambie al directorio donde tiene el archivo `.msi` del agente de Windows de vRealize Log Insight.
- 3 Haga doble clic en el archivo `.msi` del agente de Windows de vRealize Log Insight, acepte los términos del contrato de licencia y haga clic en **Siguiente**.
- 4 Introduzca la dirección IP o el nombre de host del servidor de vRealize Log Insight y haga clic en **Instalar**.

El asistente instala o actualiza el agente de Windows de vRealize Log Insight como un servicio de Windows automático en la cuenta del servicio Sistema local.

- 5 Haga clic en **Finalizar**.

Pasos siguientes

Configure el agente de Windows de vRealize Log Insight editando el archivo `liagent.ini`. Consulte [Configurar Log Insight Windows Agent](#).

Instalar o actualizar el agente de Windows de vRealize Log Insight desde la línea de comandos

Puede instalar o actualizar el agente de Windows desde la línea de comandos.

Puede usar la cuenta de servicio predeterminada o especificar una, y usar los parámetros de la línea de comandos para especificar el servidor, el puerto y la información de protocolo. Para las opciones de línea de comandos de MSI, visite el sitio web de Microsoft Developer Network (MSDN) Library y busque las opciones de línea de comandos de MSI.

Requisitos previos

- Verifique que tenga una copia del archivo `.msi` del agente de Windows de vRealize Log Insight. Consulte [Descargar los archivos de instalación del agente](#).
- Verifique que tenga los permisos para efectuar las instalaciones y los servicios de inicio en la máquina de Windows.
- Si usa las opciones de instalación silenciosa `/quiet` o `/qn`, verifique que ejecute la instalación como administrador. Si no es administrador y ejecuta la instalación silenciosa, la instalación no le solicita privilegios de administrador y falla. Use la opción de registro y los parámetros `/l{xv* files_name}` para fines de diagnóstico.

Procedimiento

- 1 Inicie sesión en la máquina de Windows en la que instalará o actualizará el agente de Windows de vRealize Log Insight.
- 2 Abra una ventana **Solicitud de comandos**.
- 3 Cambie al directorio donde tiene el archivo `.msi` del agente de Windows de vRealize Log Insight.

- 4 Realice la instalación o actualice los valores predeterminados con un comando siguiendo este procedimiento. Reemplace *versión-número_compilación* por el número de compilación y la versión.

La opción `/quiet` ejecuta el comando de forma silenciosa y la opción `/lxv` crea un archivo de registro en el directorio actual.

```
Unidad:\ruta-a-archivo_msi>VMware-Log-Insight-Agent-versión-
número_compilación.msi /quiet /lxv* li_install.log
```

- 5 (opcional) Especifique una cuenta de servicio de usuario para ejecutar el servicio del agente de Windows de vRealize Log Insight.

```
Unidad:\ruta-a-archivo_msi>VMware-Log-Insight-Agent-*.msi
SERVICEACCOUNT=domain\usuario SERVICEPASSWORD=contraseña_de_usuario
```

Nota La cuenta suministrada en el parámetro `SERVICEACCOUNT` se otorga con el derecho **Iniciar sesión como servicio** y acceso de escritura completa al directorio `%ProgramData%\VMware\Log Insight Agent`. Si la cuenta proporcionada no existe, se crea. El nombre de usuario no debe tener más de 20 caracteres. Si no especifica un parámetro `SERVICEACCOUNT`, el servicio del agente de Windows de vRealize Log Insight se instala o actualiza en la cuenta de servicio `LocalSystem`.

- 6 (opcional) Puede especificar valores para las siguientes opciones de la línea de comandos según sea necesario.

Opción	Descripción
<code>SERVERHOST=nombredehost</code>	La dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight.
<code>SERVERPROTO=protocolo</code>	Protocolo que utiliza el agente para enviar eventos al servidor de vRealize Log Insight. Los valores posibles son <code>cfapi</code> y <code>syslog</code> . El valor predeterminado es <code>cfapi</code> .
<code>SERVERPORT=númerodepuerto</code>	Puerto de comunicación que utiliza el agente para enviar eventos al servidor externo vRealize Log Insight. De forma predeterminada, el agente utiliza el puerto adecuado basado en las opciones que están configuradas para SSL y el protocolo. Consulte los valores de puerto predeterminados proporcionados en la lista que se incluye a continuación. Debe especificar la opción del puerto solo si es diferente a los valores predeterminados. <ul style="list-style-type: none"> ■ <code>cfapi</code> con SSL habilitado: 9543 ■ <code>cfapi</code> con SSL deshabilitado: 9000 ■ <code>syslog</code> con SSL habilitado: 6514 ■ <code>syslog</code> con SSL deshabilitado: 514

Opción	Descripción
SERVICEACCOUNT= <i>nombre-cuenta</i>	La cuenta de servicio de usuario en la que se ejecuta el servicio de Log Insight Windows Agent. Nota La cuenta que se provee en el parámetro SERVICEACCOUNT debe tener el privilegio Iniciar sesión como Servicio y acceso de escritura al directorio %ProgramData%\VMware\Log Insight Agent para que el instalador se ejecute correctamente. Si no especifica un parámetro SERVICEACCOUNT, el servicio del agente de Windows de vRealize Log Insight se instala en la cuenta del servicio LocalSystem.
SERVICEPASSWORD= <i>contraseña</i>	Contraseña de la cuenta de servicio del usuario.
AUTOUPDATE={yes no}	Habilite o deshabilite la actualización automática del agente. También debe habilitar la actualización automática en el servidor de vRealize Log Insight para habilitar totalmente la actualización automática. El valor predeterminado es sí.
LIAGENT_SSL={yes no}	Habilite la conexión segura. Si SSL está habilitado, el agente utiliza el protocolo TLS 1.2 para comunicarse con el servidor. El valor predeterminado es sí.

Resultados

El comando instala o actualiza el agente de Windows de vRealize Log Insight como un servicio de Windows. El servicio del agente de Windows de vRealize Log Insight se inicia cuando enciende la máquina Windows.

Pasos siguientes

Verifique que los parámetros de línea de comandos que establece se aplican correctamente en el archivo `liagent.ini`. Consulte [Configurar Log Insight Windows Agent](#).

Implementar Log Insight Windows Agent en varias máquinas

Puede realizar una implementación masiva de Log Insight Windows Agent en los equipos de destino que se encuentren en un dominio de Windows.

Procedimiento

1 Crear un archivo de transformación para implementar varios agentes de Windows de vRealize Log Insight

Como parte de la implementación de varios agentes, debe crear un archivo de transformación que especifique los parámetros de configuración para la implementación. El archivo de transformación .mst se aplica al archivo .msi al instalar agentes. Entre los parámetros se incluyen el servidor de destino para los agentes y el protocolo de comunicación, el puerto y la cuenta de usuario para instalar e iniciar el servicio del agente de Log Insight.

2 Implementar varias instancias del agente de Windows de vRealize Log Insight

Es posible implementar varias instancias del agente de Windows de vRealize Log Insight en los equipos de destino en un dominio de Windows.

Crear un archivo de transformación para implementar varios agentes de Windows de vRealize Log Insight

Como parte de la implementación de varios agentes, debe crear un archivo de transformación que especifique los parámetros de configuración para la implementación. El archivo de transformación .mst se aplica al archivo .msi al instalar agentes. Entre los parámetros se incluyen el servidor de destino para los agentes y el protocolo de comunicación, el puerto y la cuenta de usuario para instalar e iniciar el servicio del agente de Log Insight.

Entre los parámetros se incluyen el servidor de destino para los agentes y el protocolo de comunicación, el puerto y la cuenta de usuario para instalar e iniciar el servicio del agente de Log Insight.

Requisitos previos

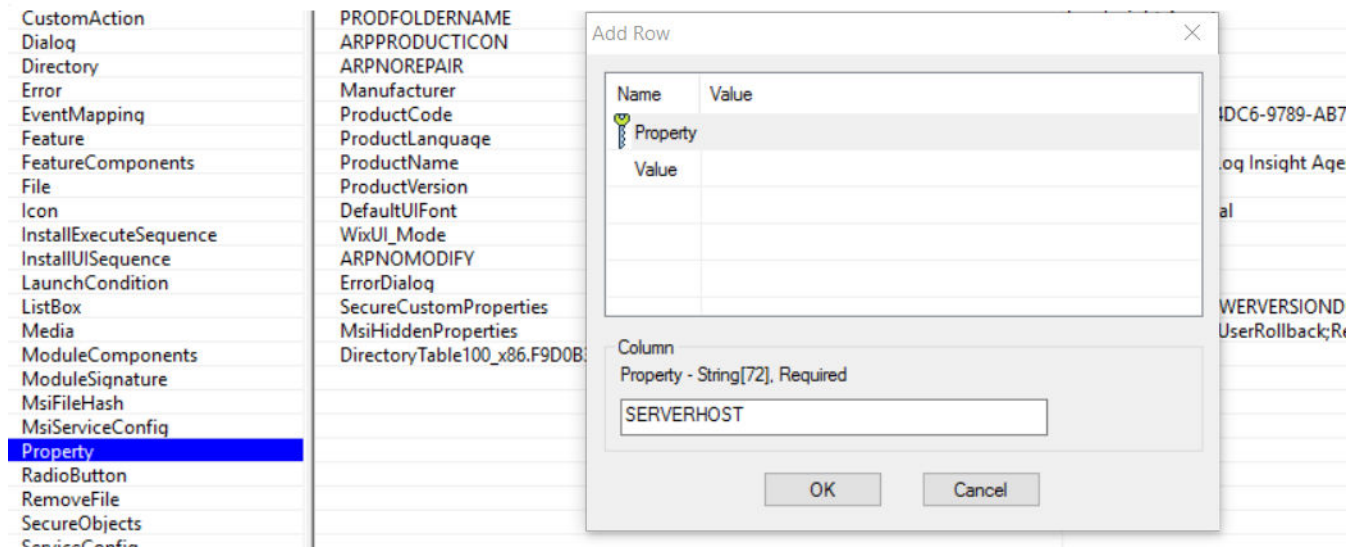
- Verifique que tenga una copia del archivo .msi del agente de Windows de vRealize Log Insight. Consulte [Descargar los archivos de instalación del agente](#).
- Descargue e instale el editor de base de datos Orca. Consulte <http://support.microsoft.com/kb/255905>.

Procedimiento

- 1 Abra el archivo .msi del agente de Windows de vRealize Log Insight en el editor Orca y seleccione **Transformar > Nueva transformación**.

- 2 Edite la tabla de Propiedades y añada los parámetros y valores necesarios para una instalación o actualización personalizada.

Figura 3-1. Tabla Propiedades



- a Haga clic en **Propiedades**.
- b En el menú desplegable **Tabla**, seleccione **Agregar fila**.
- c Introduzca un valor y un nombre para la propiedad en el cuadro de diálogo Agregar fila.

Los parámetros se muestran en la siguiente tabla.

Parámetro	Descripción
SERVERHOST	La dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight. El valor predeterminado es loginsight .
SERVERPROTO	Protocolo que utiliza el agente para enviar eventos al servidor de vRealize Log Insight. Los valores posibles son cfapi y syslog . El valor predeterminado es cfapi .
SERVERPORT	Puerto de comunicación que utiliza el agente para enviar eventos al servidor externo vRealize Log Insight. De forma predeterminada, el agente utiliza el puerto adecuado basado en las opciones que están configuradas para SSL y el protocolo. Consulte los valores de puerto predeterminados proporcionados en la lista que se incluye a continuación. Debe especificar la opción del puerto solo si es diferente a los valores predeterminados. <ul style="list-style-type: none"> ■ cfapi con SSL habilitado: 9543 ■ cfapi con SSL deshabilitado: 9000 ■ syslog con SSL habilitado: 6514 ■ syslog con SSL deshabilitado: 514

Parámetro	Descripción
SERVICEACCOUNT	La cuenta de servicio de usuario en la que se ejecuta el servicio de Log Insight Windows Agent. Nota La cuenta que se provee en el parámetro <code>SERVICEACCOUNT</code> debe tener el privilegio Iniciar sesión como Servicio y acceso de escritura al directorio <code>%ProgramData%\VMware\Log Insight Agent</code> para que el instalador se ejecute correctamente. Si no especifica un parámetro <code>SERVICEACCOUNT</code> , el servicio del agente de Windows de vRealize Log Insight se instala en la cuenta del servicio LocalSystem.
SERVICEPASSWORD	Contraseña de la cuenta de servicio del usuario.
AUTOUPDATE	Habilite o deshabilite la actualización automática del agente. También debe habilitar la actualización automática en el servidor de vRealize Log Insight para habilitar totalmente la actualización automática. El valor predeterminado es sí.
LIAGENT_SSL	Habilite la conexión segura. Si SSL está habilitado, el agente utiliza el protocolo TLS 1.2 para comunicarse con el servidor. El valor predeterminado es sí.

- 3 Seleccione **Transformar > Generar transformación** y guarde el archivo de transformación `.mst`.

Pasos siguientes

Use los archivos `.msi` y `.mst` para implementar el agente de Windows de vRealize Log Insight.

Implementar varias instancias del agente de Windows de vRealize Log Insight

Es posible implementar varias instancias del agente de Windows de vRealize Log Insight en los equipos de destino en un dominio de Windows.

Para obtener más información sobre por qué necesita reiniciar dos veces la máquina cliente, consulte <http://support.microsoft.com/kb/305293>.

Requisitos previos

- Verifique que tenga una cuenta de administrador o una cuenta con privilegios de administrador en la controladora de dominio.
- Verifique que tenga una copia del archivo `.msi` del agente de Windows de vRealize Log Insight. Consulte [Descargar los archivos de instalación del agente](#).
- Familiarícese con los procedimientos que se describen en <http://support.microsoft.com/kb/887405> y <http://support.microsoft.com/kb/816102>.

Procedimiento

- 1 Inicie sesión en la controladora de dominio como administrador o como usuario con privilegios de administrador.

- 2 Cree un punto de distribución y copie el archivo `.msi` del agente de Windows de vRealize Log Insight en el punto de distribución.
- 3 Abra la consola de administración de las directivas de grupo y cree un objeto de directiva de grupo para implementar el archivo `.msi` del agente de Windows de vRealize Log Insight.
- 4 Edite el objeto de la directiva de grupo para la implementación del software y asigne un paquete.
- 5 (opcional) Si generó un archivo `.mst` antes de la implementación, seleccione el archivo de configuración `.mst` en la pestaña **Modificaciones** de la ventana **Propiedades de GPO**. y utilice el método avanzado para editar un Objeto de directiva de grupo e implementar el paquete `.msi`.
- 6 (opcional) Actualice el agente de Windows de vRealize Log Insight.
 - a Copie el archivo `.msi` de actualización en el punto de distribución.
 - b Haga clic en la pestaña **Actualizar** en la ventana **Propiedades** del Objeto de directiva de grupo.
 - c Añada la versión instalada inicialmente del archivo `.msi` en los paquetes que este paquete actualizará la sección.
- 7 Implemente el agente de Windows de vRealize Log Insight en los grupos de seguridad específicos que incluyen los usuarios del dominio.
- 8 Cierre todas las ventanas del Editor de administración de directiva de grupo y de la Consola de administración de directivas de grupo en la controladora de dominio y reinicie las máquinas cliente.

Si se habilita la optimización de inicio de sesión rápido, reinicie dos veces las máquinas cliente.
- 9 Verifique que el agente de Windows de vRealize Log Insight esté instalado en los equipos cliente como servicio local.

Si configuró los parámetros de `SERVICEACCOUNT` y `SERVICEPASSWORD` para usar un archivo `.mst` para implementar varias instancias de agente de Windows de vRealize Log Insight, verifique que el agente de Windows de vRealize Log Insight esté instalado en los equipos cliente de la cuenta de usuario que especificó.

Pasos siguientes

Si las instancias múltiples del agente de Windows de vRealize Log Insight no se implementan correctamente, consulte la sección [Implementación masiva de Log Insight Windows Agent no finaliza correctamente](#).

Instalar o actualizar el paquete de RPM del agente de Linux de vRealize Log Insight

Puede instalar o actualizar el agente de Linux de vRealize Log Insight como usuario raíz o como usuario no raíz, y puede establecer los parámetros de la configuración durante la instalación. Después de la instalación, puede verificar la versión instalada.

Requisitos previos

- Consulte cuáles son los valores de instalación predeterminados y cómo cambiarlos en [Opciones de línea de comandos para la instalación de agentes de vRealize Log Insight en Linux](#).
- Inicie sesión como **raíz** o use `sudo` para ejecutar comandos de la consola.
- El agente de Linux de vRealize Log Insight debe tener acceso a syslog y a los servicios de administración de red para funcionar. Instale y ejecute el agente de Linux de vRealize Log Insight en los niveles de ejecución 3 y 5. Si quiere que el agente de Linux de vRealize Log Insight funcione bajo otros niveles de ejecución, configure el sistema en forma apropiada.

Procedimiento

- 1 Puede instalar o actualizar un agente desde la consola.

- Para instalar el agente de Linux de vRealize Log Insight con opciones de configuración predeterminadas, abra una consola y ejecute el siguiente comando.

```
rpm -i VMware-Log-Insight-Agent-<versión-y-número-de-compilación>.rpm
```

- Para actualizar el agente sin cambiar la configuración actual, abra una consola y ejecute el siguiente comando.

```
rpm -Uhv VMware-Log-Insight-Agent-<versión-y-número-de-compilación>.rpm
```

- 2 (opcional) Durante la actualización, es posible sobrescribir los valores de configuración predeterminados para la instalación o los valores de la configuración actual. Para ello, es necesario especificar las opciones como parte del comando de actualización o de instalación.

```
sudo <OPCIÓN=valor> rpm -i <versión-y-número-de-compilación>.rpm
```

- 3 (opcional) Ejecute el siguiente comando para verificar la versión instalada.

```
rpm -qa | grep Log-Insight-Agent
```

Ejemplo: Ejemplos de actualización y de instalación del agente de Linux

- El siguiente comando instala el agente de vRealize Log Insight para una distribución de Linux basada en RPM. Instala el agente en un servidor independiente, asigna un número de puerto que no es el predeterminado y crea un usuario para el agente de vRealize Log Insight.

```
sudo SERVERHOST=myagentserver SERVERPORT=1234 LIAGENTUSER=liagent rpm -i VMware-Log-Insight-Agent-44.1234.rpm
```

- El siguiente comando actualiza el agente con el archivo rpm determinado. La configuración del agente actual no se modifica.

```
rpm -Uvh VMware-Log-Insight-Agent-44.1234.rpm
```

Instalar o actualizar el paquete DEB del agente de Linux de vRealize Log Insight

Puede instalar o actualizar el paquete DEB (Debian) del agente de Linux de vRealize Log Insight desde la línea de comandos o mediante la base de datos debconf. Después de la instalación, puede verificar la versión instalada.

Requisitos previos

- Lea información sobre las opciones de instalación para modificarlos en [Opciones de línea de comandos para la instalación de agentes de vRealize Log Insight en Linux](#).
- Inicie sesión como **raíz** o use `sudo` para ejecutar comandos de la consola.
- Verifique que el agente de Linux de vRealize Log Insight tenga acceso a syslog y que funcionen los servicios de red. De forma predeterminada, el agente de Linux de vRealize Log Insight se ejecuta en los niveles de ejecución 2, 3, 4 y 5 y se detiene en los niveles de ejecución 0, 1 y 6.
- Para obtener más información y ejemplos, consulte [Personalización de su agente de instalación para Linux Debian](#).

Procedimiento

- 1 Para instalar o actualizar el agente de Linux de vRealize Log Insight abra una consola y ejecute el comando `dpkg -i nombre_paquete`.

El *nombre_paquete* está formado por el prefijo **vmware-log-insight-agent-** y el número de compilación de la versión de descarga.

La siguiente forma del comando instala el paquete con los valores predeterminados.

```
dpkg -i vmware-log-insight-agent-VERSION-BUILD_NUMBER_all.deb
```

2 (opcional) Ejecute el siguiente comando para verificar la versión instalada:

```
dpkg -l | grep -i vmware-log-insight-agent
```

Ejemplo

- Configure el protocolo de conexión en la línea de comandos.

Para sobrescribir el protocolo de conexión predeterminado, use la variable SERVERPROTO como aparece en el siguiente ejemplo:

```
sudo SERVERPROTO=syslog dpkg -i vmware-log-insight-agent-<versión-y-número-de-
compilación>_all.deb
```

Personalización de su agente de instalación para Linux Debian

Puede personalizar la instalación usando opciones de comando para reemplazar los valores actuales de instalación o configurando la base de datos debconf.

Personalización desde la línea de comandos

Para configurar la instalación desde la línea de comandos, use un comando de la siguiente forma:

```
sudo <OPCIÓN=valor> dpkg -i vmware-log-insight-agent-<versión-y-número-de-
compilación>_all.deb
```

Para obtener una lista completa de opciones, consulte [Opciones de línea de comandos para la instalación de agentes de vRealize Log Insight en Linux](#).

Los siguientes ejemplos muestran algunas configuraciones típicas ejecutadas desde la línea de comandos.

- Especifique un servidor vRealize Log Insight de destino.
- Para establecer el destino durante la instalación, ejecute el comando `sudo` y reemplace el nombre de host por la dirección IP o el nombre de host del servidor de vRealize Log Insight, como se muestra en este ejemplo:

```
sudo SERVERHOST=hostname dpkg -i vmware-log-insight-agent-<versión-y-número-de-
compilación>_all.deb
```

A menos que habilite la marca `--force-confold` durante la instalación, siempre que actualice a una versión más reciente, el sistema le pedirá que conserve o reemplace el archivo de configuración `liagent.ini`. Aparece el siguiente mensaje del sistema:

```
Configuration file `/var/lib/loginsight-agent/liagent.ini'
==> Modified (by you or by a script) since installation.
==> Package distributor has shipped an updated version.
What would you like to do about it ? Your options are:
  Y or I : install the package maintainer's version
  N or O : keep your currently-installed version
  D      : show the differences between the versions
  Z      : start a shell to examine the situation
The default action is to keep your current version.
*** liagent.ini (Y/I/N/O/D/Z) [default=N] ?
```

Para conservar la configuración existente, utilice `[default=N]` . Aún se aplican los parámetros adicionales que se enviaron desde la línea de comandos.

- Configure el protocolo de conexión.

Para sobrescribir el protocolo de conexión predeterminado, use la variable `SERVERPROTO` como aparece en el siguiente ejemplo:

```
sudo SERVERPROTO=syslog dpkg -i vmware-log-insight-agent-<versión-y-número-de-
compilación>_all.deb
```

- Configure el puerto de conexión.

Para anular el puerto de conexión predeterminado, proporcione un valor para la variable `SERVERPORT` en el instalador, como aparece en el siguiente ejemplo:

```
sudo SERVERPORT=1234 dpkg -i vmware-log-insight-agent-<versión-y-número-de-
compilación>_all.deb
```

- Ejecute el agente como usuario no-raíz.

Para ejecutar el agente de Linux de vRealize Log Insight como usuario **no-raíz**, ejecute el comando `sudo`.

```
sudo LIAGENTUSER=liagent dpkg -i vmware-log-insight-agent-<versión-número-de-
compilación>_all.deb
```

Si el usuario especificado no existe, el agente de Linux de vRealize Log Insight crea la cuenta de usuario durante la instalación. La cuenta creada no se elimina después de la desinstalación. Si instala el agente de Linux con el parámetro `LIAGENTUSER=usuario_no_raíz` e intenta actualizar con el parámetro `LIAGENTUSER=usuario_no_raíz2`, se produce un conflicto y aparecen advertencias, dado que el usuario `usuario_no_raíz2` no tiene los permisos del usuario `usuario_no_raíz`.

Opciones de personalización de paquete DEB para la base de datos debconf

El paquete DEB del agente también se puede configurar a través de la base de datos debconf. La siguiente tabla muestra las opciones debconf compatibles y las opciones del instalador DEB del agente de vRealize Log Insight correspondientes:

Opciones de línea de comandos	Opciones de Debconf	Descripción
<code>SERVERHOST=nombredehost</code>	<code>vmware-log-insight-agent/serverhost</code>	La dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight. El valor predeterminado es loginsight .
<code>SERVERPROTO={cfapi syslog}</code>	<code>vmware-log-insight-agent/serverproto</code>	Protocolo que utiliza el agente para enviar eventos al servidor de vRealize Log Insight. Los valores posibles son <code>cfapi</code> y <code>syslog</code> . El valor predeterminado es <code>cfapi</code> .
<code>SERVERPORT=númerodepuerto</code>	<code>vmware-log-insight-agent/serverport</code>	Puerto de comunicación que utiliza el agente para enviar eventos al servidor externo vRealize Log Insight. De forma predeterminada, el agente utiliza el puerto adecuado basado en las opciones que están configuradas para SSL y el protocolo. Consulte los valores de puerto predeterminados proporcionados en la lista que se incluye a continuación. Debe especificar la opción del puerto solo si es diferente a los valores predeterminados. <ul style="list-style-type: none"> ■ <code>cfapi</code> con SSL habilitado: 9543 ■ <code>cfapi</code> con SSL deshabilitado: 9000 ■ <code>syslog</code> con SSL habilitado: 6514 ■ <code>syslog</code> con SSL deshabilitado: 514
<code>LIAGENT_INITSYSTEM={init systemd}</code>	<code>log-insight-agent/init_system</code>	Durante el tiempo de instalación, el agente detecta automáticamente el tipo de sistema <code>init</code> para el equipo en el que se está instalando el agente. Para sobrescribir este comportamiento, especifique el valor del tipo de sistema con esta opción. Existen dos tipos de sistemas <code>init</code> compatibles: <code>init</code> y <code>systemd</code> .
<code>LIAGENT_AUTOUPDATE={yes no}</code>	<code>vmware-log-insight-agent/auto_update</code>	Habilite o deshabilite la actualización automática del agente. También debe habilitar la actualización automática en el servidor de vRealize Log Insight para habilitar totalmente la actualización automática. El valor predeterminado es sí . La actualización automática no es compatible para paquetes <code>.bin</code> de LINUX.
<code>LI_AGENT_RUNSERVICES</code>	<code>vmware-log-insight-agent/init_system</code>	Justo después de la instalación, los servicios <code>liagentd</code> (agente) y <code>liupdaterd</code> (actualizador) se inician de forma predeterminada. Para que no se inicien, establezca el parámetro debconf de <code>LIAGENT_RUNSERVICES</code> en no . El valor predeterminado es sí . Los únicos valores aceptados son yes y no ; 1 o 0 no son valores admitidos.

Opciones de línea de comandos	Opciones de Debconf	Descripción
<code>LIAGENT_SSL</code>	<code>vmware-log-insight-agent/ssl</code>	C
<code>LIAGENTUSER=nombre-cuenta-usuario</code>	<code>vmware-log-insight-agent/liagentuser</code>	<p>Especifica la cuenta en la que se ejecuta el agente. Si el usuario no existe, el instalador lo crea como un usuario normal. Si la cuenta de usuario especificada no existe, el agente de Linux de vRealize Log Insight la crea durante la instalación. La cuenta creada no se elimina después de la desinstalación.</p> <p>De forma predeterminada, el agente está instalado para ejecutarse como usuario raíz.</p> <p>Si instala el agente con el parámetro <code>LIAGENTUSER=usuario_no_raíz</code> e intenta actualizar con <code>LIAGENTUSER=usuario_no_raíz2</code>, se produce un conflicto. Aparecen advertencias porque el usuario <code>usuario_no_raíz2</code> no tiene los permisos del usuario <code>usuario_no_raíz</code>.</p> <p>El usuario creado no se elimina durante la desinstalación. Se puede eliminar manualmente. Este parámetro está indicado solo para el servicio de agente. El servicio de actualizador siempre se ejecuta como usuario raíz.</p>

Instalar el paquete binario de Log Insight Linux Agent

Instalar el paquete binario incluye cambiar el archivo `.bin` por un archivo ejecutable y luego instalar el agente.

La actualización del paquete `.bin` no se admite oficialmente. Si usó el paquete `.bin` para instalar un Log Insight Linux Agent existente, realice una copia de seguridad del archivo `liagent.ini` situado en el directorio `/var/lib/loginsight-agent` para conservar la configuración local. Después de tener una copia de seguridad, desinstale manualmente Log Insight Linux Agent. Consulte [Desinstalar manualmente el paquete bin del agente de Linux de Log Insight](#).

Si usa el paquete `.bin` para instalar agentes de Linux, el script `init.d` con el nombre `liagentd` se instala como parte de la instalación del paquete, pero el paquete no registra la secuencia de comandos. Puede registrar manualmente el script.

Puede verificar que la instalación se completó correctamente si ejecuta el comando `(/sbin/)service liagentd status`.

Requisitos previos

- Descargue y copie el paquete Log Insight Linux Agent `.bin` en la máquina Linux de destino.
- Verifique que Log Insight Linux Agent tenga acceso a syslog y que funcionen los servicios de red.

- Consulte información sobre los valores de configuración predeterminados y cómo cambiarlos en la instalación. Consulte [Opciones de línea de comandos para la instalación de agentes de vRealize Log Insight en Linux](#).

Procedimiento

- 1 Abra una consola y ejecute el comando `chmod` para cambiar el archivo `.bin` por un archivo ejecutable.

Reemplace *filename-version* por la versión adecuada.

```
chmod +x filename-version.bin
```

- 2 Desde un símbolo del sistema, ejecute el comando `./filename-version.bin` para instalar el agente.

Reemplace *filename-version* por la versión adecuada.

```
./filename-version.bin
```

- 3 (opcional) Para establecer el servidor de vRealize Log Insight de destino durante la instalación, ejecute el comando `sudo SERVERHOST=hostname ./filename-version.bin`.

Reemplace *hostname* por la dirección IP o el nombre de host del servidor de vRealize Log Insight.

```
sudo SERVERHOST=hostname ./filename-version.bin
```

- 4 (opcional) Para sobrescribir el protocolo de conexión predeterminado, use la variable `SERVERPROTO` como aparece en el siguiente ejemplo:

```
sudo SERVERPROTO=syslog ./filename-version.htm
```

- 5 (opcional) Para sobrescribir el puerto de conexión predeterminado, proporcione un valor para la variable `SERVERPORT` en el instalador, como aparece en el siguiente ejemplo:

```
sudo SERVERPORT=1234 ./filename-version.htm
```

- 6 (opcional) Para ejecutar Log Insight Linux Agent como un usuario **no-raíz**, ejecute el comando `sudo`.

```
sudo LIAGENTUSER=liagent ./filename-version.bin
```

Si el usuario especificado no existe, Log Insight Linux Agent crea la cuenta de usuario durante la instalación. La cuenta creada no se elimina después de la desinstalación. Si instala Log Insight Linux Agent con el parámetro `LIAGENTUSER=usuario_no_raíz` e intenta actualizar con `LIAGENTUSER=usuario_no_raíz2`, se produce un conflicto y aparecen advertencias dado que el usuario *usuario_no_raíz2* no tiene los permisos del usuario *usuario_no_raíz*.

Opciones de línea de comandos para la instalación de agentes de vRealize Log Insight en Linux

Cuando instale agentes de vRealize Log Insight desde la línea de comandos, puede incluir opciones para configurar la implementación durante la instalación. Estas opciones se corresponden con la configuración del archivo `liagent.ini`.

Puede utilizar las siguientes opciones durante la instalación para configurar agentes de vRealize Log Insight que se ejecutan en sistemas Linux.

Opción	Descripción
<code>SERVERHOST=<i>nombredehost</i></code>	La dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight. El valor predeterminado es <code>loginsight</code> .
<code>SERVERPROTO={<i>cfapi</i> <i>syslog</i>}</code>	Protocolo que utiliza el agente para enviar eventos al servidor de vRealize Log Insight. Los valores posibles son <code>cfapi</code> y <code>syslog</code> . El valor predeterminado es <code>cfapi</code> .
<code>SERVERPORT=<i>númerodepuerto</i></code>	Puerto de comunicación que utiliza el agente para enviar eventos al servidor externo vRealize Log Insight. De forma predeterminada, el agente utiliza el puerto adecuado basado en las opciones que están configuradas para SSL y el protocolo. Consulte los valores de puerto predeterminados proporcionados en la lista que se incluye a continuación. Debe especificar la opción del puerto solo si es diferente a los valores predeterminados. <ul style="list-style-type: none"> ■ <code>cfapi</code> con SSL habilitado: 9543 ■ <code>cfapi</code> con SSL deshabilitado: 9000 ■ <code>syslog</code> con SSL habilitado: 6514 ■ <code>syslog</code> con SSL deshabilitado: 514
<code>LIAGENT_INITSYSTEM={<i>init</i> <i>systemd</i>}</code>	Durante el tiempo de instalación, el agente detecta automáticamente el tipo de sistema <code>init</code> para el equipo en el que se está instalando el agente. Para sobrescribir este comportamiento, especifique el valor del tipo de sistema con esta opción. Existen dos tipos de sistemas <code>init</code> compatibles: <code>init</code> y <code>systemd</code> .
<code>LIAGENT_AUTOUPDATE={<i>yes</i> <i>no</i>}</code>	Habilite o deshabilite la actualización automática del agente. También debe habilitar la actualización automática en el servidor de vRealize Log Insight para habilitar totalmente la actualización automática. El valor predeterminado es <code>sí</code> . La actualización automática no es compatible para paquetes <code>.bin</code> de LINUX.

Opción	Descripción
<code>LIAGENT_SSL={yes no}</code>	Habilite la conexión segura. Si SSL está habilitado, el agente utiliza el protocolo TLS 1.2 para comunicarse con el servidor. El valor predeterminado es sí.
<code>LIAGENTUSER=nombre-cuenta-usuario</code>	<p>Especifica la cuenta en la que se ejecuta el agente. Si el usuario no existe, el instalador lo crea como un usuario normal. Si la cuenta de usuario especificada no existe, el agente de Linux de vRealize Log Insight la crea durante la instalación. La cuenta creada no se elimina después de la desinstalación.</p> <p>De forma predeterminada, el agente está instalado para ejecutarse como usuario raíz.</p> <p>Si lleva a cabo la instalación con el parámetro <code>LIAGENTUSER=usuario_no_raíz</code> e intenta actualizar con <code>LIAGENTUSER=usuario_no_raíz2</code>, se producirá un conflicto. Aparecen advertencias porque el usuario <code>usuario_no_raíz2</code> no tiene los permisos del usuario <code>usuario_no_raíz</code>.</p> <p>El usuario creado no se elimina durante la desinstalación. Se puede eliminar manualmente. Este parámetro está indicado solo para el servicio de agente. El servicio de actualizador siempre se ejecuta como usuario raíz.</p>

Actualización automática para los agentes de vRealize Log Insight

La función de actualización automática para los agentes de vRealize Log Insight permite a los agentes activos comprobar, descargar y actualizar automáticamente paquetes de instalación basados en el agente desde el servidor de vRealize Log Insight.

Puede habilitar la actualización automática desde el servidor para todos los agentes, o bien desde los clientes para instancias de agentes individuales. Los agentes deben tener un estado activo y la versión 4.3 o una versión posterior.

La actualización automática no es compatible para paquetes .bin de LINUX.

Habilitar o deshabilitar la actualización automática para agentes individuales

Puede habilitar o deshabilitar la actualización automática para los agentes individuales editando el archivo de configuración del lado cliente para dicho agente.

De forma predeterminada, la actualización automática está habilitada en el lado cliente para un agente.

Requisitos previos

Los agentes deben tener la versión 4.3 o una versión posterior.

Procedimiento

- 1 Abra el archivo `liagent.ini` local en un editor.
- 2 Encuentre la sección `[update]`.

Es similar al siguiente ejemplo.

```
[update]
; Do not change this parameter
package_type=msi
; Enable automatic update of the agent. If enabled:
; the agent will silently check for updates from the server and
; if available will automatically download and apply the update.
; auto_update=yes
```

- 3 Para deshabilitar la actualización automática, anule el comentario de `auto_update=yes` y cámbielo a `auto_update=no`.

Nota La actualización automática de los agentes está habilitada de forma predeterminada. Por lo tanto, el valor predeterminado para `auto_update` es "yes", incluso cuando está comentado.

- 4 Guarde y cierre el archivo `liagent.ini`.

Configurar agentes de vRealize Log Insight

4

Después de haber implementado un agente, puede configurarlo para enviar eventos al servidor de vRealize Log Insight que seleccione, especificar protocolos de comunicación y configurar otros parámetros.

Use estas instrucciones cuando sea necesario para configurar sus agentes de acuerdo a sus necesidades.

- **Configurar Log Insight Windows Agent**

Puede configurar el Log Insight Windows Agent después de instalarlo. Edite el archivo `liagent.ini` para configurar el Log Insight Windows Agent a fin de que envíe eventos a vRealize Log Insight, establezca el protocolo y el puerto de comunicaciones, agregue canales de eventos de Windows y configure la recopilación de registros de archivos planos. El archivo se encuentra en el directorio `%ProgramData%\VMware\Log Insight Agent`.

- **Configurar Log Insight Linux Agent**

Puede configurar Log Insight Linux Agent después de instalarlo.

- **Filtrado de eventos de agentes de vRealize Log Insight**

Puede proporcionar la información que envía un agente a un destino con la opción de filtro en la sección `[server|<dest_id>]` del archivo `liagent.ini` local.

- **Reenviar información desde un agente de vRealize Log Insight**

Puede reenviar los eventos recopilados por un agente a un máximo de tres destinos. Un destino puede incluir un reenviador o servidores de vRealize Log Insight, o bien soluciones de gestión de registros de terceros.

- **Configuración centralizada de agentes vRealize Log Insight**

Puede configurar varios agentes vRealize Log Insight.

- **Uso de valores comunes para la configuración del agente**

Puede reemplazar los valores predeterminados del archivo de configuración del agente por valores de parámetros comunes que se aplican a la sección de configuración de cada agente para los agentes de Linux o de Windows.

■ Analizar registros

Los analizadores de registros del agente extraen datos estructurados de registros sin procesar antes de enviarlos al servidor de vRealize Log Insight. Con los analizadores de registros, vRealize Log Insight puede analizar registros, extraer información de ellos y mostrar esos resultados en el servidor. Los analizadores de registros pueden configurarse para agentes de Windows y Linux de vRealize Log Insight.

Configurar Log Insight Windows Agent

Puede configurar el Log Insight Windows Agent después de instalarlo. Edite el archivo `liagent.ini` para configurar el Log Insight Windows Agent a fin de que envíe eventos a vRealize Log Insight, establezca el protocolo y el puerto de comunicaciones, agregue canales de eventos de Windows y configure la recopilación de registros de archivos planos. El archivo se encuentra en el directorio `%ProgramData%\VMware\Log Insight Agent`.

Configuración predeterminada del Log Insight Windows Agent

Después de la instalación, el archivo `liagent.ini` contiene la configuración predeterminada configurada previamente para Log Insight Windows Agent.

Configuración predeterminada `liagent.ini` del Log Insight Windows Agent

Si usa nombres y valores que no son ASCII, guarde la configuración como UTF-8.

Si utiliza la configuración central, la configuración final es este archivo junto con ajustes del servidor para generar el archivo `liagent-effective.ini`.

Posiblemente le resulte más eficiente configurar los parámetros desde la página de agentes del servidor.

```
; Client-side configuration of VMware Log Insight Agent.
; See liagent-effective.ini for the actual configuration used by VMware Log Insight Agent.

[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
;hostname=LOGINSIGHT

;Enables or disables centralized configuration from the vRealize Log Insight server.
;When enabled, agent configuration changes made to the liagent.ini file on the server
;are joined with the settings in this file. to this agent. Accepted values are yes or no and
0 or 1.
;The default is yes.
;
;central_config=yes
;

; Set protocol to use:
; cfapi - Log Insight REST API
; syslog - Syslog protocol
; If omitted the default value is cfapi
```

```

;
;proto=cfapi

; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 514
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
;port=9000

;ssl - enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
;ssl=no

; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30

[storage]
;max_disk_buffer - max disk usage limit (data + logs) in MB:
; 100 - 2000 MB, default 200
;max_disk_buffer=200

[logging]
;debug_level - the level of debug messages to enable:
; 0 - no debug messages
; 1 - trace essential debug messages
; 2 - verbose debug messages (will have negative impact on performance)
;debug_level=0
;
;The interval in minutes to print statistics
;stats_period=15

[update]
; Do not change this parameter
package_type=msi

; Enable automatic update of the agent. If enabled:
; the agent will silently check for updates from the server and
; if available will automatically download and apply the update.
;auto_update=yes

[winlog|Application]
channel=Application
raw_syslog=no

[winlog|Security]
channel=Security

[winlog|System]
channel=System

```

Parámetro	Valor predeterminado	Descripción
hostname	LOGINSIGHT	La dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight. El valor predeterminado es loginsight .
central_config	yes	Habilite o deshabilite la configuración centralizada para este agente. Cuando la configuración centralizada esté deshabilitada, el agente ignora la configuración del servidor vRealize Log Insight. Los valores aceptados son <i>yes</i> , <i>no</i> , <i>1</i> o <i>0</i> . El valor predeterminado es <i>yes</i> .
proto	cfapi	Protocolo que utiliza el agente para enviar eventos al servidor de vRealize Log Insight. Los valores posibles son <i>cfapi</i> y <i>syslog</i> . El valor predeterminado es <i>cfapi</i> .
port	9543, 9000, 6514 y 514	Puerto de comunicación que utiliza el agente para enviar eventos al servidor externo vRealize Log Insight. De forma predeterminada, el agente utiliza el puerto adecuado basado en las opciones que están configuradas para SSL y el protocolo. Consulte los valores de puerto predeterminados proporcionados en la lista que se incluye a continuación. Debe especificar la opción del puerto solo si es diferente a los valores predeterminados. <ul style="list-style-type: none">■ cfapi con SSL habilitado: 9543■ cfapi con SSL deshabilitado: 9000■ syslog con SSL habilitado: 6514■ syslog con SSL deshabilitado: 514
ssl	yes	Habilita o deshabilita SSL. El valor predeterminado es <i>sí</i> . Si <i>ssl</i> se establece como <i>sí</i> , en el caso de no configurar un valor para el puerto, se selecciona automáticamente el puerto 9543.
max_disk_buffer	200	El espacio máximo en disco en MB que utiliza Log Insight Windows Agent para regular eventos y sus propios registros. Cuando se alcanza el <i>max_disk_buffer</i> especificado, el agente comienza a descartar los eventos entrantes nuevos.

Parámetro	Valor predeterminado	Descripción
debug_level	0	Define el nivel de detalles de registro. Consulte Definir el nivel de detalles de registro en los Log Insight Agents .
channel	Aplicación, Seguridad, Sistema	Los canales de registro de eventos de Windows Aplicación, Seguridad y Sistema se comentan de modo predeterminado; el Log Insight Windows Agent no recopila registros de estos canales. Consulte Recopilar eventos de canales de eventos de Windows .
raw_syslog	no	Para los agentes que utilizan el protocolo syslog, permite al agente recopilar y enviar eventos syslog sin formato. El valor predeterminado es No, lo que significa que los eventos recopilados se transforman con los atributos de syslog especificados por el usuario. Habilite esta opción para recopilar eventos sin transformaciones syslog. Los valores que se aceptan son sí o 1, y no o 0.

Recopilar eventos de canales de eventos de Windows

Puede añadir un canal de eventos de Windows a la configuración de Log Insight Windows Agent. El Log Insight Windows Agent recopilará los eventos y los enviará al servidor vRealize Log Insight.

Los nombres de campos están restringidos. Los siguientes nombres están reservados y no se pueden utilizar como nombres de campo.

- event_type
- hostname
- source
- text

Requisitos previos

Inicie sesión en el equipo Windows donde instaló el agente de Windows de vRealize Log Insight e inicie el administrador de servicios para verificar que el servicio del agente de vRealize Log Insight esté instalado.

Procedimiento

- 1 Desplácese hasta el directorio de datos del programa del agente de Windows de vRealize Log Insight.

```
%ProgramData%\VMware\Log Insight Agent
```

- 2 Abra el archivo `liagent.ini` en cualquier editor de texto.
- 3 Añada los siguientes parámetros y configure los valores para su entorno.

Parámetro	Descripción
<code>[winlog section_name]</code>	Un nombre único para la sección de configuración.
<code>channel</code>	El nombre completo del canal de eventos como aparece en la aplicación de Windows incorporada del Visor de eventos. Para copiar el nombre de canal correcto, haga clic con el botón derecho en un canal del Visor de eventos, seleccione Propiedades y copie los contenidos del campo Nombre completo .
<code>enabled</code>	Un parámetro opcional para habilitar o deshabilitar la sección de configuración. Los valores posibles son sí o no (distingue mayúsculas de minúsculas). El valor predeterminado es sí.
<code>tags</code>	<p>El parámetro opcional para añadir etiquetas personalizadas a los campos de eventos recopilados. Defina las etiquetas usando la anotación JSON. Los nombres de etiquetas pueden incluir letras, números y guiones bajos. Un nombre de etiqueta solo puede comenzar con una letra o un guion bajo y no puede tener más de 64 caracteres. Los nombres de las etiquetas no distinguen entre mayúsculas y minúsculas. Por ejemplo, si utiliza las etiquetas={"etiqueta_nombre1" : "etiqueta valor 1", "Etiqueta_Nombre1" : "etiqueta valor 2" }, Etiqueta_Nombre1 se ignora, por tratarse de una instancia duplicada. No es posible utilizar evento_tipo y la marca de tiempo como nombres de etiqueta. Los duplicados dentro de la misma declaración se ignoran.</p> <p>Si el destino es un servidor syslog, las etiquetas pueden anular el campo APP-NAME. Por ejemplo, etiquetas={"appname":"VROPS"}.</p>
<code>whitelist, blacklist</code>	<p>Los parámetros opcionales para incluir o excluir de manera explícita los eventos de registro.</p> <p>Nota La opción <code>blacklist</code> sirve únicamente para campos; no se puede usar para bloquear texto.</p>
<code>exclude_fields</code>	(Opcional) Un parámetro para excluir de la recopilación a los campos individuales. Puede proporcionar múltiples valores como una lista separada por punto y coma. Por ejemplo, <code>exclude_fields=EventId; ProviderName</code>

```
[winlog|section_name]
channel=event_channel_name
enabled=yes_or_no
tags={"tag_name1" : "Tag value 1", "tag_name2" : "tag value 2" }
```

- 4 Guarde y cierre el archivo `liagent.ini`.

Ejemplo: Configuraciones

Vea los siguientes ejemplos de configuración [winlog].

```
[winlog|Events_Firewall ]
channel=Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
enabled=no
```

```
[winlog|custom]
channel=Custom
tags={"ChannelDescription": "Events testing channel"}
```

Configurar filtros para los canales de eventos de Windows

Puede configurar filtros para los canales de eventos de Windows para incluir o excluir explícitamente los eventos de registro.

Puede usar los parámetros `whitelist` y `blacklist` para evaluar una expresión de filtro. La expresión del filtro es una expresión booleana que consta de operadores y campos de eventos.

Nota La opción `blacklist` sirve únicamente para campos; no se puede usar para bloquear texto.

- El parámetro `whitelist` recopila solo los eventos de registro para los cuales la expresión del filtro evalúa como distinta a cero. Si omite este parámetro, el valor se implica en 1.
- El parámetro `blacklist` excluye los eventos de registro para los cuales la expresión del filtro evalúa como distinta a cero. El valor predeterminado es 0.

Para obtener una lista completa de los operadores y campos de eventos Windows, consulte [Campos de eventos y operadores](#).

Requisitos previos

Inicie sesión en el equipo Windows donde instaló el agente de Windows de vRealize Log Insight e inicie el administrador de servicios para verificar que el servicio del agente de vRealize Log Insight esté instalado.

Procedimiento

- 1 Desplácese hasta el directorio de datos del programa del agente de Windows de vRealize Log Insight.

```
%ProgramData%\VMware\Log Insight Agent
```

- 2 Abra el archivo `liagent.ini` en cualquier editor de texto.

3 Añada un parámetro `whitelist` o `blacklist` en la sección `[winlog|]`.

Por ejemplo

```
[winlog|nombre_exclusivo_sección]
channel = nombre_canal_evento
blacklist = expresión_filtro
```

4 Cree una expresión de filtro a partir de operadores y campos de eventos Windows.

Por ejemplo

```
whitelist = level > WINLOG_LEVEL_SUCCESS and level < WINLOG_LEVEL_INFO
```

5 Guarde y cierre el archivo `liagent.ini`.

Ejemplo: Configuraciones del filtro

Puede configurar el agente para, por ejemplo, recopilar solo eventos de error

```
[winlog|Security-Error]
channel = Security
whitelist = Level == WINLOG_LEVEL_CRITICAL or Level == WINLOG_LEVEL_ERROR
```

Puede configurar el agente para, por ejemplo, recopilar solo eventos de la red VMware del canal Aplicación

```
[winlog|VMwareNetwork]
channel = Application
whitelist = ProviderName == "VMnetAdapter" or ProviderName == "VMnetBridge" or ProviderName == "VMnetDHCP"
```

Puede configurar el agente para, por ejemplo, recopilar todos los eventos del canal Seguridad excepto los eventos particulares

```
[winlog|Security-Verbose]
channel = Security
blacklist = EventID == 4688 or EventID == 5447
```

Campos de eventos y operadores

Use los campos de eventos y operadores de Windows para crear expresiones de filtro.

Operadores de expresión de filtro

Operador	Descripción
<code>==</code> , <code>!=</code>	igual y no igual. Usar con campos numéricos y de cadenas.
<code>>=</code> , <code>></code> , <code><</code> , <code><=</code>	mayor o igual, mayor que, menor que, menor o igual. Usar con campos numéricos solamente.
<code>&</code> , <code> </code> , <code>^</code> , <code>~</code>	AND, OR, XOR bit a bit y operadores de complementos. Usar con campos numéricos solamente.
<code>and</code> , <code>or</code>	AND y OR lógicos. Usar para crear expresiones complejas mediante la combinación de expresiones simples.

Operador	Descripción
not	Operador NOT lógico unario. Usar para revertir el valor de una expresión.
()	Usar paréntesis en una expresión lógica para cambiar el orden de evaluación.

Campos de eventos de Windows

Puede usar los siguientes campos de eventos de Windows en una expresión de filtro.

Nombre de campo	Tipo de campo
Nombre de host	cadena
Texto	cadena
ProviderName	cadena
EventSourceName	cadena
EventID	numérico
EventRecordID	numérico
Canal	cadena
UserID	cadena
Nivel	numérico Puede usar las siguientes constantes predefinidas <ul style="list-style-type: none"> ■ WINLOG_LEVEL_SUCCESS = 0 ■ WINLOG_LEVEL_CRITICAL = 1 ■ WINLOG_LEVEL_ERROR = 2 ■ WINLOG_LEVEL_WARNING = 3 ■ WINLOG_LEVEL_INFO = 4 ■ WINLOG_LEVEL_VERBOSE = 5
Tarea	numérico
OpCode	numérico
Palabras clave	numérico Puede usar las siguientes máscaras de bit predefinidas <ul style="list-style-type: none"> ■ WINLOG_KEYWORD_RESPONSETIME = 0x0001000000000000; ■ WINLOG_KEYWORD_WDICONTEXT = 0x0002000000000000; ■ WINLOG_KEYWORD_WDIDIAGNOSTIC = 0x0004000000000000; ■ WINLOG_KEYWORD_SQM = 0x0008000000000000; ■ WINLOG_KEYWORD_AUDITFAILURE = 0x0010000000000000; ■ WINLOG_KEYWORD_AUDITSUCCESS = 0x0020000000000000; ■ WINLOG_KEYWORD_CORRELATIONHINT = 0x0040000000000000; ■ WINLOG_KEYWORD_CLASSIC = 0x0080000000000000;

Ejemplos

Recopilar todos los eventos críticos, de error y advertencia

```
[winlog|app]
channel = Application
whitelist = level > WINLOG_LEVEL_SUCCESS and level < WINLOG_LEVEL_INFO
```

Recopilar solo eventos Auditar falla del canal de seguridad

```
[winlog|security]
channel = Security
whitelist = Keywords & WINLOG_KEYWORD_AUDITFAILURE
```

Recopilar eventos de un archivo de registro

Puede configurar el agente de Windows de vRealize Log Insight para que recopile eventos desde uno o más archivos de registro.

Los nombres de campos están restringidos. Los siguientes nombres están reservados y no se pueden utilizar como nombres de campo.

- event_type
- hostname
- source
- text

Puede tener un máximo de tres destinos para la información del agente y filtrar la información antes de enviarla. Consulte [Reenviar información desde un agente de vRealize Log Insight](#).

Nota

- Supervisar un gran número de archivos, como mil o más, da lugar a un mayor uso de recursos por parte del agente y tiene un impacto sobre el rendimiento general de la máquina host. Para evitar esto, configure el agente para supervisar solo los archivos necesarios con patrones y globs, o archive los archivos de registro anteriores. Si la supervisión de un gran número de archivos es un requisito, considere la posibilidad de aumentar los parámetros de host, como la CPU y la memoria RAM.
 - El agente puede realizar recopilaciones desde una directorios cifrados, pero solo si lo ejecuta el usuario que cifró el directorio.
 - El agente solo admite estructuras de directorio estáticas. Si se cambió el nombre de los directorios o se agregaron, debe reiniciar el agente para comenzar a supervisar estos directorios, siempre que la configuración abarque los directorios.
-

Requisitos previos

Inicie sesión en el equipo Windows donde instaló el agente de Windows de vRealize Log Insight e inicie el administrador de servicios para verificar que el servicio del agente de vRealize Log Insight esté instalado.

Procedimiento

- 1 Desplácese hasta el directorio de datos del programa del agente de Windows de vRealize Log Insight.

```
%ProgramData%\VMware\Log Insight Agent
```

- 2 Abra el archivo `liagent.ini` en cualquier editor de texto.
- 3 Busque la sección `[servidor|<id_de_dest>]` del archivo. Añada los parámetros de configuración y fije los valores para su entorno.

```
[filelog|nombre_sección]
directory=ruta_acceso_a_directorio_registro
include=patrón_glob
...
```

Parámetro	Descripción
<code>[filelog section_name]</code>	Un nombre único para la sección de configuración.
<code>directory=full-path-to-log-file</code>	<p>La ruta de acceso completa al directorio del archivo de registro. Se admiten los patrones glob. Configuraciones de ejemplo:</p> <ul style="list-style-type: none"> ■ Para recopilar de todos los subdirectorios del directorio <code>D:\Logs\new_test_logs</code>, utilice <code>directory=D:\Logs\new_test_logs*</code> ■ Si sus subdirectorios tienen sus propios subdirectorios, utilice la siguiente configuración para supervisar todos los subdirectorios <code>directory=D:\Logs\new_test_logs**</code> <p>Nota Para limitar el número de archivos y directorios, y evitar un alto consumo de recursos, no puede definir un patrón glob de directorio para los directorios de primer o segundo nivel, como: <code>directory=c:/tmp/*</code> o <code>directory=c:\Logs*</code>. La ruta del directorio debe tener al menos dos niveles.</p> <p>Si define una ruta de acceso a un directorio que aún no existe, el agente recopilará los archivos de registro de ese directorio una vez que se cree el directorio y los archivos.</p> <p>Puede definir el mismo directorio en una o más secciones de configuración diferentes para reunir los registros varias veces desde el mismo archivo. Este proceso hace que sea posible aplicar distintas etiquetas y filtros al mismo origen de eventos.</p> <p>Nota Si utiliza configuraciones idénticas para estas secciones, los eventos duplicados se muestran del lado del servidor.</p>

Parámetro	Descripción
<code>include=file_name; ...</code>	<p>(Opcional) El nombre de un archivo o una máscara de archivo (patrón glob) desde el cual reunir los datos. Puede proporcionar los valores en una lista de valores separados con punto y coma. El valor predeterminado es <code>*</code>, lo cual significa que se incluyen todos los archivos. El parámetro distingue entre mayúsculas y minúsculas.</p> <p>Se puede utilizar una máscara de archivo (patrón global) con los archivos de grupo que sigan la misma convención de nomenclatura, así como con los que usen el mismo nombre de archivo. Por ejemplo, los nombres de archivo que incluyen espacios, como <code>vRealize Ops Analytics.log</code> y <code>vRealize Ops Collector.log</code>, se pueden escribir como <code>vRealize?Ops?Analytics*.log</code> o <code>vRealize*.log</code>. Las máscaras de archivo permiten especificar los nombres de archivo aceptables para la configuración del agente en los hosts Windows y Linux.</p> <p>De manera predeterminada, se excluyen de la recopilación los archivos <code>.zip</code> y <code>.gz</code>.</p> <hr/> <p>Importante Si está recopilando un archivo de registro rotado, use los parámetros <code>include</code> y <code>exclude</code> para especificar un patrón glob que coincida con el archivo principal y el archivo rotado. Si el patrón glob solo coincide con el archivo de registro principal, los agentes de vRealize Log Insight pueden perder eventos durante la rotación. Los agentes de vRealize Log Insight determinan automáticamente el orden correcto de los archivos rotados y envían eventos al servidor de vRealize Log Insight en el orden correcto. Por ejemplo, si el archivo de registro principal se denomina <code>myapp.log</code> y los registros rotados son <code>myapp.log.1</code>, <code>myapp.log.2</code> y así sucesivamente, puede usar el siguiente patrón <code>include</code>:</p> <pre>include= myapp.log;myapp.log.*</pre> <hr/>
<code>exclude=regular_expression</code>	<p>(Opcional) Un nombre de archivo o máscara de archivo (patrón glob) para excluir de la colección. Puede proporcionar los valores en una lista de valores separados con punto y coma. El valor predeterminado es un valor vacío, lo cual significa que no se excluye ningún archivo.</p> <hr/>
<code>event_marker=regular_expression</code>	<p>(Opcional) Una expresión regular que denota el inicio de un evento en el archivo de registro. Si se omite, de manera predeterminada para a una nueva línea. Las expresiones introducidas deben usar la sintaxis de expresiones regulares de Perl (lenguaje práctico de extracción e informes).</p> <hr/> <p>Nota Los símbolos, por ejemplo las comillas (" "), no se consideran como envoltorios para las expresiones regulares. Se consideran como parte del patrón.</p> <hr/> <p>Siendo que el agente de vRealize Log Insight se optimiza para la recopilación en tiempo real, los mensajes del registro parcial que se escriben con una demora interna pueden dividirse en eventos múltiples. Si el anexo del archivo del registro se detiene durante más de 200 ms sin observarse un nuevo <code>event_marker</code>, el evento parcial se considera completo, analizado y entregado. Esta lógica de sincronización no es configurable y tiene prioridad sobre el ajuste de <code>event_marker</code>. Los adionadores del archivo de registro deben alinear los eventos completos.</p> <hr/>
<code>enabled=yes no</code>	<p>(Opcional) Un parámetro para habilitar o deshabilitar la sección configurable. Los valores posibles son <code>yes</code> o <code>no</code>. El valor predeterminado es <code>yes</code>.</p> <hr/>

Parámetro	Descripción
charset= <i>char-encoding-type</i>	<p>(Opcional) La codificación de caracteres de los archivos de registro que supervisa el agente. Los valores posibles son:</p> <ul style="list-style-type: none"> ■ UTF-8 ■ UTF-16LE ■ UTF-16BE <p>El valor predeterminado es UTF-8.</p>
tags= <i>{"nombre-de-etiqueta": "valor-de-etiqueta", ...}</i>	<p>(Opcional) Un parámetro para añadir etiquetas personalizadas a los campos de eventos recopilados. Defina las etiquetas usando la anotación JSON. Los nombres de etiquetas pueden incluir letras, números y guiones bajos. Un nombre de etiqueta solo puede comenzar con una letra o un guion bajo y no puede tener más de 64 caracteres. Los nombres de las etiquetas no distinguen entre mayúsculas y minúsculas. Por ejemplo, si utiliza las etiquetas={"etiqueta_nombre1" : "etiqueta valor 1", "Etiqueta_Nombre1" : "etiqueta valor 2" }, Etiqueta_Nombre1 se ignora, por tratarse de una instancia duplicada. No es posible utilizar evento_tipo y la marca de tiempo como nombres de etiqueta. Los duplicados dentro de la misma declaración se ignoran.</p> <p>Si el destino es un servidor syslog, las etiquetas pueden anular el campo APP-NAME. Por ejemplo, etiquetas={"appname":"VROPS"}.</p>
exclude_fields	<p>(Opcional) Un parámetro para excluir de la recopilación a los campos individuales. Puede proporcionar los valores múltiples en una lista de valores separados con punto y coma o por coma. Por ejemplo,</p> <ul style="list-style-type: none"> ■ exclude_fields=hostname; filepath ■ exclude_fields=type; size ■ exclude_fields=type, size
raw_syslog= Yes No	<p>Para los agentes que utilizan el protocolo syslog, esta opción permite al agente recopilar y enviar eventos syslog sin formato. El valor predeterminado es No, lo que significa que los eventos recopilados se transforman con los atributos de syslog especificados por el usuario. Habilite esta opción para recopilar eventos sin transformaciones syslog.</p>

Ejemplo: Configuraciones

```
[filelog|vCenterMain]
directory=C:\ProgramData\VMware\VMware VirtualCenter\Logs
include=vpxd-*.log
exclude=vpxd-alert-*.log;vpxd-profiler-*.log
event_marker=^{\d{4}}-\d{2}-\d{2}[A-Z]\d{2}:\d{2}:\d{2}\.\d{3}
```

```
[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
include=*.log
exclude=*_old.log
tags={"Provider" : "Apache"}
```

```
[filelog|MSSQL]
directory=C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log
```

```
charset=UTF-16LE
event_marker=[^\s]
```

Configurar filtros para los canales del archivo de registro de Windows

Puede establecer los filtros para los archivo de registro de Windows para incluir o excluir explícitamente los eventos de registro.

Puede usar los parámetros `whitelist` y `blacklist` para evaluar una expresión de filtro. La expresión del filtro es una expresión booleana que consta de operadores y campos de eventos.

Nota La opción `blacklist` sirve únicamente para campos; no se puede usar para bloquear texto.

- El parámetro `whitelist` recopila solo los eventos de registro para los cuales la expresión del filtro evalúa como distinta a cero. Si omite este parámetro, el valor se implica en 1.
- El parámetro `blacklist` excluye los eventos de registro para los cuales la expresión del filtro evalúa como distinta a cero. El valor predeterminado es 0.

Para obtener una lista completa de los operadores y campos de eventos Windows, consulte [Campos de eventos y operadores](#).

Requisitos previos

Inicie sesión en el equipo Windows donde instaló el agente de Windows de vRealize Log Insight e inicie el administrador de servicios para verificar que el servicio del agente de vRealize Log Insight esté instalado.

Procedimiento

- 1 Desplácese hasta el directorio de datos del programa del agente de Windows de vRealize Log Insight.

```
%ProgramData%\VMware\Log Insight Agent
```

- 2 Abra el archivo `liagent.ini` en cualquier editor de texto.
- 3 Añada un parámetro `whitelist` o `blacklist` en la sección `[filelog|]`.

Por ejemplo:

```
[filelog|apache]
directory = ruta_acceso_a_directorio_registro
include = patrón_glob
blacklist = expresión_filtro
```

- 4 Cree una expresión de filtro a partir de operadores y campos de eventos Windows.

Por ejemplo

```
whitelist = myServer
```

5 Guarde y cierre el archivo `liagent.ini`.

Ejemplo: Configuraciones del filtro

Puede configurar el agente para que recopile únicamente registros donde el nombre del servidor sea

```
[filelog|apache]
directory=C:\Program Files\Apache Software Foundation\Apache2.4\logs
include=error.log
parser=clf
whitelist = server_name == "sample.com"
blacklist = remote_host == "127.0.0.1"
```

Reenviar eventos a Log Insight Windows Agent

Puede reenviar eventos de máquinas Windows a una máquina en la que se ejecute Log Insight Windows Agent.

Puede usar Windows Event Forwarding para reenviar eventos de múltiples máquinas Windows a una máquina en la que esté instalado Log Insight Windows Agent. A continuación, podrá configurar Log Insight Windows Agent para recopilar todos los eventos reenviados y enviarlos a un servidor de vRealize Log Insight.

Familiarícese con Windows Event Forwarding. Consulte <http://technet.microsoft.com/en-us/library/cc748890.aspx> y [http://msdn.microsoft.com/en-us/library/windows/desktop/bb870973\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb870973(v=vs.85).aspx).

Requisitos previos

Consulte [Recopilar eventos de canales de eventos de Windows](#).

Procedimiento

- 1 Añada una nueva sección a la configuración de Log Insight Windows Agent para recopilar eventos del canal de eventos de Windows que reciba eventos reenviados.

El nombre del canal predeterminado es ForwardedEvents.

- 2 Establezca Windows Event Forwarding.

Pasos siguientes

Vaya a la interfaz de usuario web de vRealize Log Insight y verifique que reciba los eventos reenviados.

Configurar Log Insight Linux Agent

Puede configurar Log Insight Linux Agent después de instalarlo.

Puede utilizar la [Configuración de agentes centralizada](#) para configurar el agente a fin de que envíe eventos a un servidor de vRealize Log Insight, establezca el protocolo y el puerto de comunicaciones, y configure la recopilación de registros de archivos sin formato. Para obtener la ubicación del archivo `liagent.ini`, consulte [Definir el nivel de detalles de registro en los Log Insight Agents](#).

Configuración predeterminada del agente de Linux de vRealize Log Insight

Después de la instalación, el archivo `liagent.ini` contiene la configuración predeterminada preconfigurada para el Log Insight Windows Agent.

Configuración predeterminada `liagent.ini` del agente de Linux de vRealize Log Insight

Si usa nombres y valores que no son ASCII, guarde la configuración como UTF-8.

Si utiliza la configuración central, la configuración final es este archivo junto con ajustes del servidor para generar el archivo `liagent-effective.ini`.

Posiblemente le resulte más eficiente configurar los parámetros desde la página de agentes del servidor.

```
[server]
; Hostname or IP address of your Log Insight server / cluster load balancer. Default:
;hostname=LOGINSIGHT

;Enables or disables centralized configuration from the vRealize Log Insight server.
;When enabled, agent configuration changes made to the liagent.ini file on the server
;are joined with the settings in this file. to this agent. Accepted values are yes or no and
0 or 1.
;The default is yes.
;
;central_config=yes
;
;
; Protocol can be cfapi (Log Insight REST API), syslog. Default:
;proto=cfapi

; Log Insight server port to connect to. Default ports for protocols (all TCP):
; syslog: 514; syslog with ssl: 6514; cfapi: 9000; cfapi with ssl: 9543. Default:
;port=9543

; SSL usage. Default:
;ssl=yes
; Example of configuration with trusted CA:
;ssl=yes
;ssl_ca_path=/etc/pki/tls/certs/ca.pem

; Time in minutes to force reconnection to the server.
; This option mitigates imbalances caused by long-lived TCP connections. Default:
;reconnect=30
```

```
[logging]
; Logging verbosity: 0 (no debug messages), 1 (essentials), 2 (verbose with more impact on
performance).
; This option should always be 0 under normal operating conditions. Default:
;debug_level=0

[storage]
; Max local storage usage limit (data + logs) in MBs. Valid range: 100-2000 MB.
;max_disk_buffer=200

; Uncomment the appropriate section to collect system logs
; The recommended way is to enable the Linux content pack from LI server
;[filelog|syslog]
;directory=/var/log
;include=messages;messages.?.syslog;syslog.?
```

Parámetro	Valor predeterminado	Descripción
hostname	LOGINSIGHT	La dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight. El valor predeterminado es loginsight .
central_config	yes	Habilite o deshabilite la configuración centralizada para este agente. Cuando la configuración centralizada esté deshabilitada, el agente ignora la configuración del servidor vRealize Log Insight. Los valores aceptados son <i>yes</i> , <i>no</i> , <i>1</i> o <i>0</i> . El valor predeterminado es <i>yes</i> .
proto	cfapi	Protocolo que utiliza el agente para enviar eventos al servidor de vRealize Log Insight. Los valores posibles son <i>cfapi</i> y <i>syslog</i> . El valor predeterminado es <i>cfapi</i> .
port	9543, 9000, 6514 y 514	Puerto de comunicación que utiliza el agente para enviar eventos al servidor vRealize Log Insight. Los valores predeterminados son 9543 para <i>cfapi</i> con SSL habilitado, 9000 para <i>cfapi</i> con SSL deshabilitado, 6514 para <i>syslog</i> con SSL habilitado y 514 para <i>syslog</i> con SSL deshabilitado.
ssl	yes	Habilita o deshabilita SSL. El valor predeterminado es <i>sí</i> . Si <i>ssl</i> se establece como <i>sí</i> , en el caso de no configurar un valor para el puerto, se selecciona automáticamente el puerto 9543.

Parámetro	Valor predeterminado	Descripción
<code>max_disk_buffer</code>	200	El espacio máximo en disco en MB que utiliza Log Insight Windows Agent para regular eventos y sus propios registros. Cuando se alcanza el <code>max_disk_buffer</code> especificado, el agente comienza a descartar los eventos entrantes nuevos.
<code>debug_level</code>	0	Define el nivel de detalles de registro. Consulte Definir el nivel de detalles de registro en los Log Insight Agents .

Recopilar eventos de un archivo de registro

Puede configurar el agente de Linux de vRealize Log Insight para que recopile eventos desde uno o más archivos de registro.

De forma predeterminada, el agente de Linux de vRealize Log Insight recopila los archivos ocultos creados por aplicaciones o editores. Los nombres de archivos ocultos empiezan por punto. Puede evitar que el agente de Linux de vRealize Log Insight recopile archivos ocultos agregando un parámetro de exclusión **`exclude=.*`**.

Los nombres de campos están restringidos. Los siguientes nombres están reservados y no se pueden utilizar como nombres de campo.

- `event_type`
- `hostname`
- `source`
- `text`

Puede especificar hasta tres destinos para la información del agente y filtrar la información antes de enviarla. Consulte [Reenviar información desde un agente de vRealize Log Insight](#)

Nota Supervisar un gran número de archivos, como mil o más, da lugar a un mayor uso de recursos por parte del agente de vRealize Log Insight y tiene un impacto sobre el rendimiento general de la máquina host. Para evitar esto, configure el agente para supervisar solo los archivos necesarios con patrones y globs, o archive los archivos de registro anteriores. Si la supervisión de un gran número de archivos es un requisito, considere la posibilidad de aumentar los parámetros de host, como la CPU y la memoria RAM.

Requisitos previos

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

Procedimiento

- 1 Abra el archivo `/var/lib/loginsight-agent/liagent.ini` en cualquier editor de texto.
- 2 Busque la sección `[servidor|<id_de_dest>]` del archivo. Añada los parámetros de configuración y fije los valores para su entorno.

```
[filelog|nombre_sección]
directory=ruta_acceso_a_directorio_registro
include=patrón_glob
...
```

Parámetro	Descripción
<code>[filelog section_name]</code>	Un nombre único para la sección de configuración.
<code>directory=full-path-to-log-file</code>	<p>La ruta de acceso completa al directorio del archivo de registro. Se admiten los patrones glob. Configuraciones de ejemplo:</p> <ul style="list-style-type: none"> ■ Para recopilar de todos los subdirectorios del directorio <code>D:\Logs\new_test_logs</code>, utilice <code>directory=D:\Logs\new_test_logs*</code> ■ Si sus subdirectorios tienen sus propios subdirectorios, utilice la siguiente configuración para supervisar todos los subdirectorios <code>directory=D:\Logs\new_test_logs**</code> <p>Nota Para limitar el número de archivos y directorios, y evitar un alto consumo de recursos, no puede definir un patrón glob de directorio para los directorios de primer o segundo nivel, como: <code>directory=c:/tmp/*</code> o <code>directory=c:\Logs*</code>. La ruta del directorio debe tener al menos dos niveles.</p> <p>Si define una ruta de acceso a un directorio que aún no existe, el agente recopilará los archivos de registro de ese directorio una vez que se cree el directorio y los archivos.</p> <p>Puede definir el mismo directorio en una o más secciones de configuración diferentes para reunir los registros varias veces desde el mismo archivo. Este proceso hace que sea posible aplicar distintas etiquetas y filtros al mismo origen de eventos.</p> <p>Nota Si utiliza configuraciones idénticas para estas secciones, los eventos duplicados se muestran del lado del servidor.</p>

Parámetro	Descripción
<code>include=file_name; ...</code>	<p>(Opcional) El nombre de un archivo o una máscara de archivo (patrón glob) desde el cual reunir los datos. Puede proporcionar los valores en una lista de valores separados con punto y coma. El valor predeterminado es <code>*</code>, lo cual significa que se incluyen todos los archivos. El parámetro distingue entre mayúsculas y minúsculas.</p> <p>Se puede utilizar una máscara de archivo (patrón global) con los archivos de grupo que sigan la misma convención de nomenclatura, así como con los que usen el mismo nombre de archivo. Por ejemplo, los nombres de archivo que incluyen espacios, como <code>vRealize Ops Analytics.log</code> y <code>vRealize Ops Collector.log</code>, se pueden escribir como <code>vRealize?Ops?Analytics*.log</code> o <code>vRealize*.log</code>. Las máscaras de archivo permiten especificar los nombres de archivo aceptables para la configuración del agente en los hosts Windows y Linux.</p> <p>De manera predeterminada, se excluyen de la recopilación los archivos <code>.zip</code> y <code>.gz</code>.</p> <p>Importante Si está recopilando un archivo de registro rotado, use los parámetros <code>include</code> y <code>exclude</code> para especificar un patrón glob que coincida con el archivo principal y el archivo rotado. Si el patrón glob solo coincide con el archivo de registro principal, los agentes de vRealize Log Insight pueden perder eventos durante la rotación. Los agentes de vRealize Log Insight determinan automáticamente el orden correcto de los archivos rotados y envían eventos al servidor de vRealize Log Insight en el orden correcto. Por ejemplo, si el archivo de registro principal se denomina <code>myapp.log</code> y los registros rotados son <code>myapp.log.1</code>, <code>myapp.log.2</code> y así sucesivamente, puede usar el siguiente patrón <code>include</code>:</p> <pre>include= myapp.log;myapp.log.*</pre>
<code>exclude=regular_expression</code>	<p>(Opcional) Un nombre de archivo o máscara de archivo (patrón glob) para excluir de la colección. Puede proporcionar los valores en una lista de valores separados con punto y coma. El valor predeterminado es un valor vacío, lo cual significa que no se excluye ningún archivo.</p>
<code>event_marker=regular_expression</code>	<p>(Opcional) Una expresión regular que denota el inicio de un evento en el archivo de registro. Si se omite, de manera predeterminada para a una nueva línea. Las expresiones introducidas deben usar la sintaxis de expresiones regulares de Perl (lenguaje práctico de extracción e informes).</p> <p>Nota Los símbolos, por ejemplo las comillas (" "), no se consideran como envoltorios para las expresiones regulares. Se consideran como parte del patrón.</p> <p>Siendo que el agente de vRealize Log Insight se optimiza para la recopilación en tiempo real, los mensajes del registro parcial que se escriben con una demora interna pueden dividirse en eventos múltiples. Si el anexo del archivo del registro se detiene durante más de 200 ms sin observarse un nuevo <code>event_marker</code>, el evento parcial se considera completo, analizado y entregado. Esta lógica de sincronización no es configurable y tiene prioridad sobre el ajuste de <code>event_marker</code>. Los adionadores del archivo de registro deben alinear los eventos completos.</p>
<code>enabled=yes no</code>	<p>(Opcional) Un parámetro para habilitar o deshabilitar la sección configurable. Los valores posibles son <code>yes</code> o <code>no</code>. El valor predeterminado es <code>yes</code>.</p>

Parámetro	Descripción
charset=char-encoding-type	<p>(Opcional) La codificación de caracteres de los archivos de registro que supervisa el agente. Los valores posibles son:</p> <ul style="list-style-type: none"> ■ UTF-8 ■ UTF-16LE ■ UTF-16BE <p>El valor predeterminado es UTF-8.</p>
tags={"nombre-de-etiqueta": "valor-de-etiqueta", ...}	<p>(Opcional) Un parámetro para añadir etiquetas personalizadas a los campos de eventos recopilados. Defina las etiquetas usando la anotación JSON. Los nombres de etiquetas pueden incluir letras, números y guiones bajos. Un nombre de etiqueta solo puede comenzar con una letra o un guion bajo y no puede tener más de 64 caracteres. Los nombres de las etiquetas no distinguen entre mayúsculas y minúsculas. Por ejemplo, si utiliza las etiquetas={"etiqueta_nombre1" : "etiqueta valor 1", "Etiqueta_Nombre1" : "etiqueta valor 2" }, Etiqueta_Nombre1 se ignora, por tratarse de una instancia duplicada. No es posible utilizar evento_tipo y la marca de tiempo como nombres de etiqueta. Los duplicados dentro de la misma declaración se ignoran.</p> <p>Si el destino es un servidor syslog, las etiquetas pueden anular el campo APP-NAME. Por ejemplo, etiquetas={"appname":"VROPS"}.</p>
exclude_fields	<p>(Opcional) Un parámetro para excluir de la recopilación a los campos individuales. Puede proporcionar los valores múltiples en una lista de valores separados con punto y coma o por coma. Por ejemplo,</p> <ul style="list-style-type: none"> ■ exclude_fields=hostname; filepath ■ exclude_fields=type; size ■ exclude_fields=type, size
raw_syslog=Yes No	<p>Para los agentes que utilizan el protocolo syslog, esta opción permite al agente recopilar y enviar eventos syslog sin formato. El valor predeterminado es No, lo que significa que los eventos recopilados se transforman con los atributos de syslog especificados por el usuario. Habilite esta opción para recopilar eventos sin transformaciones syslog.</p>

3 Guarde y cierre el archivo liagent.ini.

Ejemplo: Configuraciones

```
[filelog|messages]
directory=/var/log
include=messages;messages.?

[filelog|syslog]
directory=/var/log
include=syslog;syslog.?

[filelog|Apache]
directory=/var/log/apache2
include=*
```

Filtrar eventos

Puede filtrar todos los eventos recopilados en el agente de Linux de vRealize Log Insight en función de los valores de los campos para especificar qué eventos de registro se deben seleccionar o quitar. Puede utilizar las opciones de recopilador de `whitelist` y `blacklist` para definir filtros.

Sugerencia De forma predeterminada, el agente de Linux de vRealize Log Insight recopila los archivos ocultos creados por los programas o los editores. Los nombres de archivos ocultos comienzan con un punto. Puede evitar que el agente de Linux de vRealize Log Insight recopile archivos ocultos añadiendo un parámetro de exclusión `exclude=.*`.

Para cada evento, el recopilador evalúa las expresiones de filtro `whitelist` y `blacklist`. Si la expresión `whitelist` se evalúa como `true` (verdadero) y la expresión `blacklist` se evalúa como `false` (falso) o no se puede evaluar, el evento se mueve a la cola para su procesamiento posterior. En cualquier otro caso, el recopilador quita el evento. El valor predeterminado de la expresión `whitelist` es `true` y el valor predeterminado de la expresión `blacklist` es `false`.

Sugerencia El recopilador de `Filelog` proporciona menos campos para filtrar. Para obtener campos para filtrar, puede analizar los registros. Para obtener más información, consulte [Analizar registros](#).

Un filtro `whitelist` o `blacklist` es un conjunto de variables, literales y operadores que se evalúan como un único valor lógico o entero. Los campos de eventos se utilizan como variables y cadenas con comillas dobles y números como literales. Para obtener información sobre los operadores que puede utilizar en una expresión de filtro, consulte [Campos de eventos y operadores](#).

Nota

- Si compara un número con una cadena o si la comparación incluye cadenas numéricas, cada cadena se convierte en un número y la comparación se realiza numéricamente. Por ejemplo:
 - La expresión `whitelist = 123.0 == "000123"` se evalúa como `true`.
 - La expresión `whitelist = "00987" == "987.00"` se evalúa como `true`.
 - En la expresión `whitelist = response_size >= "12.12"`, si el campo `response_size` tiene un valor numérico, la expresión se evalúa numéricamente. Si el tamaño de respuesta es mayor que 12,12, la expresión es verdadera (`true`); de lo contrario, es falsa (`false`).
 - En la expresión `whitelist = "09123" < "234"`, los dos literales de cadena se convierten en valores numéricos y la expresión se evalúa como `false`.
- Si uno de los operandos de cadena no se puede convertir en valores numéricos, ambos operandos se convierten en una cadena. Se realiza una simple comparación lexicográfica con distinción entre mayúsculas y minúsculas. Por ejemplo:
 - La expresión `whitelist = "1234a" == "1234A"` es una comparación de cadena que se evalúa como `false`.
 - La expresión `whitelist = 4 < "four"` convierte 4 en "4" y se evalúa como `true`.
 - En la expresión `whitelist = response_size > "thousand"`, el valor del campo `response_size` se convierte en un valor de cadena, que evalúa la expresión como `false`.
- Si una expresión de filtro se evalúa como un valor entero, se trata como `false` si es 0 y como `true` en caso contrario.

Por ejemplo, la expresión `whitelist = some_integer & 1` se evalúa como `true` si el campo `some_integer` tiene un conjunto de bits menos significativo y como `false` en caso contrario.

Para obtener una lista completa de los operadores y campos de eventos, consulte [Recopilar eventos de un archivo de registro](#).

En este ejemplo, se recopilan los registros de acceso de Apache del archivo `/var/log/httpd/access`. Algunos de los registros de ejemplo del archivo son:

- 127.0.0.1 - frank [10/Oct/2016:13:55:36 +0400] "GET /apache_pb.gif HTTP/1.0" 200 2326
- 198.51.100.56 - john [10/Oct/2016:14:15:31 +0400] "GET /some.gif HTTP/1.0" 200 8270
- 198.51.100.12 - smith [10/Oct/2016:14:15:31 +0400] "GET /another.gif HTTP/1.0" 303 348

- 198.51.100.32 - test [10/Oct/2016:15:22:55 +0400] "GET /experimental_page.gif HTTP/1.0" 400 46374
- 127.0.0.1 - test [10/Oct/2016:15:22:57 +0400] "GET /experimental_page2.gif HTTP/1.0" 301 100

Requisitos previos

- 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.

Procedimiento

- 1 Defina un analizador para los registros, como se muestra en el siguiente fragmento de código:

```
[parser|apache-access]
base_parser=clf
format=%h %l %u %t \"%r\" %s %b
```

El analizador que ha definido extrae los campos `remote_host`, `remote_log_name`, `remote_auth_user`, `timestamp`, `request`, `status_code` y `response_size` para cada evento recopilado desde el archivo `/var/log/httpd/access`. Puede utilizar estos campos para filtrar eventos.

- 2 Abra el archivo `/var/lib/loginsight-agent/liagent.ini` en cualquier editor de texto.
- 3 Defina una sección de `Filelog` en el archivo para recopilar y analizar registros, como se muestra en el siguiente fragmento de código:

```
[filelog|apache-access]
directory = /var/log/httpd/
include = access
parser = apache-access
```

- 4 Filtre los eventos según sus requisitos.

- Para recopilar registros en los que el estado de HTTP es 200, puede definir una opción `whitelist` en la sección `Filelog`, tal como se muestra en el siguiente fragmento de código:

```
[filelog|apache-access]
directory = /var/log/httpd/
include = access
parser = apache-access
whitelist = status_code == 200
```

La expresión `whitelist` se evalúa como `true` solo para el primer y el segundo evento de los registros de ejemplo y el recopilador selecciona estos eventos.

Si el campo `status_code` no existe en el evento porque no está presente en el registro o no se analiza, no se puede evaluar la expresión `whitelist`, lo que significa que se evalúa como `false` y el recopilador quita el evento.

- Para quitar un evento que no le interese, puede usar la opción `blacklist`. Por ejemplo, si no le interesa el tráfico local, puede bloquear la IP local, como se muestra en el siguiente fragmento de código:

```
[filelog|apache-access]
directory = /var/log/httpd/
include = access
parser = apache-access
blacklist = remote_host == "127.0.0.1"
```

El recopilador selecciona el segundo, tercer y cuarto evento de los registros de ejemplo.

- Para filtrar eventos en función de más de un predicado, puede usar los operadores `or` y `and`. Por ejemplo, puede quitar eventos generados a partir de una IP local o eventos generados por usuarios de prueba desde cualquier host que no necesite, como se muestra en el siguiente fragmento de código:

```
[filelog|apache-access]
directory = /var/log/httpd/
include = access
parser = apache-access
blacklist = remote_host == "127.0.0.1" or remote_auth_user == "test"
```

Al usar el operador `or`, la expresión `blacklist` se evalúa como `true` para omitir un evento no deseado. La expresión indica al recopilador que quite el evento si el valor del campo `remote_host` es "127.0.0.1" o el valor del campo `remote_auth_user` es "test".

El recopilador selecciona el segundo y tercer evento de los registros de ejemplo.

- Para quitar los eventos generados desde una IP local por usuarios de prueba, puede usar `and` en la expresión `blacklist`, como se muestra en el siguiente fragmento de código:

```
[filelog|apache-access]
directory = /var/log/httpd/
include = access
parser = apache-access
blacklist = remote_host == "127.0.0.1" and remote_auth_user == "test"
```

El recopilador quita el quinto evento de los registros de ejemplo.

- Puede usar los filtros `whitelist` y `blacklist` juntos. Por ejemplo, si necesita eventos en los que el tamaño de la respuesta sea superior a 1024 bytes, pero no requiere eventos que se hayan originado desde un host local, puede usar el siguiente fragmento de código:

```
[filelog|apache-access]
directory = /var/log/httpd/
```

```
include = access
parser = apache-access
whitelist = response_size > 1024
blacklist = remote_host == "127.0.0.1" or remote_host == "localhost"
```

El recopilador selecciona el segundo evento de los registros de ejemplo.

Recopilar eventos de `journald`

A partir de vRealize Log Insight 4.6, los agentes pueden leer registros del servicio de sistema `journald` para datos de registro en distribuciones de Linux que ejecuten `systemd`. `journald` ahora es el estándar predeterminado para el inicio de sesión en plataformas Linux basadas en `systemd`. La sección de configuración de `journald` admite las siguientes opciones:

`journal_files`

Los archivos de diario que se van a supervisar. Se admiten los siguientes valores:

Valor	Descripción
todo	Permite abrir y supervisar todos los archivos de diario disponibles.
local	Permite supervisar y leer solo los archivos de diario generados en la máquina local.
runtime	Permite supervisar y leer solo los archivos de diario volátiles, sin incluir los archivos en el almacenamiento persistente.
system	Permite supervisar y leer solo los archivos del sistema y los archivos de diario del kernel.
user	Permite supervisar y leer solo los archivos de diario del usuario actual.

`fetch_fields`

Los campos que se deben recuperar con el mensaje de las entradas del registro del diario. El valor de esta opción es una lista sin distinción entre mayúsculas y minúsculas de los nombres de campos separados por comas. Se admiten los siguientes valores:

Valor	Descripción
pri_severity,pri_facility,syslog_identifier	Valor predeterminado para esta opción.
*	Recupera todos los campos.
todo	No recupera ningún campo.

Filtrado de eventos de agentes de vRealize Log Insight

Puede proporcionar la información que envía un agente a un destino con la opción de filtro en la sección `[server|<dest_id>]` del archivo `liagent.ini` local.

La opción sigue el siguiente formato:

```
filter = {collector_type; collector_filter; event_filter}
```

Tipo de filtro	Descripción
collector_type	Una lista separada por comas que define los tipos de recopiladores. Los valores admitidos son filelog o winlog. Si no se proporciona ningún valor, se utilizarán todos los tipos de recopiladores.
collector_filter	Especifica el nombre de una sección del recopilador en un formato de expresión regular. Por ejemplo, <code>vcops_.*</code> se refiere a todas las secciones del recopilador que comienzan con "vcops_".
event_filter	Los filtros de los campos de eventos usan la misma sintaxis que las de elementos permitidos y no permitidos en las secciones del recopilador. Un agente envía solo eventos que evalúan la expresión como True o un valor distinto de cero. Si <code>event_filter</code> está vacío, siempre se evaluará como True. Para utilizar <code>event_filter</code> en eventos, debe tener un analizador en las secciones del recopilador adecuadas para la extracción de campos. Si no se puede evaluar una expresión debido a la ausencia de campos en el evento recopilado, se descartará el evento.

Puede especificar más de una expresión de filtro si las separa con una coma, como se muestra en el siguiente ejemplo:

```
filter=
{winlog;Micr.*},{filelog;apache-access;level=="error"}
```

Si un mensaje cumple más de un conjunto de criterios de filtro para un destino, se enviará solo una vez.

Tabla 4-1. Ejemplos de sintaxis

Filter (Filtrar)	Significado
filter= {winlog;Microsoft.*;}	Envía eventos de recopiladores de winlog solo si el nombre del evento comienza con "Microsoft".
filter= {winlog;Microsoft.*; eventid == 1023}	Envía eventos de recopiladores de winlog solo si el nombre del evento comienza con "Microsoft" y el ID de evento es igual a 1023.
filter= {.*;}	Valor predeterminado del filtro. Envía todos los eventos de todas las fuentes.
filter= {winlog;.*;}	Envía todos los eventos de secciones de winlog.
filter= {filelog;syslog;facility<5}	Envía eventos de la sección [filelog syslog] si el valor de facility es inferior a 5. Las secciones [filelog syslog] deben tener un analizador que extraiga el campo facility. De lo contrario, se omitirán todos los eventos.
filter= {;;}	No coincide con ningún evento. Utilice esta sintaxis para deshabilitar el reenvío de eventos.

En el ejemplo siguiente se agrega un filtro a la configuración del segundo destino del ejemplo anterior.

```
; The second destination receives just syslog events through the plain syslog protocol.
[server|syslog-audit]
```

```
hostname=third_party_audit_management.eng.vmware.com
proto=syslog
ssl=no
filter= {filelog; syslog; }
```

El ejemplo siguiente utiliza una expresión de filtro más compleja.

```
; This destination receives vRealize Operations Manager events if they have the level field
equal
;to "error" or "warning" and they are collected by sections whose name begins with "vrops-"

[server|licf-prod1]
hostname=vrops-errors.licf.vmware.com
filter= {; vrops-.*; level == "error" || level == "warning"}
```

Puede especificar más de una expresión de filtro si las separa con una coma, como se muestra en el siguiente ejemplo.

```
filter= e.
{winlog;Micr.*;},{filelog;apache-access;level=="error"}
```

Reenviar información desde un agente de vRealize Log Insight

Puede reenviar los eventos recopilados por un agente a un máximo de tres destinos. Un destino puede incluir un reenviador o servidores de vRealize Log Insight, o bien soluciones de gestión de registros de terceros.

Por ejemplo, es posible que quiera enviar registros de sistemas o auditorías a un servidor para el equipo de seguridad, registros de aplicaciones a un servidor del equipo de desarrollo y operaciones y registros de métricas a un sistema de administración de TI. Utilice filtros para especificar la información que se envía al destino. Puede reenviar información desde un mismo agente de vRealize Log Insight hasta un máximo de tres destinos.

La configuración del agente se lleva a cabo a través de la sección `[server|<id_dest>]` del archivo local `liagent.ini`. Utilice el protocolo cfapi con los reenviadores o los servidores de vRealize Log Insight y syslog con otros destinos.

Si especifica más de un destino para un agente, el primero usará la ubicación predeterminada `loginsight`. Deberá especificar la información de la ubicación de los otros destinos.

El siguiente ejemplo muestra una parte de un archivo `liagent.ini` que especifica dos destinos. El nombre del servidor `loginsight` se aplica al primer destino de forma predeterminada y no se especifica. La segunda sección `[server|<dest_id>]` especifica un destino.

```
; The first (default) destination receives all collected events.
[server]
ssl=yes
```



```
; The second destination receives just syslog events through the plain syslog protocol.
[server|syslog-audit]
hostname=third_party_audit_management.eng.vmware.com
proto=syslog
ssl=no
```

Para obtener más información sobre cómo crear filtros para agentes, consulte [Filtrado de eventos de agentes de vRealize Log Insight](#).

Configurar el servidor vRealize Log Insight de destino

Puede establecer o cambiar el servidor de vRealize Log Insight de destino para un agente de vRealize Log Insight que se ejecute en Windows. Puede enviar eventos a un máximo de tres destinos y filtrar los resultados por destino.

Se puede configurar el destino predeterminado en la sección `[server]` del archivo `liagent.ini`. El destino predeterminado siempre está presente y, de forma predeterminada, el nombre de host se establece como `loginsight`. Para agregar más destinos, cree una sección `[server|<id_dest>]` para cada destino. Debe especificar un nombre de host único como ID de destino para cada conexión adicional. Puede utilizar las mismas opciones para los destinos adicionales y para la sección `[server]` predeterminada. No configure destinos adicionales para las actualizaciones automáticas ni los use para configurar agentes. Puede especificar dos destinos adicionales.

De forma predeterminada, el agente envía todos los eventos recopilados a todos los destinos. Puede filtrar eventos para enviar eventos diferentes a destinos diferentes con la opción `file`. Para obtener más información, consulte [Filtrado de eventos de agentes de vRealize Log Insight](#).

Requisitos previos

- Inicie sesión en el equipo Windows donde instaló el agente de Windows de vRealize Log Insight e inicie el administrador de servicios para verificar que el servicio del agente de vRealize Log Insight esté instalado.
- Si tiene un clúster de vRealize Log Insight con un Equilibrador de carga integrado habilitado, consulte [Habilitar equilibrador de carga integrado](#) para ver los requisitos específicos del certificado SSL personalizado.

Procedimiento

- 1 Desplácese hasta el directorio de datos del programa del agente de Windows de vRealize Log Insight.

```
%ProgramData%\VMware\Log Insight Agent
```

- 2 Abra el archivo `liagent.ini` en cualquier editor de texto.

3 Modifique los siguientes parámetros y fije los valores para su entorno.

Parámetro	Descripción
proto	<p>Protocolo que utiliza el agente para enviar eventos al servidor de vRealize Log Insight. Los valores posibles son <code>cfapi</code> y <code>syslog</code>.</p> <p>El valor predeterminado es <code>cfapi</code>.</p>
hostname	<p>La dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight.</p> <p>Se puede especificar una dirección IPv4 o IPv6. La dirección IPv6 se puede especificar con o sin corchetes. Por ejemplo:</p> <pre>hostname = 2001:cdba::3257:9652 or hostname = [2001:cdba::3257:9652]</pre> <p>Si el host admite pilas de IPv4 y de IPv6 y se indica un nombre de dominio como nombre de host, el agente selecciona la pila de IP según la dirección IP que devuelve la resolución de nombres. Si la resolución devuelve direcciones tanto IPv4 como IPv6, el agente intenta conectarse secuencialmente a ambas direcciones en el orden establecido.</p>
max_disk_buffer	<p>El espacio de disco máximo en MB que el agente de Windows de Log Insight puede usar para almacenar en búfer los eventos recopilados para ese servidor particular. Esta opción anula el valor <code>[storage].max_disk_buffer</code> para ese servidor.</p> <p>El valor predeterminado es 150 MB y puede establecer el tamaño de búfer entre 50 y 8.000 MB.</p>
port	<p>Puerto de comunicación que utiliza el agente para enviar eventos al servidor externo vRealize Log Insight. De forma predeterminada, el agente utiliza el puerto adecuado basado en las opciones que están configuradas para SSL y el protocolo. Consulte los valores de puerto predeterminados proporcionados en la lista que se incluye a continuación. Debe especificar la opción del puerto solo si es diferente a los valores predeterminados.</p> <ul style="list-style-type: none"> ■ <code>cfapi</code> con SSL habilitado: 9543 ■ <code>cfapi</code> con SSL deshabilitado: 9000 ■ <code>syslog</code> con SSL habilitado: 6514 ■ <code>syslog</code> con SSL deshabilitado: 514
ssl	<p>Habilita o deshabilita SSL. El valor predeterminado es <code>sí</code>.</p> <p>Cuando <code>ssl</code> se configura como <code>sí</code>, el puerto se establece a 9543, a menos que especifique lo contrario.</p>
reconnect	<p>El tiempo en minutos que transcurre antes de forzar la reconexión con el servidor. El valor predeterminado es 30.</p>
filter	<p>Especifica la información que un agente envía a un destino. Esta opción utiliza tres argumentos:</p> <pre>{collector_type; collector_filter; event_filter}</pre>


```
[server]
hostname=LOGINSIGHT
; Hostname or IP address of your Log Insight server / cluster load balancer. Default:
```

```

;hostname=LOGINSIGHT

; Protocol can be cfapi (Log Insight REST API), syslog. Default:
;proto=cfapi

; Log Insight server port to connect to. Default ports for protocols (all TCP):
; syslog: 514; syslog with ssl: 6514; cfapi: 9000; cfapi with ssl: 9543. Default:
;port=9543

; SSL usage. Default:
;ssl=yes

```

4 Guarde y cierre el archivo `liagent.ini`.

Ejemplo

El siguiente ejemplo de configuración establece un servidor vRealize Log Insight de destino que utiliza una entidad de certificación de confianza.

```

[server]
proto=cfapi
hostname=LOGINSIGHT
port=9543
ssl=yes;
ssl_ca_path=/etc/pki/tls/certs/ca.pem

```

El siguiente ejemplo muestra una configuración de varios destinos que incluye el filtro de mensajes por destino.

```

; The first (default) destination receives all collected events.
[server]
hostname=prod1.licf.vmware.com

; The second destination receives just syslog events through the plain syslog protocol.
[server|syslog-audit]
hostname=third_party_audit_management.eng.vmware.com
proto=syslog
ssl=no
filter={filelog; syslog; }

; The third destination receives vRealize Operations Manager events if they have the level
field equal to "error" or "warning"
; and they are collected by sections whose name begins with "vrops-"

[server|licf-prod1]
hostname=vrops-errors.licf.vmware.com
filter={; vrops-.*; level == "error" || level == "warning"}

; Collecting syslog messages.
[filelog|syslog]
directory=/var/log
include=messages

```

```
; various vROPs logs. Note that all section names begin with a "vrops-" prefix, which is used
in third destination filter.
[filelog|vrops-ANALYTICS-analytics]
directory=/data/vcops/log
include=analytics*.log*
exclude=analytics*-gc.log*
parser=auto

[filelog|vrops-COLLECTOR-collector]
directory=/data/vcops/log
include=collector.log*
event_marker=^{\d{4}}-{\d{2}}-{\d{2}} [\s]{\d{2}}:{\d{2}}:{\d{2}}\.,{\d{3}}
parser=auto

[filelog|vrops-COLLECTOR-collector_wrapper]
directory=/data/vcops/log
include=collector-wrapper.log*
event_marker=^{\d{4}}-{\d{2}}-{\d{2}} [\s]{\d{2}}:{\d{2}}:{\d{2}}\.\d{3}
parser=auto
```

Pasos siguientes

Puede configurar las opciones SSL adicionales para el agente de vRealize Log Insight. Vea [Configurar conexión SSL entre el servidor y los agentes de Log Insight](#).

Especificar el destino de un agente

Puede especificar hasta tres destinos a los que el agente de Linux de vRealize Log Insight enviará eventos.

Se definen varias conexiones de destino a través de la sección `[server|<dest_id>]` del archivo `li-agent.ini`, donde `<dest_id>` se corresponde con un único ID de conexión por configuración. Puede utilizar las mismas opciones para los destinos adicionales y para la sección `[server]` predeterminada. Sin embargo, no configure destinos adicionales para las actualizaciones automáticas ni tampoco los use para configurar agentes. Puede especificar dos destinos adicionales.

El primer destino que defina puede usar el valor predeterminado del servidor `loginsight`. Si define más destinos, puede especificar un nombre de host en las secciones de `[server]` para los destinos siguientes. Si no se aplican filtros, el agente envía todos los eventos recopilados a todos los destinos. Este es el comportamiento predeterminado. Sin embargo, puede filtrar para enviar eventos diferentes a destinos diferentes.

Requisitos previos

- 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.

- Si tiene un clúster de vRealize Log Insight con un Equilibrador de carga integrado habilitado, consulte [Habilitar equilibrador de carga integrado](#) para ver los requisitos específicos del certificado SSL personalizado.

Procedimiento

- 1 Abra el archivo `/var/lib/loginsight-agent/liagent.ini` en cualquier editor de texto.
- 2 Modifique los siguientes parámetros y fije los valores para su entorno.

Parámetro	Descripción
proto	<p>Protocolo que utiliza el agente para enviar eventos al servidor de vRealize Log Insight. Los valores posibles son <code>cfapi</code> y <code>syslog</code>.</p> <p>El valor predeterminado es <code>cfapi</code>.</p>
hostname	<p>La dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight.</p> <p>Se puede especificar una dirección IPv4 o IPv6. La dirección IPv6 se puede especificar con o sin corchetes. Por ejemplo:</p> <pre>hostname = 2001:cdba::3257:9652 or hostname = [2001:cdba::3257:9652]</pre> <p>Si el host admite pilas de IPv4 y de IPv6 y se indica un nombre de dominio como nombre de host, el agente usa la pila de IP en función de la dirección IP que devuelve la resolución de nombres. Si la resolución devuelve direcciones tanto IPv4 como IPv6, el agente intenta conectarse secuencialmente a ambas direcciones en el orden establecido.</p>
max_disk_buffer	<p>El espacio de disco máximo en MB que el agente de Linux de Log Insight puede usar para almacenar en búfer los eventos recopilados de ese servidor particular. Esta opción anula el valor <code>[storage].max_disk_buffer</code> para ese servidor.</p> <p>El valor predeterminado es 150 MB y puede establecer el tamaño de búfer entre 50 y 8.000 MB.</p>
port	<p>Puerto de comunicación que utiliza el agente para enviar eventos al servidor externo vRealize Log Insight. De forma predeterminada, el agente utiliza el puerto adecuado basado en las opciones que están configuradas para SSL y el protocolo. Consulte los valores de puerto predeterminados proporcionados en la lista que se incluye a continuación. Debe especificar la opción del puerto solo si es diferente a los valores predeterminados.</p> <ul style="list-style-type: none"> ■ <code>cfapi</code> con SSL habilitado: 9543 ■ <code>cfapi</code> con SSL deshabilitado: 9000 ■ <code>syslog</code> con SSL habilitado: 6514 ■ <code>syslog</code> con SSL deshabilitado: 514

Parámetro	Descripción
ssl	Habilita o deshabilita SSL. El valor predeterminado es sí. Si ssl se establece como sí, en el caso de no configurar un valor para el puerto, se selecciona automáticamente el puerto 9543.
reconnect	El tiempo en minutos para forzar la reconexión con el servidor. El valor predeterminado es 30.

```
[server]
hostname=LOGINSIGHT
; Hostname or IP address of your Log Insight server / cluster load balancer. Default:
;hostname=LOGINSIGHT

; Protocol can be cfapi (Log Insight REST API), syslog. Default:
;proto=cfapi

; Log Insight server port to connect to. Default ports for protocols (all TCP):
; syslog: 514; syslog with ssl: 6514; cfapi: 9000; cfapi with ssl: 9543. Default:
;port=9543

; SSL usage. Default:
;ssl=yes
```

3 Guarde y cierre el archivo `liagent.ini`.

Ejemplo

El siguiente ejemplo de configuración establece un servidor vRealize Log Insight de destino que utiliza una entidad de certificación de confianza.

```
[server]
proto=cfapi
hostname=LOGINSIGHT
port=9543
ssl=yes;
ssl_ca_path=/etc/pki/tls/certs/ca.pem
```

El siguiente ejemplo muestra una configuración de varios destinos.

- El primer destino (predeterminado) recibe todos los eventos recopilados.

```
[server]
hostname=prod1.licf.vmware.com
```

- El segundo destino recibe solo eventos syslog a través del protocolo syslog sin formato.

```
[server|syslog-audit]
hostname=third_party_audit_management.eng.vmware.com
proto=syslog
ssl=no
filter= {filelog; syslog; }
```

- El tercer destino recibe eventos vRealize Operations Manager si tienen el campo de nivel igual a "error" o "advertencia" y se recopilan por secciones cuyos nombres empiezan por "vrops-"

```
[server|licf-prod1]
hostname=vrops-errors.licf.vmware.com
filter= {; vrops-.*; level == "error" || level == "warning"}

;Collecting syslog messages.
[filelog|syslog]
directory=/var/log
include=messages

;various vRops logs. Note that all section names begin with "vrops-" prefix, which is used in
third destination filter.
[filelog|vrops-ANALYTICS-analytics]
directory=/data/vcops/log
include=analytics*.log*
exclude=analytics*-gc.log*
parser=auto
[filelog|vrops-COLLECTOR-collector]
directory=/data/vcops/log
include=collector.log*
event_marker=^\d
{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\, \d{3}
parser=auto

[filelog|vrops-COLLECTOR-collector_wrapper]
directory=/data/vcops/log
include=collector-wrapper.log*
event_marker=^\d{4}
-\d
{2}-\d{2}
[\s]\d
{2}:\d{2}
:\d
{2}
\.\d
{3}
parser=auto
```

Pasos siguientes

Puede configurar las opciones SSL adicionales para el agente de Linux de vRealize Log Insight. Vea [Configurar conexión SSL entre el servidor y los agentes de Log Insight](#).

Configuración centralizada de agentes vRealize Log Insight

Puede configurar varios agentes vRealize Log Insight.

Cada agente vRealize Log Insight tiene una configuración local y una configuración del lado del servidor. La configuración local se guarda en el archivo `liagent.ini` de la máquina virtual o física donde está instalado el agente vRealize Log Insight. La configuración del lado del servidor se puede acceder y editar; por ejemplo, desde **Administración > Agentes** en la interfaz de usuario web. La configuración de cada agente vRealize Log Insight está formada por secciones y claves. Las claves tienen valores configurables.

Los agentes vRealize Log Insight sondean periódicamente el servidor vRealize Log Insight y reciben la configuración del lado del servidor. La configuración del lado del servidor y la configuración local se fusionan y el resultado es la configuración efectiva. Cada agente vRealize Log Insight usa la configuración efectiva como su configuración operativa. Las configuraciones se fusionan sección por sección y clave por clave. Los valores de la configuración del lado del servidor sustituyen a los valores de la configuración local. Las reglas de fusión son las siguientes:

- Si una sección está presente únicamente en la configuración local o únicamente en la configuración del lado del servidor, esta sección y todo su contenido se convierten en parte de la configuración efectiva.
- Si una sección está presente en las configuraciones local y del lado del servidor, las claves de la sección se fusionan de acuerdo con las siguientes reglas:
 - Si una clave está presente únicamente en la configuración local o únicamente en la configuración del lado del servidor, la clave y su valor se convierten en parte de esta sección en la configuración efectiva.
 - Si una clave está presente en las configuraciones local y del lado del servidor, la clave y su valor se convierten en parte de esta sección en la configuración efectiva, y se utiliza la configuración del valor del lado del servidor.

Un usuario administrador de vRealize Log Insight puede aplicar la configuración centralizada a todos los agentes de vRealize Log Insight. Por ejemplo, puede desplazarse hasta la página **Administración** y, en la sección **Administración**, hacer clic en **Agentes**. Introduzca los parámetros de configuración en el cuadro **Configuración de agente** y haga clic en **Guardar configuración para todos los agentes**. La configuración se aplicará a todos los agentes activos configurables durante el próximo ciclo de sondeo.

Un usuario administrador de vRealize Log Insight también puede utilizar filtros específicos en grupos de agentes, como por sistema operativo, versión de agente, nombre de host o rangos de IP, y aplicar la configuración a agentes de vRealize Log Insight específicos. Para obtener información sobre los grupos de agentes, consulte *Trabajar con grupos de agentes*.

Nota

- Puede aplicar una configuración centralizada únicamente a los agentes vRealize Log Insight que utilizan el protocolo cfapi.
- Un agente de vRealize Log Insight no se puede configurar en ninguno de los siguientes escenarios:
 - El servidor de vRealize Log Insight actual no es un destino principal. Para obtener información sobre la configuración de varios destinos, consulte [Especificar el destino de un agente](#).
 - El parámetro `central_config = no` se utiliza en la configuración del agente. Para obtener información sobre la configuración predeterminada del agente para Windows, consulte [Configuración predeterminada del Log Insight Windows Agent](#).

Un ejemplo de fusión de configuración

Un ejemplo de fusión de configuración local y de servidor de Log Insight Windows Agent.

Configuración local

Puede tener la siguiente configuración local de Log Insight Windows Agent.

```
[server]
proto=cfapi
hostname=HOST
port=9000

[winlog|Application]
channel=Application

[winlog|Security]
channel=Security

[winlog|System]
channel=System

[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
include=*.log
exclude=*_old.log
event_marker=^(\d{1,3}\.){3}\d{1,3} - -
```

Configuración del lado del servidor

Puede usar la página **Administración > Agentes** de la interfaz de usuario web para aplicar la configuración centralizada a todos los agentes. Por ejemplo, puede excluir y añadir canales de recopilación, y cambiar la configuración de reconexión predeterminada.

```
[server]
reconnect=20

[winlog|Security]
channel=Security
enabled=no

[winlog|Microsoft-Windows-DeviceSetupManagerOperational]
channel=Microsoft-Windows-DeviceSetupManager/Operational
```

Configuración efectiva

La configuración efectiva es una consecuencia de la fusión de las configuraciones local y del servidor. El Log Insight Windows Agent está configurado para:

- reconectarse con el servidor de vRealize Log Insight cada 20 minutos
- continuar recopilando canales de eventos de la aplicación y del sistema
- detener la recopilación del canal de eventos de seguridad
- iniciar la recopilación del canal de eventos Microsoft-Windows-DeviceSetupManager/Operational
- continuar recopilando ApacheAccessLogs

```
[server]
proto=cfapi
hostname=HOST
port=9000
reconnect=20

[winlog|Application]
channel=Application

[winlog|Security]
channel=Security
enabled=no

[winlog|System]
channel=System

[winlog|Microsoft-Windows-DeviceSetupManagerOperational]
channel=Microsoft-Windows-DeviceSetupManager/Operational

[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
include=*.log
```

```
exclude=*_old.log
event_marker=^(\d{1,3}\.){3}\d{1,3} - -
```

Uso de valores comunes para la configuración del agente

Puede reemplazar los valores predeterminados del archivo de configuración del agente por valores de parámetros comunes que se aplican a la sección de configuración de cada agente para los agentes de Linux o de Windows.

Opciones comunes

Las opciones que se especifican en la sección `[common|global]` del archivo de configuración `liagent.ini` se propagan a todas las secciones; por su parte, las opciones especificadas en la sección `[common|filelog]` lo hacen únicamente a todas las secciones de filelog, al igual que las opciones `[common|winlog]` se propagan únicamente a todas las secciones de winlog.

Puede definir los siguientes parámetros en las secciones comunes: `tags`, `include`, `exclude`, `event_marker`, `charset`, `exclude_fields` y `parser` como aparece en este ejemplo. Este ejemplo es de un agente de Windows:

```
[common|global]

tags = {"log_source_vm":"win-2008r2-64"}
exclude_fields = test_tag;some_other_tag
parser = auto

[common|filelog]
tags = {"collector_type":"filelog"}
exclude = *.trc

[filelog|channel_1]
directory = C:\app\log
include = *.log

...
```

Este ejemplo especifica el siguiente comportamiento:

- Todos los registros de las secciones de filelog cuentan con las etiquetas `log_source_vm` y `collector_type` con sus correspondientes valores.
- Las etiquetas `test_tag` y `some_other_tag` se excluyen de todos los registros que se envían.
- Se aplica el analizador `auto` a todos los registros obtenidos.
- De forma predeterminada, todos los recopiladores excluyen los archivos `*.trc` de la supervisión.

También se aplican las opciones incluidas en `[common|global]` a todas las secciones de winlog.

Combinar y reemplazar criterios

Si las opciones están definidas en más de una sección, sus valores se combinan o se reemplazan y la sección que cuente con el ámbito más pequeño tiene mayor prioridad en dichos procesos. Esto significa que un valor contenido en `[common|global]` se combina con o se reemplaza por un valor de `[common|filelog]` que, a su vez, se combina con o se reemplaza por un valor de `[filelog|sample_section]`.

El comportamiento de reemplazo y combinación sigue estas reglas:

- Las opciones cuyos valores representan una lista (`tags`, `include`, `exclude` y `excluded_fields`) se combinan con los valores de dicha opción de una sección con mayor prioridad. Además, en el caso de las etiquetas, los valores de las secciones con mayor prioridad reemplazan al de la misma etiqueta incluida en una sección con menor prioridad, como se describe anteriormente.
- El valor de las opciones que puedan tener un valor simple (`event_maker`, `charset` y `parser`) se reemplazan por los valores de la misma opción que aparecen en secciones con mayor prioridad.

Esto supone que el valor `charset=UTF-8` de `[filelog|sample_section]` reemplaza el valor global `charset= UTF-16LE` de `[common|global]`.

Así que, por ejemplo, si cuenta con `tags={"app":"global-test"}` en `[common|filelog]` y con `tags={"app":"local-test", "section":"flg_test_section"}` en `[filelog|flg_test_section]`, el valor de la etiqueta "app" de la sección `[filelog|flg_test_section]` reemplaza el valor de `[common|filelog]`. Todos los registros recopilados a través de esta sección de filelog tendrán una etiqueta "app" adicional con un valor "local-test" y una etiqueta "section" con el valor "flg_test_section". En las secciones de winlog, la cadena de prioridad es la misma, donde todas las secciones `[winlog|...]` tienen la prioridad más alta y `[common|global]` tienen la más baja.

Si se especifican valores no válidos en secciones comunes, normalmente se omiten y no se combinan con los valores de las secciones correspondientes de filelog o de winlog previas. En el caso de valores no válidos en etiquetas u opciones `exclude_fields`, el agente extrae todos los datos válidos posibles y omite el resto del archivo una vez que encuentra los datos no válidos. Todas las anomalías aparecen en el archivo de registro del agente. Consulte el archivo de registro si se produce un comportamiento inesperado y repare todos los errores de los que informa el agente.

Si el agente detecta un valor no válido para una opción en una sección de filelog o winlog, no combina los valores de la opción de dicha sección con los correspondientes de las secciones comunes. Además, no habilita dicha sección. Todos los errores aparecen en un archivo de registro del agente. Consulte el archivo de registro si se produce un comportamiento inesperado y repare todos los errores de los que informa el agente.

Analizar registros

Los analizadores de registros del agente extraen datos estructurados de registros sin procesar antes de enviarlos al servidor de vRealize Log Insight. Con los analizadores de registros, vRealize

Log Insight puede analizar registros, extraer información de ellos y mostrar esos resultados en el servidor. Los analizadores de registros pueden configurarse para agentes de Windows y Linux de vRealize Log Insight.

Si se usa el protocolo de syslog, los campos extraídos por los analizadores forman parte de los DATOS ESTRUCTURADOS de acuerdo a RFC5424.

Configurar analizadores de registros

Puede configurar analizadores para recopiladores FileLog y WinLog.

Requisitos previos

Para el agente de Linux de vRealize Log Insight:

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

Para el agente de Windows de vRealize Log Insight:

- Inicie sesión en la máquina Windows donde instaló el agente de Windows de Log Insight e inicie el administrador de servicios para comprobar que esté instalado el servicio de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la carpeta que contiene 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 Abra el archivo `liagent.ini` en cualquier editor de texto.
- 3 Para configurar un analizador específico, defina una sección de analizador. `[parser | myparser]`

Donde `myparser` es un nombre arbitrario del analizador al que se puede consultar desde los orígenes de registro. La sección del analizador debe hacer referencia a cualquier analizador incorporado (o a cualquier otro definido). Configure las opciones obligatorias de ese analizador y las opciones no obligatorias si es necesario.

Por ejemplo, `base_parser=csv` muestra que el analizador `myparser` deriva del analizador integrado `csv`. Se espera que los registros de entrada consten de dos campos separados por punto y coma.

```
[parser|myparser]
```

```
base_parser=csv

fields=field_name1,field_name2

delimiter=";"
```

- 4 Después de definir `myparser`, consúltelo desde los orígenes de registro `winlog` o `filelog`.

```
[filelog|some_csv_logs]

directory=D:\Logs

include=*.txt;*.txt.*

parser=myparser
```

Los registros recopilados desde los orígenes `some_csv_logs`, por ejemplo desde el directorio `D:\Logs`, son analizados por `myparser` y los eventos extraídos aparecen en el servidor como `field_name1` y `field_name2` respectivamente.

Nota Los registros estáticos en el directorio `D:\Logs` no se extraen a vRealize Log Insight por el agente. Sin embargo, los archivos nuevos que se crean en el directorio `D:\Logs` están disponibles en vRealize Log Insight.

- 5 Guarde y cierre el archivo `liagent.ini`.

Opciones comunes para analizadores

Puede configurar opciones comunes para todos los analizadores que producen campos con nombres.

Palabras reservadas para nombres de campo

Los nombres de campos están restringidos. Los siguientes nombres están reservados y no se pueden utilizar como nombres de campo.

- `event_type`
- `hostname`
- `source`
- `text`

Opciones comunes del analizador

Las opciones de la siguiente tabla se pueden usar con todos los analizadores admitidos.

Opción	Descripción
<code>base_parser</code>	El nombre del analizador básico que amplía este analizador personalizado. Puede ser un nombre de analizador integrado u otro nombre de analizador personalizado. Esta clave de configuración es obligatoria.
<code>field_decoder</code>	<p>Los analizadores anidados se especifican como cadenas JSON. Las claves son los nombres del campo a los que se aplica el analizador anidado y el valor es el nombre del analizador que se utiliza para ese campo. Cada analizador anidado se aplica al campo correspondiente decodificado por el analizador básico. Los decodificadores de campo resultan útiles cuando el valor de un campo es un valor complejo; por ejemplo, una marca de tiempo. La opción field_decoder también admite más objetos JSON complejos como argumentos que permiten utilizar condiciones para valores de campos específicos que se comprueban antes de que se aplique el analizador anidado.</p> <p>Nota Para obtener más información sobre las configuraciones condicionales y de uso, consulte Configuraciones condicionales para la siguiente sección de la opción <code>field_decoder</code>.</p>
<code>field_rename</code>	Vuelve a nombrar campos extraídos. Use una cadena JSON donde las claves son los nombres originales de los campos y los valores son los nuevos nombres de dichos campos. La opción <code>field_decoder</code> se aplica siempre antes de <code>field_rename</code> . El orden de estas opciones en el archivo INI no tiene importancia. Para mayor claridad, especifique primero <code>field_decoder</code> .
<code>next_parser</code>	<p>Nombre del siguiente analizador que se debe ejecutar. Permite que múltiples analizadores se ejecuten secuencialmente en la misma entrada.</p> <p>Nota Los analizadores procesan a todos los analizadores resultantes definidos por la palabra clave <code>next_parser</code> y pueden reemplazar un valor de campo ya extraído por un analizador anterior.</p>

Opción	Descripción
<code>exclude_fields</code>	Una lista de nombres de campos separados por punto y coma que se deben eliminar del evento antes de entregarlo al servidor. Los nombres de los campos se eliminan antes de filtrar los eventos, de modo que el campo que se excluyó durante el análisis no se puede utilizar en la condición del filtro.
<code>debug</code>	<p>Opción Sí o No que permite la depuración de un analizador en particular. Con la depuración habilitada, el analizador realiza un registro detallado de las entradas que recibe, la operación que llevó a cabo y el resultado que produjo. La opción se aplica por sección, es decir, únicamente al analizador definido por una sección en particular.</p> <p>El valor predeterminado para la depuración es <code>debug=no</code> para analizadores.</p>

Configuraciones condicionales para la opción `field_decoder`

Para registros con el mismo formato común, pero con diferencias significativas relacionadas con valores de campos específicos, los registros con gravedades **info** y **error**, por ejemplo, pueden utilizar el analizador anidado condicional para reducir la aplicación de analizadores innecesarios a los campos correspondientes de los registros ya analizados.

Por ejemplo, en el uso de estos registros:

```
2019-03-29T11:00:54.858Z host-FQDN Hostd: error hostd[2099230] [Originator@6876 sub=Default
opID=1983bdbe-cl-800f user=admin.user] AdapterServer caught exception: SSLExceptionE(SSL
Exception: error:140000DB:SSL routines:SSL routines:short read: The connection was closed by
the remote end during handshake.)
```

```
2019-03-29T11:00:55.477Z host-FQDN Hostd: info hostd[6D620B70] ['commonhost' opID=5759adcc-
cf] [transportConnector] -- FINISH task-internal-5726666 -- -- Completed connection restart
--
```

Puede utilizar la siguiente configuración para analizarlas:

```
[parser|clf_parser]
base_parser=clf
format=%t %{generator_host}i %i: %{log_severity}i %i[%{thread_id}i]%M
field_decoder={"log_message" : {"log_severity" : {"error" : "error_parser", "info" :
"info_parser"}}}
exclude_fields=log_message

[parser|info_parser]
base_parser=clf
format=[%{common_info}i] [%{process}i] %M
field_rename={"log_message" : "info_log_content"}

[parser|error_parser]
base_parser=clfformat=[%{common_info}i] %{exception_handler}i %i:%{exception_type}i:%i:%
```



```
{error_id}i:%i:%i:%i: %M
field_rename={"log_message" : "exception_content"}
```

Esta configuración genera los siguientes resultados:

```
timestamp=2019-03-29T11:00:54.858000 generator_host="host-FQDN" log_severity="error"
thread_id="2099230" common_info=Originator@6876 sub=Default opID=1983bdbbe-c1-800f
user=admin.user exception_handler="AdapterServer" exception_type="SSLExceptionE(SSL
Exception" error_id="140000DB" exception_content="The connection was closed by the remote end
during handshake.)"
```

Además, se analizan los siguientes campos para el registro **info**:

```
timestamp=2019-03-29T11:00:55.477000 generator_host="host-FQDN" log_severity="info"
thread_id="6D620B70" log_message="['commonhost' opID=5759adcc-cf] [transportConnector]
-- FINISH task-internal-5726666 -- -- Completed connection restart --"
common_info="'commonhost' opID=5759adcc-cf" process="transportConnector" info_log_content="--
FINISH task-internal-5726666 -- -- Completed connection restart --"
```

Analizadores de registros de valores separados por comas

Puede configurar analizadores de valores separados por comas (Comma-Separated Value, CSV) para recopiladores `FileLog` y `WinLog`.

Las opciones disponibles para el analizador `csv` son `fields` y `delimiter`.

Opciones de analizadores de valores separados por comas

Tenga en cuenta la siguiente información acerca de la estructura del analizador de `csv`.

Opción	Descripción
<code>fields</code>	<p>La opción <code>fields</code> especifica los nombres de los campos que existen en el registro. La cantidad total de nombres de campos listados debe ser igual a la cantidad total de campos separados por comas en los registros.</p> <p>La opción <code>fields</code> es obligatoria para el analizador de CSV. Si no se especifica, no se analiza nada. Las comillas dobles que rodean el valor de campo son opcionales, y dependen del contenido del campo. Los nombres de campos deben estar separados por comas, por ejemplo</p> <pre>fields = field_name1, field_name2, field_name3, field_name4</pre> <p>Esta definición supone que los nombres <code>field_name1</code>, <code>field_name2</code>, <code>field_name3</code> y <code>field_name4</code> están asignados secuencialmente a los campos extraídos.</p> <p>Si el analizador de CSV debe omitir algunos campos, sus nombres se pueden omitir de la lista. Por ejemplo,</p> <pre>fields = field_name1, , field_name3, field_name4</pre> <p>En este caso, el analizador extrae únicamente los campos primero, tercero y cuarto del evento y posteriormente les asigna los nombres <code>field_name1</code>, <code>field_name3</code> y <code>field_name4</code>.</p> <p>Si la opción <code>fields</code> no especifica una lista completa de los campos en sus registros, el analizador devolverá una lista vacía. Por ejemplo, si el archivo de registro contiene <code>field1</code>, <code>field2</code>, <code>field3</code>, <code>field4</code> y <code>field5</code>, pero únicamente se especifica <code>fields= field1,field2,field3</code>, el analizador devuelve una lista de campos vacía.</p> <p>No puede usar <code>fields=*</code> para un analizador de CSV porque el analizador devuelve una lista de campos vacía. Se debe especificar una lista completa de los campos, a menos que necesite que determinados campos se omitan como ya se ha descrito.</p>
<code>delimiter</code>	<p>La opción <code>delimiter</code> especifica el delimitador que debe usar el analizador. De forma predeterminada, el analizador de <code>csv</code> usa una coma como delimitador; sin embargo, puede cambiar el delimitador por un punto y coma, un espacio u otro carácter especial. El delimitador definido debe estar encerrado entre comillas dobles.</p> <p>Por ejemplo, <code>delimiter=","</code> y <code>delimiter=";"</code>.</p> <p>El analizador de <code>csv</code> es compatible con cualquier conjunto de caracteres como delimitadores que se encuentran encerrados entre comillas (por ejemplo, <code>" "</code> o <code>"asd"</code>). Los separadores de valores de campos en los registros deben coincidir exactamente con el patrón definido por el parámetro de delimitador; de lo contrario, se producirá un error en el analizador.</p> <p>Pueden definirse caracteres especiales, como un espacio o un carácter de tabulación, como delimitadores para el analizador de <code>csv</code>, siempre que el carácter de escape esté antes del carácter especial para (<code>\</code>, <code>\s</code>, <code>\t</code>). Por ejemplo, <code>delimiter="\s"</code> o <code>delimiter=" "</code>.</p> <p>La opción <code>delimiter</code> es opcional.</p>

Configuración del analizador de registros CSV

Para analizar sintácticamente los registros de cualquiera de los dos orígenes, `winlog` o `filelog`, utilice la siguiente configuración.

```
[filelog|some_csv_logs]
directory=D:\Logs
include=*.txt;*.txt.*
parser=parser

[parser|parser]
```

```
base_parser = csv
fields = timestamp,field_name1, field_name2, field_name3
delimiter = ";"
field_decoder={"timestamp": "tsp_parser"}
[parser|tsp_parser]
; timestamp is a built-in parser
base_parser=timestamp
; "format" is an option of timestamp parser
format=%Y-%m-%d %H:%M:%S
```

Con esta configuración, los registros recopilados desde el origen `some_csv_logs`, por ejemplo desde el directorio `directory=D:\Logs`, son analizados sintácticamente por `myparser`. Si los registros recopilados contienen tres valores que están separados por punto y coma, los eventos analizados recibirán secuencialmente los nombres `field_name1`, `field_name2` y `field_name3`.

Para analizar el siguiente registro de CSV:

```
"United States","USA","North America","High income: OECD","Fiscal year end: September 30;
reporting period for national accounts data: CY."
```

Defina la configuración del analizador de CSV:

```
[parser|csv_log_parser]
base_parser=csv
fields=country_name, country_code, region, income_group, special_notes
```

El analizador de CSV devuelve los siguientes campos:

```
country_name=United States
country_code=USA
region=North America
income_group=High income: OECD
special_notes=Fiscal year end: September 30; reporting period for national accounts data: CY.
```

Analizador de registros del formato de registros comunes (Apache)

Puede configurar el analizador Apache de formato de registro común (Common Log Format, CLF) `FileLog` y `WinLog` los recopiladores.

Analizador de formato de registro común (Apache)

El analizador CLF predeterminado define el siguiente orden y nombres de campos.

```
host ident authuser datetime request statuscode bytes
```

Nombre de analizador: `clf`

La opción específica al analizador CLF es `format`.

Opción formato

La opción `format` especifica el formato con el que se generan los registros de Apache. La opción no es obligatoria.

Si no se especifica un formato, se usa el siguiente formato de registro común predeterminado.

```
%h %l %u %t \"%r\" %s %b
```

La cadena de formato del analizador CLF no acepta expresiones regex. Por ejemplo, especifique un espacio en lugar de la expresión `\s+`.

Para analizar otros formatos de registro, especifique el formato en la configuración del agente. Los campos analizados aparecen en el lado del servidor con los siguientes nombres.

Nota En los casos que requieren de una variable, si `{VARNAME}` no se proporciona en la configuración, los campos se ignoran.

Campos	Valor
'%a':	"remote_ip"
'%A':	"local_ip"
'%B', '%b':	"response_size"
'%C':	depende del nombre de la variable especificada en el formato
'%c':	depende del nombre de la variable especificada en el formato
'%D':	"request_time_mcs"
'%E':	"error_status"
'%e':	depende del nombre de la variable especificada en el formato
'%F', '%f':	"file_name"
'%h':	"remote_host"
'%H':	"request_protocol"
'%i':	depende del nombre de la variable especificada en el formato
'%k':	"keepalive_request_count"
'%l':	"remote_log_name"
'%L':	"request_log_id"
'%M':	"log_message" (el analizador detiene el análisis del registro de entradas después de alcanzar este especificador)
'%m':	"request_method"
'%n':	depende del nombre de la variable especificada en el formato
'%o':	depende del nombre de la variable especificada en el formato

Campos	Valor
'%p':	"Server_port". Se pueden usar formatos adicionales con este especificador: %{format}p. Los formatos compatibles son "canonical", "local" o "remote". Si se usa el formato "canonical", el nombre del campo sigue siendo "server_port". En caso de usar el formato "local", el nombre del campo cambiará a "local_server_port" y cuando se usa el formato "remote", el nombre del campo será "remote_server_port".
'%P':	"Process_id". Se pueden usar formatos adicionales con este especificador: %{format}P. Los formatos compatibles son "pid", "tid" y "hexid". Si se usa "pid" como formato, el nombre del campo será "process_id", mientras que los formatos "tid" y "hexid" generan campos con el nombre "thread_id".
'%q':	"query_string"
'%r':	"request"
'%R':	"response_handler"
'%s':	"status_code" que genera el estado final de la solicitud, también es compatible. Aparece en el servidor como "status_code".

Campos	Valor
'%t':	<p>"timestamp" funcionará como una marca de tiempo en el consumo y usa el analizador de marca de tiempo. Para anular la detección automática de la marca de tiempo, el formato de fecha y hora puede especificarse entre llaves: %{Y-%m-%d %H:%M:%S}t. Consulte Analizador de marca de tiempo para obtener más información.</p> <p>El formato de la marca de tiempo del analizador CLF puede comenzar con los prefijos "begin:" o "end:". Si el formato empieza con begin: (predeterminado), la hora se obtiene al comienzo del proceso de la solicitud. Si comienza con end:, se corresponde con la hora en que se escribió la entrada del registro, cerca del final del proceso de solicitud. Por ejemplo, el analizador CLF es compatible con formatos como los que se especifican a continuación: %h %l %u [%{begin:%d/%b/%Y %T}t.%{msec_frac}t] \"%r\" %>s %b</p> <p>Los siguientes tokens de formato también son compatibles con el especificador de formato de marca de tiempo del analizador CLF:</p> <p>sec</p> <p>número de segundos a partir de época. Es equivalente al especificador %s del analizador de la marca de tiempo.</p> <p>msec</p> <p>número de milisegundos a partir de época</p> <p>usec</p> <p>número de microsegundos a partir de época</p> <p>msec_frac</p> <p>fracción de milisegundo (es equivalente al especificador %f del analizador de la marca de tiempo)</p> <p>musec</p> <p>fracción de microsegundo (es equivalente al especificador %f del analizador de la marca de tiempo)</p> <p>Para analizar los registros donde la marca de tiempo se representa con tokens de formato, se pueden utilizar los siguientes formatos en la configuración:</p> <pre>format=%h %l %u %{sec}t \"%r\" %s %b format=%h %l %u %{msec}t \"%r\" %s %b format=%h %l %u %{usec}t \"%r\" %s %b</pre> <p>Estos tokens no se pueden combinar unos con otros o con el analizador de la marca de tiempo que se encuentren en la misma cadena de formato. En su lugar, puede usar varios tokens %{format}t. Por ejemplo, para usar la marca de tiempo que incluye milisegundos, excepto al usar el especificador %f del analizador de la marca de tiempo, se pueden usar las siguientes marcas de tiempo combinadas: %{d/%b/%Y %T}t.%{msec_frac}t .</p>
'%T':	"request_time_sec"
'%u':	"remote_auth_user"
'%U':	"requested_url"
'%v':	"server_name"

Campos	Valor
'%V':	"self_referential_server_name"
'%X':	"connection_status" depende del nombre de la variable especificada en el formato
'%x':	depende del nombre de la variable especificada en el formato
'%I':	"received_bytes"
'%O':	"sent_bytes"
'%S':	"transferred_size"

Por ejemplo, para analizar registros desde orígenes winlog o filelog con el analizador CLF, especifique la siguiente configuración:

```
[filelog|clfflogs]
directory=D:\Logs
include=*.txt
parser=myclf

[parser|myclf]
debug=yes ;Note: use this option only while debugging and set it to 'no' when used in
production.
base_parser=clf
format=%h %l %u %b %t \"%r\" %s
```

Mediante esta configuración, los registros que se recopilan desde el origen clfflogs, por ejemplo desde el directorio directory=D:\Logs, son analizados sintácticamente por myclf. El analizador myclf analiza únicamente aquellos registros que se generaron con el formato que se describe en la configuración.

El valor predeterminado para la depuración es debug=no para analizadores.

Analizar registros generados mediante CLF

Para analizar sintácticamente los registros que se generaron mediante CLF, deberá definir el formato correspondiente en la configuración. Por ejemplo,

```
format=%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User_Agent}i\"
```

Los campos que no están vacíos y que utilizan los especificadores %{Referer}i y %{User_Agent}i aparecen en el servidor vRealize Log Insight con los nombres referer y user_agent, respectivamente.

Integrar el analizador de marca de tiempo con el analizador de CLF

Puede analizar sintácticamente los registros Apache con un formato de hora personalizado.

Acceda a los registro con formato de hora personalizado de la siguiente manera.

```
format = %h %l %u %{%a, %d %b %Y %H:%M:%S}t \"%r\" %>s %b
```

Si no se especifica una hora personalizada, el analizador de CLF intenta deducir automáticamente el formato de hora ejecutando el analizador de marca de tiempo; de lo contrario, se utiliza el formato de hora personalizado.

Los formatos de hora personalizados compatibles que se admiten para registros de error son:

Formato de hora personalizado	Descripción	Formato de configuración
%{u}t	Hora actual incluidos microsegundos	format=[%{u}t] [%l] [pid %P] [client %a] %M
%{cu}t	Hora actual en formato ISO 8601 compacto, incluidos microsegundos	format=[%{cu}t] [%l] [pid %P] [client %a] %M

Para obtener una lista completa de los especificadores de marca de tiempo compatibles, consulte [Analizador de marca de tiempo](#).

Ejemplo: Configuración de registros de acceso predeterminados Apache para Windows

Ejemplo: Configuración de registros de error predeterminados Apache para Windows

Este ejemplo muestra el modo en que se pueden formatear las configuraciones de los registros de acceso Apache v2.4 para Windows.

```
;ACCESS LOG
;127.0.0.1 - - [13/May/2015:14:44:05 +0400] "GET /xampp/navi.php HTTP/1.1" 200 4023 "http://localhost/xampp/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0"
;format=%h %l %u %{d/%b/%Y:%H:%M:%S %z}t \"%r\" %>s %b \"%{Referer}i\" \"%{User_agent}i\"

; Section to collect Apache ACCESS logs
[filelog|clflogs-access]
    directory=C:\xampp\apache\logs
    include=acc*
    parser=clfparsed_apache_access
    enabled=yes

;Parser to parse Apache ACCESS logs
[parser|clfparsed_apache_access]
    debug=yes
    base_parser=clf
    format=%h %l %u %{d/%b/%Y:%H:%M:%S %z}t \"%r\" %>s %b \"%{Referer}i\" \"%{User_agent}i\"
```

Defina el formato de registro de acceso:

1 Configure Apache para el formato de registro de acceso (httpd.conf):

```
LogFormat "%h %l %u %{d-%b-%Y:%H:%M:%S}t \"%r\" %a %A %e %k %l %L %m %n %T %v %V %>s %b \"%{Referer}i\" \"%{User-Agent}i\" combined
```

2 Defina la configuración del analizador de CLF:

```
;ACCESS LOG
;127.0.0.1 unknown - 21-May-2015:13:59:35 "GET /xampp/navi.php HTTP/1.1" 127.0.0.1 127.0.0.1
- 0 unknown - GET - 1 localhost localhost 200 4023 "http://localhost/xampp/" "-"
```



```
[filelog|clfflogs-access]
    directory=C:\xampp\apache\logs
    include=acc*,_myAcc*
    parser=clfparsed_apache_access
    enabled=yes
; Parser to parse Apache ACCESS logs
[parser|clfparsed_apache_access]
    debug=yes
    base_parser=clf
    format=%h %l %u {%d-%b-%Y:%H:%M:%S}t \"%r\" %a %A %e %k %l %L %m %n %T %v %V %>s %b \"%
{Referer}i\" \"%{User-Agent}i\"
```

El analizador de CLF devuelve lo siguiente:

```
remote_host=127.0.0.1
timestamp=2015-05-13T10:44:05
request=GET /xampp/navi.php HTTP/1.1
status_code=200
response_size=4023
referer=http://localhost/xampp/
user_agent=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0
```

Este ejemplo muestra el modo en que se pueden formatear las configuraciones de los registros de error Apache v2.4 para Windows.

```
;ERROR LOG
;[Wed May 13 14:37:17.042371 2015] [mpm_winnt:notice] [pid 4488:tid 272] AH00354: Child:
Starting 150 worker threads.
;[Wed May 13 14:37:27.042371 2015] [mpm_winnt:notice] [pid 5288] AH00418: Parent: Created
child process 3480
;format=[%{a} %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P:tid %t{thread_id}i] %E: %M
;format=[%{a} %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P] %E: %M

; Section to collect Apache ERROR logs
[filelog|clfflogs-error]
    directory=C:\xampp\apache\logs
    include=err*
    parser=clfparsed_apache_error
    enabled=yes

;Parser to parse Apache ERROR logs
[parser|clfparsed_apache_error]
    debug=yes
    base_parser=clf
    format=[%{a} %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P:tid %t{thread_id}i] %E: %M
    next_parser=clfparsed_apache_error2

;Parser to parse Apache ERROR logs
[parser|clfparsed_apache_error2]
    debug=yes
```

```
base_parser=clf
format=[%{a %b %d %H:%M:%S%f %Y)t] [%m:%{severity}i] [pid %P] %E: %M
```

Nota Los nombres proporcionados corresponden al formato de registro combinado. Los registros de error Apache también se describen usando las claves de formateo anteriores, no el formato de registro de error Apache.

Defina el formato de registro de error:

1 Configure Apache para el formato de registro de error (httpd.conf):

```
LogFormat "%h %l %u %{d-%b-%Y:%H:%M:%S}t \"%r\" %a %A %e %k %l %L %m %n %T %v %V %>s %b\n\"%{Referer}i\" \"%{User-Agent}i\" combined
```

2 Defina la configuración del analizador de CLF:

```
;Parser to parse Apache ERROR logs
[parser|clfparsed_apache_error]
  debug=yes
  base_parser=clf
  format=[%{a} %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P] %E: %M
  next_parser=clfparsed_apache_error2

;Parser to parse Apache ERROR logs
[parser|clfparsed_apache_error2]
  debug=yes
  base_parser=clf
  format=[%{a} %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P:tid %{thread_id}i] %E: %M
```

Entrada de registro:

```
[Wed May 13 14:37:17.042371 2015] [mpm_winnt:notice] [pid 4488:tid 272] AH00354: Child:
Starting 150 worker threads.
```

El analizador de CLF devuelve los siguientes campos para la entrada de registro (si utiliza un analizador en una zona horaria +0400):

```
timestamp=2015-05-13T10:37:17.042371
request_method=mpm_winnt
severity=notice
process_id=4488
thread_id=272
error_status=AH00354
log_message=Child: Starting 150 worker threads.
```

Entrada de registro:

```
[Wed May 13 14:37:27.042371 2015] [mpm_winnt:notice] [pid 5288] AH00418: Parent: Created
child process 3480
```

El analizador de CLF devuelve los siguientes campos para la entrada de registro (si utiliza un analizador en una zona horaria +0400):

```
timestamp=2015-05-13T10:37:27.042371
request_method=mpm_winnt
severity=notice
process_id=5288
error_status=AH00418
log_message=Parent: Created child process 3480
```

Analizador de par de clave/valor

Puede configurar el analizador de par de clave/valor (KVP) para recopiladores de FileLog y WinLog.

Analizador de par de clave/valor (KVP)

El analizador de `kvp` busca y extrae todas las coincidencias de `key=value` de un texto de mensaje de registro arbitrario. El siguiente ejemplo muestra el formato del analizador de `kvp`.

```
[parser|kvp_parser]
base_parser=kvp
fields=*
```

Por ejemplo, el registro de clave-valor puede estar en el siguiente formato: `scope=local;`
`abstract=false;` `lazyInit=false;` `autowireMode=0;` `dependencyCheck=0;`

Con el analizador de `kvp`, debe especificar los campos de los que se deben extraer los valores. Por ejemplo, si la definición `fields=name,lastname,country` existe en la configuración, solo se analizan los valores con las claves especificadas y se envían al servidor.

Opcionalmente, tanto la clave como el valor pueden rodearse por comillas dobles “ ” para definir espacios en blanco u otros caracteres especiales.

Cuando se usan comillas dobles para la clave o el valor, se puede usar una barra invertida “ \ ” como carácter de escape. Cualquier carácter que aparece a continuación de la barra invertida se define literalmente, incluidos los caracteres de comillas dobles o barra invertida. Por ejemplo: “ \\ ”

Tenga en cuenta las siguientes consideraciones.

- Si la clave en un par de clave/valor no está seguida por un signo igual y no se proporciona `VALUE`, la opción se omite, al igual que con texto libre.
- La clave no puede estar vacía; el valor puede estar vacío.
- Un signo igual no seguido por un valor se trata como texto libre y se omite.
- Un valor puede ser una cadena de caracteres rodeada por caracteres de comillas dobles, o puede estar vacía. Use una barra invertida para escapar caracteres especiales que forman parte del valor.

Opciones del analizador de KVP

Tenga en cuenta la siguiente información sobre la estructura del analizador de `kvp`.

Opción	Descripción
<code>fields</code>	<p>La información que desea extraer, descrita como unidades de datos. Por ejemplo, <code>fields=name,lastname,country</code>.</p> <p>Si los nombres de campos específicos se definen mediante la opción <code>fields</code>, cada carácter no válido en el nombre de un campo extraído de un registro se reemplaza con un guion bajo. Por ejemplo, si la opción <code>fields</code> busca los campos "x-A" y "a*(X+Y)", el analizador extrae estos campos de los registros y les asigna los nombres "x_a" y "a__x_y", respectivamente. Esto permite extraer campos que contengan cualquier carácter en el nombre.</p> <p>Si se especifica la opción <code>fields</code> como <code>"*"</code>, el analizador de <code>kvp</code> reconoce pares campo/valor automáticamente. Por tanto, busca campos que tengan solo caracteres "alfanuméricos + guion bajo" (compatibles con el servidor de LI). En lugar de convertir el resto de caracteres no válidos en guiones bajos, estos se eliminan. De esta forma, se impide que el analizador extraiga información innecesaria y la aplique a los campos estáticos.</p>
<code>delimiter</code>	<p>Opcional.</p> <p>Los delimitadores predeterminados son el carácter de espacio, el carácter de tabulación, los caracteres de líneas nuevas, la coma y los caracteres de punto y coma.</p> <p>Si no se especifican delimitadores en la configuración, el analizador de <code>kvp</code> usa los predeterminados para el análisis.</p> <p>Para cambiar los delimitadores predeterminados por delimitadores específicos, deberá definirlos entre comillas dobles. Por ejemplo: <code>delimiter = "#^ "</code>. Esta definición implica que cada uno de los caracteres entre comillas dobles se usa como delimitador. El analizador de <code>kvp</code> puede considerar cada carácter como delimitador. Puede incluir los delimitadores predeterminados junto con otros en la definición.</p> <p>Por ejemplo, la instrucción <code>delimiter = "#^ \t\r\n\s"</code> incluye el carácter de tabulación, los caracteres de líneas nuevas y el espacio como delimitadores. Si se usan estos caracteres, deben estar precedidos por el carácter de escape. Por ejemplo, para definir el carácter de espacio como delimitador, introduzca el carácter de escape <code>"\"</code> antes del carácter de espacio al definirlo como delimitador (por ejemplo, <code>delimiter="\s"</code>).</p>
<code>field_decoder</code>	<p>Los analizadores anidados se especifican como una cadena JSON en donde las claves son los nombres del campo para aplicar al analizador anidado, y el valor es el nombre del analizador para usar para ese campo.</p> <p>Cada analizador anidado se aplica al campo adecuado, tal como se decodifica por el analizador base.</p> <p>Los decodificadores de campo son útiles cuando el valor de un par clave-valor es un valor complejo, tal como una marca de tiempo y una lista separada por comas.</p>
<code>debug =</code>	<p>Opcional. El valor de <code>debug</code> = puede ser <code>yes</code> o <code>no</code>. El valor predeterminado para la depuración es <code>debug=no</code> para analizadores.</p> <p>Cuando se establece la opción en <code>yes</code>, puede ver registros detallados del consumo del analizador en <code>liagent_<date>.log</code>.</p>

Opciones adicionales de clave y valor

Clave	Definición
KVP_MESSAGE = * (MESSAGE_ENTRY [WSPR])	Una lista de entradas de mensajes separadas por un espacio en blanco opcional
MESSAGE_ENTRY = KVP / FREE_TEXT	La entrada es un par de clave/valor o simplemente una cadena de texto libre
KVP = KEY ["=" VALUE]	Par de clave/valor. Si la CLAVE no va seguida por un signo igual y VALOR, se omite como una cadena de texto libre.
KEY = BARE_KEY / QUOTED_KEY	
FREE_TEXT = "="	Un signo igual libre es considerado como una cadena de texto libre y se omite.
BARE_KEY = *1BARE_KEY_CHAR	Al menos un carácter
BARE_KEY_CHAR = %0x00-08 / %0x10-19 / %0x21-3C / %3E-%FF	Cualquier carácter, excepto un signo igual, un espacio o un carácter de tabulación
QUOTED_KEY = 0x22 *1(QUOTED_STRING_CHAR / "\" CHAR) 0x22	Al menos un carácter rodeado por caracteres de comillas dobles. La barra invertida se usa como un carácter de escape.
QUOTED_STRING_CHAR = %0x00-21 / %0x23-FF	Cualquier carácter, excepto las comillas dobles
VALUE = BARE_VALUE / QUOTED_VALUE	
BARE_VALUE = *BARE_VALUE_CHAR	Cero o más caracteres
BARE_VALUE_CHAR = %0x00-08 / %0x10-19 / %0x21-FF	Cualquier carácter, excepto un espacio o un carácter de tabulación
QUOTED_VALUE = 0x22 * (QUOTED_STRING_CHAR / "\" CHAR) 0x22	Una cadena de caracteres rodeada por caracteres de comillas dobles. Esta cadena puede estar vacía. La barra invertida se usa como un carácter de escape.

Ejemplos de configuración de analizadores de KVP

Puede usar `fields=*` para analizar todos los campos, si es necesario.

```
[parser|simple_kv]
base_parser =kvp
fields=*
```

Este ejemplo muestra como especificar el decodificador de campo.

```
[parser|mykvp]
debug=no
base_parser=kvp
delimiter="#"^|"
fields=*
;OR fields=scope,abstract,lazyInit,autowireMode,dependencyCheck
field_decoder={"field1":"field1_parser1"}

[parser|field1_parser1]
base_parser=clf
```

```
format=[%{value1}i]]
field_decoder={"value1":"field_parser2"}
```

Para analizar el siguiente registro de KVP:

```
Configuring transport... proto = cfapi server_hostname = LOCALHOST ssl = no port = 9000
reconnect = 30
```

Defina la configuración del analizador de KVP:

```
[parser|kvp_log_parser]
base_parser=kvp
fields=*
```

El analizador de KVP devuelve los siguientes campos:

```
proto=cfapi
server_hostname=LOCALHOST
ssl=no
port=9000
reconnect=30
```

Ejemplo: Ejemplos de analizadores de KVP simples y complejos

Ejemplo de analizador de KVP simple

```
[filelog|MyLog]
directory=C:\<folder_name>\Parser_logs
include=*.log
parser=my_KVP_parser

[parser|my_KVP_parser]
base_parser=kvp
fields=*
```

Ejemplo de analizador de KVP complejo

```
[filelog|MyLog]
directory=C:\<folder_name>\Parser_logs
include=*.log
parser=my_KVP_parser

[parser|my_KVP_parser]
base_parser=kvp
fields=*
field_decoder={"field1":" field1_parser1"}

[parser| field1_parser1]
base_parser=clf
format=[%{value1}i]]
field_decoder={"value1":" field1_parser2"}
```

Analizador de marca de tiempo

El analizador `timestamp` no genera campos, sino que transforma su entrada de una cadena a un formato de marca de tiempo interna que se muestra en milisegundos desde el inicio de época UNIX, 1 de enero de 1970 (medianoche UTC/GMT).

La única opción de configuración admitida es `format`. Por ejemplo, `format=%Y-%m-%d %H:%M:%S`.

A diferencia del analizador CLF, el analizador de `timestamp` puede analizar el tiempo cuando no hay delimitadores entre los especificadores; por ejemplo `%A%B%d%H%M%S%Yz`.

Los especificadores de formato que utiliza el analizador `timestamp` son los siguientes:

```
'%a':    Abbreviated weekday name, for example: Thu
'%A':    Full weekday name, for example: Thursday
'%b':    Abbreviated month name, for example: Aug
'%B':    Full month name, for example: August
'%d':    Day of the month, for example: 23. strftime() expects zero-padded (01-31) digits
          for this specifier but Log Insight agents can parse space-padded and non-padded
          day numbers, too.
'%e':    Day of the month, for example: 13. strftime() expects space-padded ( 1-31) digits
          for this specifier but Log Insight agents can parse zero-padded and non-padded
          day numbers too.
'%f':    Fractional seconds of time, for example: .036 'f' specifier assumes that '.' or ','
          character should exist before fractional seconds and there is no need to mention
          that character in the format. If none of these characters precedes fractional
seconds,
          timestamp wouldn't be parsed.
'%H':    Hour in 24h format (00-23), for example: 14. Zero-padded, space-padded, and non-
padded hours
          are supported.
'%I':    Hour in 12h format (01-12), for example: 02. Zero-padded, space-padded and non-
padded hours
          are supported.
'%m':    Month as a decimal number (01-12), for example: 08. Zero-padded, space-padded
and non-padded month numbers are supported.
'%M':    Minute (00-59), for example: 55
'%p':    AM or PM designation, for example: PM
'%S':    Second (00-61), for example: 02
'%s':    Total number of seconds from the UNIX epoch start, for example 1457940799
          (represents '2016-03-14T07:33:19' timestamp)
'%Y':    Year, for example: 2001
'%z':    ISO 8601 offset from UTC in timezone (1 minute=1, 1 hour=100)., for example: +100
```

El analizador de marca de tiempo acepta especificadores adicionales, pero sus valores se ignoran y no afectan la hora analizada.

```
'%C':    Year divided by 100 and truncated to integer (00-99), for example: 20
'%g':    Week-based year, last two digits (00-99), for example, 01
'%G':    Week-based year, for example, 2001
'%j':    Day of the year (001-366), for example: 235
'%u':    ISO 8601 weekday as number with Monday as 1 (1-7), for example: 4
'%U':    Week number with the first Sunday as the first day of week one (00-53), for example:
33
```



```
'%V':    ISO 8601 week number (00-53), for example: 34
'%w':    Weekday as a decimal number with Sunday as 0 (0-6), for example: 4
'%W':    Week number with the first Monday as the first day of week one (00-53), for example:
34
'%y':    Year, last two digits (00-99), for example: 01
```

Si no se define un parámetro `format`, el analizador `Timestamp` analiza las marcas de tiempo usando los formatos predeterminados.

Analizador automático de marcas de tiempo

El analizador automático de la marca de tiempo se utiliza cuando no hay formato definido para el analizador de marca de tiempo o se puede invocar el analizador directamente sin definir la marca de tiempo usando `timestamp` en `field_decoder`. Por ejemplo:

```
[parser|mycsv]
base_parser=csv
debug=yes
fields=timestamp,action,source_id,dest
field_decoder={"timestamp": "timestamp"}
```

Ejemplo: Un analizador de marca de tiempo con la configuración predeterminada

Este ejemplo muestra un analizador `timestamp` con una configuración predeterminada.

```
[parser|tsp_parser]
base_parser=timestamp
debug=no
format=%Y-%m-%d %H:%M:%S%f
```

Para integrar un analizador `timestamp` con otros analizadores, por ejemplo el analizador CSV, especifique la siguiente configuración.

```
[parser|mycsv]
base_parser=csv
fields=timestamp,action,source_id,dest
field_decoder={"timestamp": "tsp_parser"}
```

Cuando se define esta configuración, el analizador `mycsv` extrae los campos con los nombres que se especifican en la configuración y ejecuta `tsp_parser` en el contenido del campo `timestamp`. Si `tsp_parser` recupera una marca de tiempo válida, el servidor utiliza esa marca de tiempo para el mensaje del registro.

Analizador de registros automático

El analizador automático detecta de manera automática la marca de tiempo dentro de los primeros 200 caracteres de una línea. El formato de las marcas de tiempo detectadas automáticamente es el mismo que para el analizador de `timestamp`.

El analizador automático no cuenta con opciones. Además de detectar automáticamente la marca de tiempo, el analizador de clave/valor se ejecuta en la entrada de los registros, detecta automáticamente los pares de clave/valor existentes en los registros, y extrae los campos en consecuencia. Por ejemplo,

```
[filelog|some_logs]
directory=/var/log
include=*
parser=auto
```

Como con otros analizadores, puede definir una acción aparte para el analizador automático.

```
[filelog|kvplogs]
directory=C:\temp_logs\csv-itbm
include=*.txt
parser=myauto
[parser|myauto]

base_parser=auto
debug=yes
```

Si tiene `debug` habilitado para el analizador automático, se imprime la información adicional acerca del análisis. Por ejemplo, la información sobre en qué registro se ejecutó el analizador automático y qué campos se extrajeron del registro.

El valor predeterminado para la depuración es `debug=no` para analizadores.

Analizador Syslog

El analizador syslog admite las opciones `message_decoder` y `extract_sd`, y detecta automáticamente dos formatos: RFC-6587, RFC-5424 y RFC-3164.

Configurar la opción `message_decoder`

Todas las opciones comunes y la opción `message_decoder` están disponibles para el analizador syslog. De forma predeterminada, solo se extraen los campos `timestamp` y `appname`. Habilite la opción `message_decoder`. Para ello, defina los valores de configuración del archivo `liagent.ini` para que sean similares a los del siguiente ejemplo:

```
[filelog|data_logs]
directory=D:\Logs
include=*.txt
parser=mysyslog

[parser|mysyslog]
base_parser=syslog
message_decoder=syslog_message_decoder
debug=yes

[parser|syslog_message_decoder]
base_parser=kvp
fields=*
```

Ejemplo: Analizar con la opción message_decoder

El siguiente ejemplo incluye un evento de muestra y los campos que un analizador syslog configurado para utilizar la opción message_decoder le agrega:

- Evento de ejemplo:

```
2015-09-09 13:38:31.619407 +0400 smith01 john: Fri Dec 5 08:58:26 2014 [pid 26123]
[jsmith.net] status_code=FAIL oper_
ation=LOGIN: Client "176.31.17.46"
```

- Devuelto por un analizador syslog al que se le aplica la opción message_decoder para ejecutar un analizador de KVP:

```
timestamp=2015-09-09T09:38:31.619407 appname=john status_code=FAIL operation=LOGIN:
```

Configurar la opción extract_sd para analizar datos estructurados

Para analizar datos estructurados, habilite la opción extract_sd. Para ello, defina los valores de configuración del archivo liagent.ini para que sean similares a los del siguiente ejemplo:

```
[filelog|simple_logs]
directory=/var/log
include=*.txt
parser=syslog_parser

[parser|syslog_parser]
base_parser=syslog
extract_sd=yes
```

Ejemplo: Analizar con la opción extract_sd

El siguiente ejemplo incluye un evento de muestra y los campos que un analizador syslog configurado para utilizar la opción extract_sd le agrega:

- Evento de ejemplo: <165>1 2017-01-24T09:17:15.719Z localhost evntslog
 - ID47 [exampleSDID@32473 iut="3" eventSource="Application" eventID="1011"] [examplePriority@32473 class="high"] Found entity IPSet, display name dummy ip set 1411
- El analizador syslog agrega los siguientes campos al evento:

```
timestamp=2017-01-24T09:17:15.719000
pri_facility=20
pri_severity=5
procid="-"
msgid="ID47"
iut="3"
eventsource="Application"
eventid="1011"
class="high"
appname="evntslog"
```

Campos extraídos por el analizador

El analizador extrae automáticamente los siguientes campos de un evento:

Clasificación de RFC	pri_facility	pri_severity	timestamp	appname	procid	msgid
Sin RFC			X	X		
RFC-3164	X	X	X	X		
RFC-5424	X	X	X	X	X	X

Opciones del analizador syslog

La siguiente tabla describe las opciones de syslog disponibles.

Opción	Descripción
message_decoder	Define un analizador adicional, que se utiliza para analizar el cuerpo del mensaje de un evento. Puede ser un analizador integrado, ya sea automático o personalizado.
extract_sd	Analiza datos estructurados. La opción extract_sd option solo admite los valores yes o no. Está deshabilitada de forma predeterminada. Cuando se habilita la opción extract_sd, simplemente extrae todos los pares clave-valor de los datos estructurados.

Ejemplo: Analizar el estándar RFC-5424

Los siguientes ejemplos muestran dos eventos analizados por una instancia de syslog configurada. Se incluye la configuración utilizada para el recopilador, un evento de muestra y los campos que le agrega el analizador syslog.

■ Configuración:

```
[filelog|simple_logs]
directory=/var/log
include=*.txt
parser=syslog
```

■ Un evento generado en el archivo supervisado:

```
<165>1 2017-01-24T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
[junos@2636.1.1.1.2.18 username=\"regress\"] User 'regress' exiting configuration
mode - Juniper format
```

■ Campos que el analizador syslog agrega al evento:

```
The following fields will be added to the event by Syslog parser:
timestamp=2017-01-24T09:17:15.719000
pri_facility = 20
pri_severity = 5
```

```

procid = 3046
msgid = UI_DBASE_LOGOUT_EVENT
appname = mgd

```

Ejemplo: Analizar el estándar RFC-3164

El siguiente ejemplo muestra la configuración utilizada para el recopilador, un evento de RFC-3164 de muestra y los campos que syslog agrega al evento.

- Configuración:

```

[filelog|simple_logs]
directory=/var/log
include=*.txt
parser=syslog

```

- Un evento de RFC-3164 generado en el archivo supervisado:

```

<13>2017-01-24T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT User 'regress' exiting
configuration mode - Juniper format

```

- Campos que el analizador syslog agrega al evento:

```

timestamp=2017-01-24T09:17:15.719000
pri_facility=1
pri_severity=5
appname="mgd"

```

Analizador de valores separados por tabulaciones etiquetados

El formato Valores separados por tabulaciones etiquetados (LTSV) es una variante de Valores separados por tabulaciones (TSV).

Cada registro en un archivo LTSV está representado como una línea única. Cada campo está separado por <TAB> y tiene una etiqueta y un valor. La etiqueta y el valor están separados por :. Con el formato LTSV, puede analizar cada línea dividiendo la línea con <TAB> (al igual que el formato TSV) y extender los campos con etiquetas únicas sin un orden específico. Para obtener más información sobre la definición y el formato LTSV, consulte <http://ltsv.org/>.

Ejemplo: Configuración del analizador de LTSV

Ejemplo: Registro de LTSV de ejemplo

El analizador de LTSV no requiere opciones de configuración específicas. Para usar el analizador de LTSV, especifique el nombre del analizador de `ltsv` integrado en la configuración.

```

[parser|myltsv]
base_parser=ltsv

```

Un archivo de LTSV debe ser una secuencia de bytes que coincida con la producción de LTSV en el formato ABNF.

```
ltsv = *(record NL) [record]
record = [field *(TAB field)]
field = label ":" field-value
label = 1*1byte
field-value = *fbyte

TAB = %x09
NL = [%x0D] %x0A
lbyte = %x30-39 / %x41-5A / %x61-7A / "_" / "." / "-" ;; [0-9A-Za-z_.-]
fbyte = %x01-08 / %x0B / %x0C / %x0E-FF
```

```
host:127.0.0.1<TAB>ident:--<TAB>user:frank<TAB>time:[10/Oct/2000:13:55:36 -0700]<TAB>req:GET /
apache_pb.gif HTTP/1.0<TAB>status:200<TAB>size:2326<TAB>referer:http://www.example.com/
start.html<TAB>ua:Mozilla/4.08 [en] (Win98; I ;Nav)
```

Con la configuración de LTSV de ejemplo, el análisis del registro debe devolver los campos siguientes:

```
host=127.0.0.1
ident=--
user=frank
time=[10/Oct/2000:13:55:36 -0700]
req=GET /apache_pb.gif HTTP/1.0
status=200
size=2326
referer=http://www.example.com/start.html
ua=Mozilla/4.08 [en] (Win98; I ;Nav)
```

Configuración de depuración

La depuración adicional también está disponible para el analizador de LTSV. De forma predeterminada, la depuración de LTSV está deshabilitada. Para activar la depuración de LTSV, introduzca `debug=yes`.

```
[parser|myltsv]
base_parser=ltsv
debug=yes
```

Cuando la depuración está activada, el analizador de LTSV extrae los valores de todas las etiquetas válidas del registro. El analizador de LTSV requiere que los nombres de etiquetas comprendan solo caracteres alfanuméricos, el guion bajo ('_'), punto('.') y guion ('-'). Si existe al menos un nombre de etiqueta no válido en el registro, su análisis fallará. Incluso si el nombre de la etiqueta es válido, el agente comprobará el nombre del campo. Si existen nombres no válidos, el nombre de la etiqueta debe corregirse por un nombre de campo válido.

Configurar el analizador de LTSV desde la sección `filelog`

También puede configurar el analizador de LTSV directamente desde la sección `filelog`.

```
[filelog|simple_logs]
directory=/var/log
include=*
parser=ltsv
```

Analizador de regex

El analizador de `regex` permite el uso de algunas expresiones regulares en datos recopilados.

Los agentes de vRealize Log Insight usan la expresión regular de biblioteca Boost de C++, que utiliza la sintaxis Perl. El analizador de `regex` se puede definir especificando un patrón de una expresión regular que contenga grupos de captura con nombre. Por ejemplo: `(?<campo_1>\d{4}) [-] (?<campo_2>\d{4}) [-] (?<campo_3>\d{4}) [-] (?<campo_4>\d{4})`

Los nombres especificados en los grupos (por ejemplo: `campo_1`, `campo_2`, `campo_3` y `campo_4`) se convierten en los nombres de los campos extraídos correspondientes. Los nombres tienen los siguientes requisitos:

- Los nombres especificados en el patrón de expresión regular deben ser nombres de campos válidos para vRealize Log Insight.
- Los nombres deben contener solamente caracteres alfanuméricos y el carácter de guion bajo `"_"`.
- El nombre no puede comenzar con un carácter digital.

Si se proporcionan nombres no válidos, se produce un error en la configuración.

Opciones del analizador de regex

La única opción requerida para el analizador de `regex` es la opción `format`.

Se puede usar la opción `debug` si se requiere información de depuración adicional.

Configuración

Para crear un analizador de `regex`, utilice `regex` como `base_parser` y proporcione la opción `format`.

Ejemplo: Ejemplos de configuración de regex

Ejemplo: Ejemplo de análisis de registros de Apache

El siguiente ejemplo se puede usar para analizar `1234-5678-9123-4567`:

```
[parser|regex_parser]
base_parser=regex
format=(?<tag1>\d{4}) [-] (?<tag2>\d{4}) [-] (?<tag3>\d{4}) [-] (?<tag4>\d{4})
[filelog|some_info]
directory=D:\Logs
```

```
include=*.txt
parser=regex_parser
```

Los resultados son los siguientes:

```
tag1=1234
tag2=5678
tag3=9123
tag4=4567
```

Para analizar registros de Apache con el analizador de `regex`, proporcione el formato de `regex` específico para los registros de Apache:

```
[parser|regex_parser]
base_parser=regex
format=(?<remote_host>.*) (?<remote_log_name>.*) (?<remote_auth_user>.*) \[(?<log_timestamp>.*)\] "(?<request>.*) " (?<status_code>.*) (?<response_size>.)
```

Los resultados son los siguientes:

```
127.0.0.1 - admin [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
remote_host=127.0.0.1
remote_log_name=-
remote_auth_user=admin
log_timestamp=10/Oct/2000:13:55:36 -0700
request=GET /apache_pb.gif HTTP/1.0
status_code=200
response_size=2326
```

El siguiente código muestra otro ejemplo de análisis de registros Apache.

```
[parser|regex_parser]
base_parser=regex
format=(?<remote_host>.* (?<remote_log_name>.*)) (?<remote_auth_user>.*) \[(?<log_timestamp>.*)\] "(?<request>.* (?<resource>.*) (?<protocol>.*))" (?<status_code>.*) (?<response_size>.*)
127.0.0.1 unknown - [17/Nov/2015:15:17:54 +0400] "\"GET /index.php HTTP/1.1\" 200 4868
remote_host=127.0.0.1 unknown
remote_log_name=unknown
remote_auth_user=-
log_timestamp=17/Nov/2015:15:17:54 +0400
request=GET /index.php HTTP/1.1
resource=/index.php
protocol=HTTP/1.1
status_code=200
response_size=4868
```

Consideraciones sobre rendimiento

El analizador de `regex` consume más recursos que otros analizadores como el analizador de `CLF`. Si puede analizar registros con otros analizadores, para obtener un mejor rendimiento, considere la posibilidad de utilizar esos analizadores en lugar del analizador de `regex`.

Si no se proporciona un analizador y utiliza el analizador de `regex`, defina los formatos de la manera más clara posible. El siguiente ejemplo muestra una configuración que proporciona mejores resultados de rendimiento. Este ejemplo especifica campos que poseen valores digitales.

```
(?<remote_host>\d+\.\d+\.\d+\.\d+) (?<remote_log_name>.*) (?<remote_auth_user>.*) \[(?<log_timestamp>.*)\] "(?<request>.*)" (?<status_code>\d+) (?<response_size>\d+)
```

Analizador JSON

Puede personalizar la configuración del analizador JSON para analizar de forma selectiva el registro JSON.

Puede configurar analizadores de valores separados por comas (CSV) para recopiladores **FileLog** y **WinLog**. Solo los registros JSON válidos se analizan con el analizador JSON de Log Insight Agent. Los analizadores de registros JSON que no son válidos devuelven resultados vacíos.

La configuración predeterminada del analizador JSON extrae todos los campos del registro JSON mediante el agente de Log Insight. Cuando el registro JSON se representa como un objeto JSON complejo, que también puede contener objetos JSON, el analizador utiliza un guion bajo (_) para concatenar los nombres de los objetos JSON anidados de mayor nivel. Esto genera un nombre de campo informativo para los elementos correspondientes. Si el registro JSON también contiene una matriz, los nombres de los elementos miembro contienen el nombre de la matriz seguido del índice del elemento en la matriz.

El analizador JSON también proporciona una opción específica, conocida como **fields**.

Opción "fields" del analizador JSON

Puede usar la opción **fields** para especificar los campos que se han analizado en la configuración. El propósito de esta opción es habilitar el análisis selectivo del registro JSON.

Nota Para el análisis selectivo, debe especificar la ruta de acceso al elemento JSON deseado. Los objetos JSON de niveles diferentes deben estar separados por un punto (.).

La siguiente lista proporciona configuraciones de ejemplo que permiten analizar de manera selectiva el registro JSON, según sea necesario.

- Para analizar más de un elemento del registro JSON, los elementos deseados deben aparecer como parámetros para la opción **fields** y estar separados por comas. Consulte el siguiente ejemplo:

```
{ "operation" : { "timestamp" :
    "2018-11-22T15:28:58.094000", "thread_id" : "0x05673", "initiator" : "connector",
    "log_severity" : "info", "log_message" : "Requested connection to the server."},
  "operation_result" : "success" }
```

- Para analizar solo los objetos JSON más internos, como **timestamp**, **log_severity** y **log_message**, consulte el siguiente ejemplo. Esta configuración de ejemplo produce los siguientes resultados de campo: `operation_timestamp="2018-11-22T15:28:58.094000"` y `operation_log_severity="info"`

```
[parser|json_parser]
base_parser=json
fields=operation.timestamp,operation.log_severity, operation.log_message
```

- Para analizar el objeto JSON completo, incluya la ruta de acceso al objeto seguida de un asterisco (*).

```
{ "product_name" : "LI Agent",
  "operation" : { "timestamp" : "2018-11-22T15:28:58.094000", "thread_id" :
    "0x05673", "initiator" : "connector", "log_severity" : "info", "log_message" :
    "Requested connection to the server."}, "operation_result" :
    "success" }
```

- Para analizar solo el objeto **operation**, utilice la siguiente configuración:

```
[parser|json_parser]
base_parser=json
fields=operation.*
```

- Si el registro JSON contiene una matriz y desea analizar solo elementos específicos de la matriz, utilice el índice de elementos de la matriz en la configuración, como se muestra en esta configuración de ejemplo:

```
{
  "Records": [{
    "object": {
      "key": "/events/mykey",
      "size": 502,
      "eTag": "091820398091823",
      "sequencer": "1123123"
    }
  },
  {
    "object": {
```

```

        "key": "/events/user_key",
        "size": 128,
        "eTag": "09182039000001",
        "sequencer": "1123231"
    },
    {
        "object": {
            "key": "/events/admin_key",
            "size": 1024,
            "eTag": "09182039547241",
            "sequencer": "1123213"
        }
    }
]
}

```

- Para analizar solo los elementos **key** y **size** del mismo registro, utilice la siguiente configuración para generar los siguientes campos:

```
records0_object_key="/events/mykey"
```

```
records0_object_size=502
```

```
records2_object_key="/events/admin_key"
```

```
records2_object_size=1024
```

```

[parser|json_parser]
base_parser=json
fields = Records0.object.key Records0.object.size, Records2.object.key,
Records2.object.size

```

- Para analizar el campo **key** para todos los elementos de la matriz, utilice la siguiente configuración:

```

[parser|json_parser]
base_parser=json
fields=Records.#.object.key

```

- Para analizar todos los campos, utilice la opción "fields" con un asterisco (*). Esta configuración equivale a la configuración predeterminada del analizador JSON.

```

[parser|json_parser]
base_parser=json
fields=*

```

Desinstalar agentes de vRealize Log Insight

5

En el caso que necesite desinstalar un agente de vRealize Log Insight, siga las instrucciones que corresponden al paquete del agente que ha instalado.

Este capítulo incluye los siguientes temas:

- [Desinstalar el Log Insight Windows Agent](#)
- [Desinstalar el paquete RPM del agente de Linux de Log Insight](#)
- [Desinstalar el paquete DEB del agente de Linux de Log Insight](#)
- [Desinstalar el paquete bin del agente de Linux de Log Insight](#)
- [Desinstalar manualmente el paquete bin del agente de Linux de Log Insight](#)

Desinstalar el Log Insight Windows Agent

Puede instalar Log Insight Windows Agent desde la pantalla Programas y características del Panel de control de Windows.

Requisitos previos

Inicie sesión en el equipo Windows donde instaló el agente de Windows de vRealize Log Insight e inicie el administrador de servicios para verificar que el servicio del agente de vRealize Log Insight esté instalado.

Procedimiento

- 1 Vaya a **Panel de control > Programas y funciones**.
- 2 Seleccione VMware vRealize Log Insight Windows Agent y haga clic en **Desinstalar**.

Resultados

El desinstalador detiene el servicio de VMware vRealize Log Insight Windows Agent y elimina sus archivos del sistema.

Desinstalar el paquete RPM del agente de Linux de Log Insight

Es posible desinstalar el paquete RPM de Log Insight Linux Agent.

Requisitos previos

- Inicie sesión como **raíz** o use `sudo` para ejecutar comandos de la consola.
- Inicie sesión en la máquina Linux en la cual ha instalado Log Insight Linux Agent, abra una consola del terminal y ejecute `pgrep liagent` para verificar que VMware Log Insight Linux Agent esté instalado y en ejecución.

Procedimiento

- ◆ Ejecute el siguiente comando reemplazando *VERSION* y *BUILD_NUMBER* con la versión y número de compilación del agente instalado.

```
rpm -e VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER
```

Resultados

El desinstalador detiene el daemon de VMware Log Insight Linux Agent y elimina todos sus archivos, excepto sus propios registros del sistema.

Desinstalar el paquete DEB del agente de Linux de Log Insight

Es posible desinstalar el paquete DEB de Log Insight Linux Agent.

Requisitos previos

- Inicie sesión como **raíz** o use `sudo` para ejecutar comandos de la consola.
- Inicie sesión en la máquina Linux en la cual ha instalado Log Insight Linux Agent, abra una consola del terminal y ejecute `pgrep liagent` para verificar que VMware Log Insight Linux Agent esté instalado y en ejecución.

Procedimiento

- ◆ Ejecute el siguiente comando

```
dpkg -P vmware-log-insight-agent
```

Resultados

El desinstalador detiene el daemon de VMware Log Insight Linux Agent y elimina todos sus archivos, excepto sus propios registros del sistema.

Desinstalar el paquete bin del agente de Linux de Log Insight

Puede desinstalar el paquete .bin Log Insight Linux Agent con el script vRealize Log Insight.

Requisitos previos

- Inicie sesión como **raíz** o use `sudo` para ejecutar comandos de la consola.

- Inicie sesión en la máquina Linux en la cual ha instalado Log Insight Linux Agent, abra una consola del terminal y ejecute `pgrep liagent` para verificar que VMware vRealize Log Insight Linux Agent esté instalado y en ejecución.

Procedimiento

- 1 En el indicador de shell, introduzca el siguiente comando para iniciar el script.

```
loginsight-agent-uninstall
```

- 2 Puede verificar que la desinstalación se realizó correctamente comprobando que el código de error devuelto del siguiente comando sea 0.

```
echo $?
```

Desinstalar manualmente el paquete bin del agente de Linux de Log Insight

Puede desinstalar manualmente el paquete Log Insight Linux Agent .bin si decide no usar el script de desinstalación.

Requisitos previos

Desinstalar manualmente el paquete bin del agente de Linux de Log Insight

- Inicie sesión como **raíz** o use `sudo` para ejecutar comandos de la consola.
- Inicie sesión en la máquina Linux en la cual ha instalado Log Insight Linux Agent, abra una consola del terminal y ejecute `pgrep liagent` para verificar que VMware vRealize Log Insight Linux Agent esté instalado y en ejecución.

Procedimiento

- 1 Detenga el daemon de Log Insight Linux Agent ejecutando el siguiente comando
`sudo service liagentd stop` o `sudo /sbin/service liagentd stop` para las versiones de Linux anteriores.
- 2 Elimine los archivos de Log Insight Linux Agent en forma manual
 - `/usr/lib/loginsight-agent` - Directorio de los archivos de licencia y binarios del daemon.
 - `/usr/bin/loginsight-agent-support` - Se utiliza para generar el paquete de soporte para Log Insight Linux Agent.
 - `/var/lib/loginsight-agent` - Directorio de almacenamiento de la base de datos y archivos de configuración.
 - `/var/log/loginsight-agent` - Directorio del registro para Log Insight Linux Agent.
 - `/var/run/liagent/liagent.pid` - Log Insight Linux Agent Archivo PID. Si no se elimina en forma automática, elimine el archivo en forma manual.

- `/etc/init.d/liagentd` - Directorio del script para el daemon de Log Insight Linux Agent.
- `/usr/lib/systemd/system/liagentd.service`

Solución de problemas de agentes de vRealize Log Insight

6

La información para la solución de problemas conocidos puede ayudarle a diagnosticar y corregir problemas relacionados con el funcionamiento de los agentes de vRealize Log Insight.

Este capítulo incluye los siguientes temas:

- Crear un paquete de soporte para el Log Insight Windows Agent
- Crear un paquete de soporte para el Log Insight Linux Agent
- Definir el nivel de detalles de registro en los Log Insight Agents
- La UI de administración no muestra a Log Insight Agents
- Los agentes de vRealize Log Insight no envían eventos
- Añadir una regla de excepción saliente para Log Insight Windows Agent
- Permitir conexiones salientes desde Log Insight Windows Agent en un firewall de Windows
- Implementación masiva de Log Insight Windows Agent no finaliza correctamente
- Los Log Insight Agents rechazan certificados autofirmados
- El servidor de vRealize Log Insight rechaza la conexión para el tráfico no cifrado

Crear un paquete de soporte para el Log Insight Windows Agent

Si el Log Insight Windows Agent no funciona según lo previsto debido a un problema, puede enviar una copia de los archivos de registro y configuración al servicio de soporte de VMware.

Procedimiento

- 1 Inicie sesión en la máquina de destino donde instaló el Log Insight Windows Agent.
- 2 Haga clic en el botón de Windows **Inicio** y luego en **VMware > Agente de Log Insight: recopilar paquete de soporte**.

- 3 (opcional) Si no está disponible el acceso directo, desplácese hasta el directorio de instalación del Log Insight Windows Agent y haga doble clic en `loginsight-agent-support.exe`.

Nota El directorio de instalación predeterminado es `C:\Program Files (x86)\VMware\Log Insight Agent`

Resultados

El paquete se genera y se guarda como un archivo `.zip` en `Mis documentos`.

Pasos siguientes

Reenvíe el paquete de soporte al servicio de soporte de VMware conforme a lo solicitado.

Crear un paquete de soporte para el Log Insight Linux Agent

Si el Log Insight Linux Agent no funciona según lo previsto debido a un problema, puede enviar una copia de los archivos de registro y configuración al servicio de soporte de VMware.

Procedimiento

- 1 Inicie sesión en la máquina de destino donde instaló el Log Insight Linux Agent.
- 2 Ejecute el siguiente comando:

```
/usr/lib/loginsight-agent/bin/loginsight-agent-support
```

Resultados

El paquete se genera y se guarda como un archivo `.zip` en el directorio actual.

Pasos siguientes

Reenvíe el paquete de soporte al servicio de soporte de VMware conforme a lo solicitado.

Definir el nivel de detalles de registro en los Log Insight Agents

Puede editar el archivo de configuración del agente de vRealize Log Insight para que cambie el nivel de registro.

Requisitos previos

Para el Log Insight Linux Agent:

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

Para el Log Insight Windows Agent:

- Inicie sesión en el equipo Windows donde instaló el agente de Windows de vRealize Log Insight e inicie el administrador de servicios para verificar que el servicio del agente de vRealize Log Insight esté instalado.

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 Abra el archivo `liagent.ini` en cualquier editor de texto.
- 3 Cambie el nivel de depuración de registros en la sección `[logging]` del archivo `liagent.ini`.

Nota Cuanto mayor es el nivel de depuración, mayor es el impacto que tiene en el agente de vRealize Log Insight. El valor predeterminado y recomendado es 0. El nivel 1 de depuración proporciona más información y se recomienda para solucionar la mayoría de los problemas. El nivel 2 de depuración proporciona información detallada. Use los niveles 1 y 2 únicamente cuando se lo solicite el soporte de VMware.

```
[logging]
; The level of debug messages to enable: 0..2
debug_level=1
```

- 4 Guarde y cierre el archivo `liagent.ini`.

Resultados

Se cambia el nivel de depuración de registros.

La UI de administración no muestra a Log Insight Agents

No aparece la información acerca de Log Insight Agents en la página Agentes de la UI de administración.

Problema

Después de instalar los Log Insight Agents, no puede ver los Log Insight Agents en la página Agentes de la UI de administración.

Causa

Las causas más frecuentes son los problemas de conectividad de red o la configuración incorrecta de Log Insight Agents en el archivo `liagent.ini`.

Solución

- ◆ Compruebe que el sistema Windows o Linux en el que Log Insight Agent está instalado tenga conectividad con el servidor vRealize Log Insight.
- ◆ Compruebe que los Log Insight Agents usen el protocolo cfapi.
Cuando utiliza el protocolo syslog, la UI no muestra Log Insight Windows Agents.
- ◆ Vea los contenidos de los archivos de registro de Log Insight Agents ubicados en los siguientes directorios.
 - Windows: %ProgramData%\VMware\Log Insight Agent\log
 - Linux: /var/log/loginsight-agent/

Busque los mensajes de registro que contienen las frases `Error de transporte de config: no se pudo resolver el nombre de host` y `Error de resolutor. No se conoce el host`.
- ◆ Compruebe que el `liagent.ini` contenga la configuración correcta para el servidor vRealize Log Insight de destino. Consulte [Configurar el servidor vRealize Log Insight de destino](#) y [Especificar el destino de un agente](#).

Los agentes de vRealize Log Insight no envían eventos

Una configuración incorrecta puede evitar que los agentes de vRealize Log Insight reenvíen eventos al servidor de vRealize Log Insight. Si un canal de recopilación de archivos no está correctamente configurado, puede ver mensajes como “Invalid settings were obtained for channel 'CHANNEL_NAME'. Channel 'CHANNEL_NAME' will stay dormant until properly configured”.

Problema

Las instancias de los agentes de vRealize Log Insight aparecen en la página **Agente > de administración**, pero no aparecen eventos en la página **Análisis interactivo** de los nombres de host de los agentes de vRealize Log Insight. El canal de recopilación de archivos planos no está correctamente configurado.

Causa

Una configuración incorrecta puede evitar que los agentes de vRealize Log Insight reenvíen eventos al servidor de vRealize Log Insight.

Solución

- ◆ Defina un canal de recopilación válido. Verifique si el canal de recopilación de archivos planos está correctamente configurado. Consulte [Capítulo 4 Configurar agentes de vRealize Log Insight](#).

- ◆ Para el agente de Windows de vRealize Log Insight, intente lo siguiente.
 - Si los canales de Windows están habilitados, vea el contenido de los archivos de registro del agente de Windows de vRealize Log Insight situados en %ProgramData%\VMware\Log Insight Agent\log. Busque mensajes de registro relacionados con la configuración de canales que incluyen las frases `Subscribed to channel CHANNEL_NAME`. Los canales que se usan con frecuencia son `Application`, `System` y `Security`.
 - Si un canal no está configurado correctamente, puede ver mensajes de registro similares a `Could not subscribe to channel CHANNEL_NAME events. Código de error: 15007. No se pudo encontrar el canal especificado. Compruebe la configuración del canal. Puede ver un número de código de error diferente a 15007.`
 - Si un canal de recopilación de archivos no está correctamente configurado, puede ver mensajes como `Invalid settings were obtained for channel 'CHANNEL_NAME'. Channel 'CHANNEL_NAME' will stay dormant until properly configured`.
- ◆ Para el agente de Windows de vRealize Log Insight y el agente de Linux de vRealize Log Insight, intente lo siguiente.
 - ◆ Si no hay canal de recopilación de archivos planos configurado, puede ver mensajes similares a `Cannot find section 'filelog' in the configuration. The flat file log collector will stay dormant until properly configured`

El contenido de los archivos de registro de los agentes de vRealize Log Insight está situado en los siguientes directorios.

 - Windows: %ProgramData%\VMware\Log Insight Agent\log
 - Linux: /var/log/loginsight-agent/

Pasos siguientes

Para obtener más información sobre la configuración de los agentes de vRealize Log Insight, consulte [Configurar Log Insight Windows Agent](#) y [Configurar Log Insight Linux Agent](#).

Añadir una regla de excepción saliente para Log Insight Windows Agent

Defina una regla de excepción para desbloquear Log Insight Windows Agent en el firewall de Windows.

El procedimiento se aplica a Windows Server 2008 R2 y versiones posteriores, y a Windows 7 y versiones posteriores.

Requisitos previos

- Verifique que tenga una cuenta de administrador o una cuenta con privilegios de administrador.

Procedimiento

- 1 Seleccione **Inicio > Ejecutar**.
- 2 Escriba `wf.msc` y haga clic en **Aceptar**.
- 3 Haga clic con el botón derecho en **Reglas salientes** en el panel izquierdo y haga clic en **Nueva regla**.
- 4 Seleccione **Personalizar** y siga las instrucciones del asistente para configurar las opciones siguientes.

Opción	Descripción
Programa	<code>liwinsvc.exe</code>
Servicio	LogInsightAgentService
Protocolo y puertos	TCP 9000 para cfapi y 514 para syslog

- 5 En la página Especificar los perfiles para los cuales se aplica esta regla, seleccione el tipo de red adecuado.
 - Dominio
 - Pública
 - Privada

Nota Puede seleccionar todos los tipos de red para asegurarse de que la regla de excepción esté activa independientemente del tipo de red.

Pasos siguientes

Diríjase al directorio de registro Log Insight Windows Agent%ProgramData%\VMware\Log Insight Agent\log y abra el archivo de registro más reciente. Si los eventos recientes contienen los mensajes `Error de transporte de config: no se pudo resolver el nombre de host` y `Error de resolutor. Host desconocido`, reinicie el servicio de Log Insight Windows Agent y el equipo Windows.

Nota El servicio de Log Insight Windows Agent puede demorar hasta 5 minutos en volver a conectarse con el servidor.

Permitir conexiones salientes desde Log Insight Windows Agent en un firewall de Windows

Configure los parámetros de firewall de Windows para permitir las conexiones salientes de Log Insight Windows Agent al servidor vRealize Log Insight.

Después de instalar e iniciar el servicio de Log Insight Windows Agent, el firewall local o de dominio Windows puede restringir la conectividad al servidor vRealize Log Insight de destino.

El procedimiento se aplica a Windows Server 2008 R2 y versiones posteriores, y a Windows 7 y versiones posteriores.

Requisitos previos

- Verifique que tenga una cuenta de administrador o una cuenta con privilegios de administrador.

Procedimiento

- 1 Seleccione **Inicio > Ejecutar**.
- 2 Escriba `wf.msc` y haga clic en **Aceptar**.
- 3 En el panel Acciones, haga clic en **Propiedades**.
- 4 En la pestaña **Perfil de dominio**, seleccione **Permitir (predeterminado)** del menú desplegable **Conexiones salientes**.

Si el equipo no está conectado a un dominio, puede seleccionar **Perfil privado** o **Perfil público**, según el tipo de red al que esté conectado el equipo.

- 5 Haga clic en **Aceptar**.

Pasos siguientes

Defina una regla de excepción de desbloqueo de Log Insight Windows Agent en el firewall de Windows. Consulte [Añadir una regla de excepción saliente para Log Insight Windows Agent](#).

Implementación masiva de Log Insight Windows Agent no finaliza correctamente

La implementación masiva de Log Insight Windows Agent no finaliza correctamente en las máquinas de destino.

Problema

Después de realizar una implementación masiva en máquinas de dominio de Windows usando Objetos de directivas de grupo, el Log Insight Windows Agent no puede instalarse como un servicio local.

Causa

La configuración de directivas de grupo puede evitar que Log Insight Windows Agent se instale correctamente.

Solución

- 1 Edite la configuración de Objetos de directivas de grupo (GPO) y vuelva a implementar el agente de Windows de Log Insight.
 - a Haga clic con el botón derecho en el GPO, haga clic en **Editar** y desplácese hasta **Configuración de equipos > Directivas > Plantillas administrativas > Sistema > Inicio de sesión**.
 - b Habilite la directiva **Siempre esperar la red al inicio del equipo e inicio de sesión**.
 - c Desplácese hasta **Configuración de equipos > Directivas > Plantillas administrativas > Sistema > Directiva de grupo**.
 - d Habilite **Tiempo de espera de procesamiento de directiva de inicio**, y establezca **Cantidad de tiempo para esperar (en segundos)** en 120.
- 2 Ejecute el comando `gpupdate /force /boot` en las máquinas de destino.

Los Log Insight Agents rechazan certificados autofirmados

Los Log Insight Agents rechazan el certificado autofirmado.

Problema

Un agente de vRealize Log Insight rechaza el certificado autofirmado y no puede establecer una conexión con el servidor.

Nota Si experimenta problemas de conexión con el agente, puede generar registros detallados y consultarlos. Para ello, cambie el nivel de depuración del agente a 1. Para obtener más información, consulte [Definir el nivel de detalles de registro en los Log Insight Agents](#).

Causa

Los mensajes que aparecen en el registro del agente incluyen motivos específicos.

Message (Mensaje)	Causa
Rechazo del certificado autofirmado del mismo nivel. La clave pública no coincide con la clave del certificado almacenada previamente.	<ul style="list-style-type: none"> ■ Esto puede suceder cuando se reemplaza el certificado devRealize Log Insight. ■ Esto puede suceder si la HA habilitada en el entorno del clúster está configurada con certificados autofirmados diferentes en los nodos de vRealize Log Insight.
Rechazo del certificado autofirmado del mismo nivel. Tiene un certificado recibido previamente que fue firmado por una CA de confianza.	Hay un certificado firmado por una CA almacenado en el agente.

Solución

- ◆ Verifique si su nombre de host de destino es una instancia de vRealize Log Insight de confianza y luego elimine manualmente el certificado previo del agente de vRealize Log Insight, directorio `cert`.
 - Para Log Insight Windows Agent, vaya a `C:\ProgramData\VMware\Log Insight Agent\cert`.
 - Para Log Insight Linux Agent, vaya a `/var/lib/loginsight-agent/cert`.

Nota Algunas plataformas pueden usar rutas de acceso no estándar para almacenar certificados de confianza. Los Log Insight Agents tienen una opción que permite configurar la ruta de acceso al almacén de certificados de confianza estableciendo el parámetro de configuración `ssl_ca_path=<fullpath>`. Reemplace `<fullpath>` por la ruta de acceso al archivo del paquete de certificados raíz de confianza. Consulte [Configurar los parámetros SSL de agentes de Log Insight](#).

El servidor de vRealize Log Insight rechaza la conexión para el tráfico no cifrado

El servidor de vRealize Log Insight rechaza la conexión con Log Insight Agents cuando intenta enviar tráfico no cifrado.

Puede configurar un servidor de vRealize Log Insight para que acepte conexiones diferentes de SSL o configurar Log Insight Agents para que envíe datos a través de la conexión de un protocolo `cfapi` de SSL.

Problema

Cuando intenta usar `cfapi` para enviar tráfico no cifrado, el servidor de vRealize Log Insight rechaza su conexión. Uno de los siguientes mensajes de error aparece en el registro del agente: `403 Prohibido` o `403 Solo se permiten conexiones SSL`.

Causa

vRealize Log Insight está configurado para aceptar únicamente conexiones SSL, pero los Log Insight Agents están configurados para usar una conexión distinta.

Solución

- 1 Configure el servidor de vRealize Log Insight para que acepte conexiones diferentes de SSL.
 - a Desplácese hasta la pestaña **Administración**.
 - b En Configuración, haga clic en **SSL**.
 - c En el encabezado API Server SSL, desmarque la casilla **Exigir conexión SSL**.
 - d Haga clic en **Guardar**.

2 Configure el agente de vRealize Log Insight para que envíe datos a través de la conexión de un protocolo Cfapi de SSL.

- a 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>

- b Abra el archivo `liagent.ini` en cualquier editor de texto.
- c Cambie el valor de la clave `ssl` en la sección `[server]` del archivo `liagent.ini` a `yes` y el protocolo a `cfapi`.

```
proto=cfapi
ssl=yes
```

- d Guarde y cierre el archivo `liagent.ini`.